dicampus

Política de Seguridad de la Información

Elaborado por Comité de Seguridad	Aprobado por CEO
Fecha: 01/03/2024	Fecha: 01/03/2024
 Firma:	 Firma:

ÍNDICE

TABLA DE REVISIONES

Versión	Resumen De Los Cambios Producidos	Elaborado Por		Revisado Por		Aprobado Por	
		Nombre	Fecha	Nombre	Fecha	Nombre	Fecha
Inicial – E00	Elaboración del Documento	Jonatan Rozada	Mar'24	Isabel Barrio	Mar'24	Isabel Barrio	Mar'24

LISTA DE DISTRIBUCIÓN

Exclusivamente el personal relacionado a continuación está autorizado para acceder al presente documento:

Responsable	**Responsable de Seguridad de la Información.**
Lista de personal autorizado a acceder al documento:	
Todo el personal de la Entidad	

1 OBJETO

El objeto de la presente Política de seguridad de la información es determinar el alcance y estructura del sistema de Información (SI) implantado en la organización, en base a las directrices determinadas por las normativas de referencia en la materia, ENS (Esquema Nacional de Seguridad) y Norma ISO 27001.

2 CAMPO DE APLICACIÓN

Esta política afecta a todo el personal de **DICAMPUS**.

El alcance del Sistema de Gestión de la Seguridad de la Información de **DICAMPUS** es el siguiente:

Los sistemas de información utilizados para prestar los servicios de diseño, seguimiento, gestión e impartición de acciones formativas en modalidad presencial, teleformación o mixtas, atendiendo a la declaración de aplicabilidad vigente.

3 DEFINICIONES

No aplica.

4 MISIÓN Y OBJETIVOS

DICAMPUS unifica las perspectivas legal y tecnológica para ofrecer a sus clientes una solución integral a sus necesidades relacionadas con el Diseño, Instalación y Mantenimiento de Sistemas de Telecomunicaciones, y resto de servicios descritos en el Alcance.

DICAMPUS basa su actividad en el tratamiento de diferentes tipos de datos e información, ello le permite ejecutar procesos básicos propios del negocio. Los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyen el activo principal de **DICAMPUS**, de tal manera que el daño o pérdida de los mismos inciden en la realización de sus operaciones, y pueden poner en peligro la continuidad de la Organización.

Todo ello a través de escenarios de innovación permanente, investigación y desarrollo como elementos clave, y una cultura totalmente orientada a la excelencia en el servicio y al establecimiento de un marco de relación con los clientes y colaboradores/as como socios/as de negocio.

Estas cuestiones se materializan con las aportaciones de un amplio equipo de personas formadas, certificadas y en permanente actualización de conocimientos, así como en métodos y prácticas.

La excelencia en la ejecución, la fidelidad en el marco de relaciones y la empatía hacia el cliente y entre compañeros/as actúan como valores y principios básicos que rigen nuestra actuación.

En el ámbito concreto de la seguridad, el SI corporativo pretende lograr alcanzar **los siguientes objetivos**:

- Cumplir con las necesidades y expectativas de las partes interesadas involucradas dentro del alcance del SI protegiendo la información interna y relacionada con la prestación de los servicios, considerando las dimensiones de:
    - **Confidencialidad** para asegurar que la información solo sea accedida por aquellos que cuenten con la autorización respectiva. Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.

- **Integridad** para preservar la veracidad y completitud de la información y los métodos de procesamiento. Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
- **Disponibilidad** para asegurar que los usuarios autorizados tienen acceso a la información y los procesos, sistemas y redes que la soportan, cuando se requiera. La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.
- **Trazabilidad**: Para asegurar que queda constancia fehaciente del uso del servicio y del acceso a los datos, es decir, que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. Toda acción desarrollada en el sistema o sobre la información, puede ser imputada a su autor, en cualquier fase de ciclo de vida o en cualquier fase de proceso.
- **Autenticidad**: Para asegurar que quien accede al servicio es realmente quien se cree y garantizar la fuente de la que proceden los datos. Toda información puede ser asignada a una fuente o todo autor puede ser contrastado y acreditar su identidad sin lugar a duda.

