POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE INNOVACIÓN RIOJANA DE SOLUCIONES IT (CIRCULAR UNIVERSE)

Código:	P-SI
Versión:	4.00
Fecha de la versión:	12/04/2024
Aprobado por:	Comité de Seguridad
Nivel de confidencialidad:	Publico

Historial de modificaciones

Fecha	Versión	Aprobado por	Descripción de la modificación
07/12/2023	1.00	Comité de Seguridad	Descripción básica del documento
05/02/2024	2.00	Comité de Seguridad	Se ha añadido el Comité de IT en el apartado 5.
10/03/2024	3.00	Comité de Seguridad	Corrección de erratas encontradas durante la revisión para la auditoría.
12/04/2024	4.00	Comité de Seguridad	Añadido línea de alta dirección

Tabla de contenido

Introducción

La información constituye un activo de primer orden para Circular Universe, ya que resulta imprescindible para la prestación de los servicios que ofrece a terceras partes. Por su parte, las tecnologías de la información y las comunicaciones (TIC) se han hecho imprescindibles para las organizaciones, ya que contribuyen de forma muy eficaz al tratamiento de esa información. Sin embargo, las mejoras que aportan las TIC al tratamiento de la información vienen acompañadas de nuevos riesgos. Por esa razón es necesario introducir medidas específicas para proteger tanto la información como los servicios que dependen de ella.

La seguridad de la información tiene como objetivo proteger la información y los servicios, reduciendo los riesgos a los que están sometidos hasta un nivel que resulte aceptable. El presente documento establece la Política de Seguridad de la Información de Circular Universe para asegurar que todo el personal a su servicio tanto directa como indirectamente, conoce, dirige y da soporte a la seguridad de la información.

Con ello se pretende lograr el alineamiento estratégico de la gestión de la seguridad de la información con las normas internacionales y las regulaciones legislativas existentes en la materia.

1. Misión y objetivos de la política de seguridad de la información

Circular Universe ha establecido un alineamiento con la gestión de la seguridad de la información según lo establecido en los marcos normativos del estándar de mercados ISO27001 y Esquema Nacional de Seguridad, reconociendo como activos estratégicos, la información y los sistemas que soportan.

Uno de los objetivos fundamentales de la implantación de esta Política de Seguridad es establecer las bases sobre las que tanto empleados internos, como terceras partes, puedan acceder a los servicios ofrecidos por Circular Universe en un entorno seguro y de confianza.

La Política de Seguridad de la Información define el marco global para la gestión de la seguridad de la información protegiendo todos los activos de la información y garantizando la continuidad en el funcionamiento de los sistemas. Se pretende de esta forma minimizar los riesgos derivados de una posible falla en la seguridad y asegurar el cumplimiento de los objetivos de Circular Universe ante un hipotético incidente de seguridad de la información.

Para ello, se establecen los siguientes objetivos generales en materia de seguridad de la información:

1. Contribuir desde la gestión de seguridad al cumplimiento de la misión y objetivos establecidos por Circular Universe.

2. Disponer de las medidas de control necesarias para garantizar el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos o telemáticos.

3. Asegurar la accesibilidad, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

4. Asegurar la prestación continuada de los servicios, tanto de forma preventiva como de forma reactiva ante los incidentes de seguridad.

5. Proteger los activos de información de Circular Universe y la tecnología que los soporta frente a cualquier amenaza, intencionada o accidental, interna o externa, con el fin de asegurar la confidencialidad, integridad y disponibilidad de estos.

Esta Política de Seguridad asegura y expone el compromiso continuo y manifiesto de la dirección de Circular Universe, para la difusión y consolidación de la cultura de la seguridad, así como la implantación y mantenimiento de infraestructura y procedimientos seguros en los distintos sistemas de la información de acuerdo con lo dispuesto por las normas y legislación de aplicación.

Dentro de este compromiso continuo de la alta dirección se pondrá especial hincapié en la dotación de recursos para: formación, implementación de arquitectura de seguridad, fomentar la productividad y eficiencia de los equipos de trabajo, promover el bienestar y satisfacción de sus empleados, y mitigar los riesgos potenciales y residuales.

2. Alcance

Esta Política de seguridad se aplicará a toda la información de Circular Universe. A estos efectos se entiende por Circular Universe:

- Las oficinas en C/ Valdegastea 2, Logroño, La Rioja.

Esta Política no se limita a los datos de carácter personal y es independiente de que el tratamiento sea manual o automatizado.

3. Marco normativo

La legislación en materia de seguridad de la información, que debe servir de referencia, se actualiza de forma continua y se queda reflejado en el **"Anexo: Legislación aplicable"**.

4. Revisión de la política

En relación con las revisiones que puedan realizarse sobre la redacción del texto que constituye la política de seguridad de la información, se distinguirán dos tipos de actividades:

- Revisiones periódicas sistemáticas: Deberán realizarse al menos con una periodicidad anual, o cuando se detecten incidencias o cambios en el marco legal que puedan cuestionar la validez de dicha Política. La revisión de la Política de Seguridad de la Información deberá garantizar que ésta se encuentra alineada con la estrategia, la misión y visión de Circular Universe en materia de seguridad de la información y que asegura el cumplimiento de los objetivos de control establecidos.

- Revisiones no planificadas: Estas revisiones deberán realizarse en respuesta a cualquier evento o incidente de seguridad que pudiera suponer un incremento significativo del nivel de riesgo actual o haya causado un impacto en la seguridad de la información de Circular Universe.