- Demostrar liderazgo por parte de la dirección, dotando de recursos al SI y asegurando que la política y los objetivos de seguridad que se establezcan sean compatibles con la estrategia de la organización.
- Gestionar la implementación del SI de manera que proporcione ventajas competitivas en relación con otros agentes del sector, aprovechando la inercia que puede otorgar la gestión adecuada de la seguridad.
- Apostar por la **mejora continua**, y la implementación de medidas de seguridad eficaces y eficientes.
- Establecer anualmente objetivos, relacionados con ámbitos específicos de seguridad alineados con las normas de referencia del SI, ENS e ISO 27001.

- Cumplir con los requisitos del negocio, legales o reglamentarios y las obligaciones contractuales de seguridad, alineando dichos requisitos con la privacidad y la seguridad de la información corporativa.
- Sensibilizar y concienciar de manera estable y permanente a todo el personal de la organización en cuanto a la seguridad de la información.
- Fomentar y mantener el buen nombre de la organización en relación con los servicios desarrollados, saber y respuesta activa (reactiva y proactiva) ante incidentes de seguridad, mantenimiento la imagen y reputación.

5 PRINCIPIOS

La política de seguridad de la información de **DICAMPUS se desarrolla de acuerdo con los siguientes principios:**

- **Principio de confidencialidad**: se deberá garantizar que la información sea accesible únicamente para aquellas personas expresamente autorizadas para ello.
- **Principio de integridad**: se deberá asegurar que la información con la que se trabaja sea completa y precisa, y se incidirá en la exactitud tanto de su contenido como de los procesos involucrados.
- **Principio de disponibilidad**: se garantizará la prestación continua de los servicios y la recuperación inmediata ante posibles contingencias, mediante medidas de recuperación orientadas a la restauración de los servicios y de la información asociada.
- **Principio de gestión del riesgo**: Se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre las medidas de seguridad y la naturaleza de la información.
- **Principio de mejora continua**: se revisará de manera recurrente el grado de eficacia de los controles de seguridad implantados para aumentar la capacidad de adaptación a la constante evolución del entorno.
- **Principio de proporcionalidad en coste**: la implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.
- **Principio de cumplimiento normativo**: todos los sistemas de información se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial aquella relacionada con la intimidad y la protección de datos de carácter personal y con la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.
- **Principio de prevención**: Los departamentos deben 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 los departamentos deben 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, los departamentos deben: 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.
- **Principio de 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.
- **Principio de respuesta**: Los departamentos deben: 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).
- **Principio de recuperación**: Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

6 MARCO NORMATIVO

La presente política se rige por la siguiente legislación y normativa de referencia:

- **Real Decreto 311/2022 de 3 de mayo**, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- **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.
- **Ley Orgánica 3/2018, de 5 de diciembre**, de Protección de Datos Personales y garantía de los derechos digitales.
- **Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas**, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- **Guías CCN-STIC (800).**
- **UNE/ISO-IEC 27001**
- **UNE/ISO-IEC 27002**

7 ROLES Y FUNCIONES; ORGANIZACIÓN DE LA SEGURIDAD

DICAMPUS dispone de un **Comité de Seguridad de la Información** formado por diferentes roles, para atender las necesidades de seguridad tanto técnicas como organizativas, permitiendo de esta forma una mejor distribución de la información y toma de decisiones.

Estos recursos, comienzan por la designación de la seguridad como función diferenciada mediante los siguientes miembros y funciones:

- **Responsable de la información** que determinará los requisitos de la información tratada. Para desempeñar este rol, se nombra a Clara Prieto Suárez.
- **Responsable del servicio** que determinará los requisitos de los servicios prestados. Para desempeñar este rol, se nombra a Orlando M. López Alonso.
- **Responsable del Tratamiento (Protección de Datos)**: que determina los fines y medios del tratamiento. Este rol lo desempeña DICAMPUS S.L.
- **Responsable de Seguridad** (CISO) que determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. Para desempeñar este rol, se nombra a Jonatan Rozada. Será además la persona de contacto (POC) para la seguridad de la información tratada y el servicio prestado. Actuará como enlace entre organizaciones y proveedor externo, garantizará la seguridad de la información y coordinará las respuestas ante incidentes.
- **Delegado de Protección de Datos**: que informará, asesorará, y supervisará sobre el cumplimiento en materia de protección de datos de carácter personal incluidos los aspectos de seguridad (integridad, confidencialidad y disponibilidad) y violación de datos personales asesorando sobre la necesidad o no de notificación a la autoridad de control y, en su caso a los propios interesados y comunicando en su caso el incidente a la autoridad de control de protección de datos en virtud de su rol de punto de contacto previsto en el RGPD y la LOPDGDD. Para desempeñar este rol, se nombra a PRODAT PRINCIPADO, S.L

Su nombramiento lo debe realizar el responsable de tratamiento de manera diferenciada al resto de miembros de Comité de Seguridad ya que sus cometidos no se ciñen únicamente a aspectos de seguridad. Para evitar el conflicto de intereses, debe tener voz pero no voto en la decisiones y deliberaciones del Comité de Seguridad.

- **Responsable del Sistema** (CIO) se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad. Para desempeñar este rol, se nombra a Alejandro López.

El procedimiento para su designación y renovación se encuentra documentado en **ENS-04 Rev. 00 Asignación de Responsabilidades para la SI.**

Se ha considerado que las funciones del Responsable de Servicio y del responsable de la información, sean asumidas por el Comité de Seguridad de la Información, y que solamente en casos puntuales, sea el Responsable del servicio quien las decisiones que sean necesarias.

Las funciones concretas de cada uno de los roles aquí definidos, así como los mecanismos de coordinación y resolución de conflictos, vienen definidos en el documento del SI, **ENS-04 Rev. 00 Asignación de Responsabilidades para la SI.**

8 COMPROMISO DE LA DIRECCIÓN

La presente **Política Interna de Seguridad de la Información** marca las líneas de actuación, normativa y compromisos de la Empresa respecto a la Seguridad de la Información, por lo que la Dirección proporciona las líneas de actuación, recursos, responsabilidades y compromisos al respecto.

La Política es aprobada y revisada de manera periódica por la Dirección y comunicada a todos los empleados para que conozcan los objetivos, normativa y responsabilidades generales y específicas en materia de Seguridad de la Información, así como la importancia de su cumplimento.

9 POLÍTICA DE USO DE LOS SISTEMAS DE INFORMACIÓN

El uso generalizado de los Sistemas de Información por parte de los usuarios hace imprescindible que todos/as los/las empleados/as sean conscientes de su responsabilidad, así como de la importancia de proteger la Información. Tanto los Sistemas como la Información son propiedad de Dicampus y deben ser utilizados para fines exclusivamente laborales.

La presente **Política Interna de Seguridad de la Información**, así como las **Cláusulas de Confidencialidad y Protección de Datos** (de acuerdo a la RGPD) recogidas en el Contrato de Trabajo y los procesos asociados a cada puesto, son de obligado cumplimiento por parte de todo el personal de la Organización, constituyendo su incumplimiento una infracción grave a efectos laborales.

La Dirección de Dicampus ha definido para los usuarios de la Organización, en función de los perfiles funcionales y puestos de trabajo, distintos permisos de acceso físico y lógico tanto a losSistemas como a la Información.

10 GESTIÓN DE LOS RECURSOS HUMANOS

El empleado/a es el gran protagonista de la seguridad en la Empresa. La tecnología es importante, pero no siempre es suficiente para proteger los Sistemas de Información, por tanto, la implicación y participación de todos/as los/as empleados/as como usuarios de los Sistemas, resulta esencial para llevar una

adecuada gestión de la seguridad de la información dentro de la Organización. Concienciar y formar a los empleados, se convierte en una de las piezas clave para crear una cultura de seguridad en la Organización, reduciendo de este modo los riesgos globales a los que se enfrenta: errores humanos, robos, fraudes, fugas de Información, mal usode las instalaciones y de los Sistemas de Información, etc.

En las condiciones de la relación laboral quedan reflejadas las responsabilidades del empleado/a en materia de seguridad de la Información. Esta responsabilidad continuará tras la finalización del Contrato. La presente **Política Interna de Seguridad de la Información**, así como las **Cláusulas de Confidencialidad y Protección de Datos** (de acuerdo a la RGPD) recogidas en el Contrato de Trabajo y los procesos asociados a cada puesto, son de obligado cumplimiento por parte de todos /as los/as empleados/as de la Empresa, constituyendo su incumplimiento una infracción grave a efectos laborales.

El intercambio de Información por parte de los empleados de la Empresa puede realizarse de manera:

- **Electrónica**. El personal, cuando acceda y trate la Información contenida en los Sistemas de Información (servidores, estaciones de trabajo, dispositivos móviles, internet, correo electrónico, impresoras), debe cumplir con la normativa de seguridad descrita en los apartados anteriores, así como con la legislación vigente aplicable a la Información transmitida.
- **Verbal**. El personal, cuando comunique verbalmente Información confidencial o sensible, debe tomar las precauciones necesarias para evitar ser oído, accidental o intencionadamente. No se debe hablar públicamente sobre Información confidencial de la Empresa en pasillos, áreas de descanso, fuera de las instalaciones, etc., ni dejar mensajes confidenciales en contestadores o grabadores, de manera que personas no autorizadas puedan acceder a la Información.
- **Soporte Papel**: El personal debe tomar las medidas de protección adecuadas para garantizar la seguridad de la Información en soporte papel, máxime si se trata de Información confidencial o datos de carácter personal protegidos por la RGPD, protegiéndola siempre contra accesos no autorizados.

Una vez finalizada la relación laboral o contractual con los/as empleados/as y con el personal externo, la Empresa procederá a la retirada de los permisos de acceso a las Instalaciones, a los Sistemas y a la Información, requiriéndose la devolución de cualquier tipo de Dispositivo móvil o Información que fue entregada al empleado/a para el desarrollo de sus tareas y funciones.

11 MANTENIMIENTO DE LOS SISTEMAS Y GESTIÓN DE INCIDENTES

La Empresa, a través de su Departamento de Sistemas, está facultada para realizar sin previo aviso todas las tareas de mantenimiento, correctivo y preventivo, que sean necesarias sobre los Sistemas de Información, así como eliminar aquellos elementos que puedan causar problemas en el normal funcionamiento de los Sistemas y de los servicios.

Un **Incidente de Seguridad de la Información** es un evento de seguridad de la Información, inesperado o no deseado, que tiene una probabilidad significativa de comprometer las operaciones Empresariales y de amenazar la seguridad de la Información.

Mientras que un **Incidente en los Sistemas de Información,** es cualquier evento que no es parte del funcionamiento normal del servicio y que causa o puede causar interrupciones de dicho servicio o una disminución de la calidad del mismo.

Por tanto, cualquier usuario que detecte un **Incidente en los Sistemas de Información** (fallo, mal funcionamiento, interrupción, comportamiento extraño o inesperado), así como un **Incidente de Seguridad de la Información** (pérdida, robo de dispositivos móviles o de Información, denegación de servicio, acceso no autorizado, infección de virus, etc. que el usuario prevea que pueda amenazar la seguridad de la Información), debe notificarlo lo antes posible al Departamento de Sistemas.

Además, en caso de **robo de Dispositivos móviles**, el usuario debe informar de inmediato al Responsable de Sistemas y presentar una denuncia a las fuerzas y cuerpos de seguridad donde se haya producido.

12 SEGUIMIENTO, SUPERVISIÓN Y MONITARIZACIÓN DE LOS SISTEMAS DE INFORMACIÓN

La Empresa, en el ejercicio de sus atribuciones, podrá establecer los medios y mecanismos que considere más oportunos de **vigilancia, monitorización y seguimiento de los Sistemas de Información** (servidores, estaciones de trabajo, dispositivos móviles, internet, correo electrónico, impresoras, etc.) para verificar el cumplimiento por parte de los trabajadores de susobligaciones y deberes laborales, garantizar la seguridad de la Información y comprobar el buen funcionamiento de los mismos, guardando siempre en su adopción y aplicación la consideración debida a la dignidad humana, respetando los principios de proporcionalidad y teniendo en cuenta la capacidad real de los trabajadores discapacitados (en su caso), de acuerdo al artículo 20.3 del Estatuto de los Trabajadores.

Sin perjuicio de que los medios o mecanismos de verificación puedan ser utilizados para la aplicación del régimen de faltas y sanciones previsto en el Convenio Colectivo de la Empresa o en la legislación laboral aplicable, por incumplimiento por parte de los trabajadores, la Empresa se reserva el derecho de:

- Monitorizar, auditar y mantener trazas de las acciones llevadas a cabo por los usuarios en los Sistemas de Información y en los equipos y dispositivos personales (autorizados por el Responsable del Sistema, a conectarse a la red interna de la Organización con el fin de realizar tareas de trabajo). Así como realizar las acciones de mantenimiento que se consideren oportunas para garantizar el buen funcionamiento de los mismos.
- Monitorizar el origen y el destino de los accesos a los Sistemas de Información, así como el volumen y contenido de la Información enviada y recibida. Pudiendo realizar auditorías periódicas de los registros de los accesos de los usuarios e iniciar las actuaciones administrativas correspondientes por el uso inadecuado de los mismos.
- Monitorizar el origen y el destino tanto de los mensajes de correo electrónico como de los accesos a internet y el volumen de la Información enviada y recibida. Pudiendo acceder y/o revelar el contenido de los mensajes y de la Información enviada y

recibida, por motivos laborales fundamentados de seguridad o de requerimiento legal.

13 ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD

El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en niveles, según el ámbito de aplicación y el nivel de detalle técnico. Dichos niveles de desarrollo son los siguientes:

- Políticas de seguridad de la información, constituido por el presente documento y el manual de seguridad.
- Normativas de obligado cumplimiento, asociados a diferentes ámbitos normativos, por ejemplo, la normativa de seguridad para empleados/as.
- Procedimientos operativos, documentos que describen explícitamente y paso a paso como realizar una cierta actividad, por ejemplo, gestión de incidentes, o copias de seguridad.
- Procedimientos técnicos / Instrucciones Técnicas, propios del área de sistemas, especifican, por ejemplo, los distintos tratamientos asociados a tipologías de incidente.

14 DATOS DE CARÁCTER PERSONAL

Los **riesgos que pueden afectar a seguridad e integridad de los datos personales** pueden ser de muy diversa índole, tales como:

- Desastres naturales: Fuego, agua, desastres ambientales…
- Errores y fallos de los sujetos autorizados para su tratamiento: destrucción no intencionada, programación inadecuada de un proceso de perfilado, fuga de información…
- Ataques informáticos: *hacking, phishing, malware*, robo…
- Incumplimiento de la normativa de protección de datos: incumplimiento del periodo de retención, ausencia de base legitimadora del tratamiento…

Si la amenaza la enfocamos desde la materia en protección de datos, se puede categorizar en 5 **tipos** en base a la tipología de daño que pueden producir en los datos:

- **Confidencialidad: acceso ilegítimo a los datos**(fuga de información, uso ilegítimo de datos, pérdida de dispositivos móviles, acceso por personal no autorizado, etc.)
- **Integridad: modificación no autorizada de los datos**(errores en los procesos de recopilación y captura de datos, modificación no autorizada de datos de forma intencionada, suplantación de identidad, etc.)
- **Disponibilidad: eliminación de los datos**(error o ataque intencionado que provoque el borrado o pérdida de datos, desastres naturales, cortes en el suministro eléctrico o en los servicios de comunicación, etc.)
- **Autenticidad: acceso no autorizado a la información**(fuga de información, ataques informáticos.)
- **Trazabilidad: Seguimiento del ciclo de vida de la información(**incumplimiento del periodo de retención, ausencia de base legitimadora del tratamiento).

En relación con el tratamiento de los datos personales, este se hará ajustándose a la regulación vigente, acogiéndose de manera especial al cumplimiento del RGPD y la RGPDGDD.

15 DOCUMENTACIÓN DE REFERENCIA

Todos los documentos necesarios en este Procedimiento se relacionan a continuación:

- ENS-04 Rev. 00 Asignación de Responsabilidades para la SI.
- Acta del Comité de Seguridad con los nombramientos asociados a cada uno de los Roles relativos a Seguridad de la Información.

16 REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad de la Información será examinada en las revisiones del Sistema por la Dirección, a través del Comité de Seguridad de la Información, siempre que se produzcan cambios significativos, como mínimo, una vez al año.

La aceptación de esta Política implica su cumplimiento en el acceso de todas y cada una de las aplicaciones internas de Dicampus, tanto en materia de protección de datos, gestión de la información, etc.