5. Organización interna de la seguridad

La seguridad de la información corresponde, con las funciones que se señalan para cada uno en este apartado, a los siguientes órganos: Comité de Seguridad de la Información de Circular Universe, Comité de IT, Responsables de la Información, Responsables del Servicio, Responsables de Seguridad y, en caso de que sea pertinente, Responsables de Seguridad Delegados.

- Comité de Seguridad de la Información de Circular Universe.

  El Comité de Seguridad de la Información es el organismo que centraliza la gestión de la seguridad de la información en la organización.

  Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, podrán crearse Comités de Seguridad delegados, dependientes funcionalmente del Comité de Seguridad de la Información principal, que serán responsables en su ámbito de las actuaciones que se les deleguen.

- Comité de IT.

  El Comité de Innovación y Tecnología ("Comité IT") es el órgano encargado de la gestión de la seguridad de la información, coordinando la gestión de la seguridad de los activos de la información de la organización, y actuando como canal de comunicación directo entre el Comité de Seguridad y las áreas implicadas en las actividades de Circular Universe.

- Responsable de la Información será la persona con competencia suficiente para decidir sobre la finalidad, contenido y uso de dicha información y determinará los requisitos de seguridad de la información tratada dentro del marco establecido que regula ISO27001 y ENS.

  a) Determinará los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el marco que regula el ISO27001 y ENS.

  b) Realizará, junto a los Responsables del Servicio y del Responsable de Seguridad, los preceptivos análisis de riesgos, y seleccionarán las salvaguardas que se han de implantar.

  c) Aceptarán los riesgos residuales respecto de la información calculados en el análisis de riesgos.

  d) Realizarán el seguimiento y control de los riesgos, con la participación del Responsable de Seguridad

- El Responsable del Servicio será la persona con competencia suficiente para decidir sobre la finalidad y prestación de dicho servicio y determinará los requisitos de seguridad de los servicios prestados dentro del marco establecido que regula ISO27001 y ENS. A tal efecto:

  a) Realizará, junto a los Responsables de la Información y de Seguridad, los preceptivos análisis de riesgos, y seleccionarán las salvaguardas que se han de implantar.

  b) Aceptarán los riesgos residuales respecto de la información calculados en el análisis de riesgos.

  c) Realizarán el seguimiento y control de los riesgos, con la participación del Responsable de Seguridad.

d) Suspenderá, de acuerdo con el Responsable de la Información y el Responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

- El Responsable de Seguridad será la persona determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Tendrá las siguientes funciones:

    a) Asunción de las funciones incluidas dentro de los marcos que regulan ISO27001 y Esquema Nacional de Seguridad.

    b) Proponer al Responsable del Servicio la determinación de los niveles de seguridad en cada dimensión de seguridad siempre que se le solicite.

    c) Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

    d) Realizar el seguimiento y control del estado de seguridad de los sistemas de información.

    e) Proponer al Comité de Seguridad de la Información las normas y los procedimientos de seguridad.

    f) Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, podrán designarse «responsables de seguridad delegados», dependientes funcionalmente del responsable principal, que serán responsables en su ámbito de las actuaciones que se les deleguen.

6. Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la Información, éste será resuelto por la Dirección de Circular Universe, y prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

7. Clasificación de la información

Circular Universe clasificará e inventariará los activos de la información en virtud de su naturaleza. El nivel de protección y las medidas a aplicar se basarán en el resultado de dicha clasificación.

8. Datos de carácter personal

Cuando un sistema al que afecte ISO27001 y ENS maneje datos de carácter personal, le será de aplicación lo dispuesto en Reglamento Europeo 679/2016 de protección de datos y en la Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos de Carácter Personal y sus normas de desarrollo, sin perjuicio de los requisitos establecidos en el marco regulatorio de ISO27001 y ENS. Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal.

9. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las

contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- al menos una vez al año (mediante revisión y aprobación formal).
- 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, se establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

10. Instrumento de desarrollo

Se establece un marco normativo en materia de seguridad de la información estructurado por diferentes niveles de forma que los objetivos marcados por el presente documento tengan un desarrollo específico. La política de seguridad estructurará su marco normativo en los siguientes niveles:

1. La presente Política de Seguridad de la Información que establece los requisitos y criterios de protección de carácter global.

2. Las normas de seguridad que definen qué hay que proteger y los requisitos de seguridad deseados. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los sistemas de información de la organización. Establecen un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política. Las propone el Responsable de Seguridad y las aprueba el Comité de Seguridad.

3. Los procedimientos de seguridad en los que describirá de forma concreta cómo proteger lo definido en las normas y las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento. Son documentos que especifican cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

   Su aprobación dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado.

Además, se podrán establecer guías con recomendaciones y buenas prácticas.
En la medida de lo posible, toda esta documentación será gestionada según establece el procedimiento vigente de Control de documentos y registros en Circular Universe, que tendrá como objetivo establecer los criterios para el control de la documentación y registros de seguridad utilizados en el Sistema de Gestión de la Seguridad de la Información y que se extiende a toda la documentación que da soporte al cumplimiento de ISO27001 y ENS.

11. Obligaciones del personal

Todo el personal con responsabilidad en el uso, operación, o administración de sistemas de tecnologías de la información y las comunicaciones tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad derivada, independientemente del tipo de relación jurídica que les vincule con Circular Universe.

Todas las personas recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

La Política de Seguridad estará accesible para todo el personal que preste sus servicios en los órganos y entidades a que se refiere el punto relativo al 'Alcance'.

Con el objetivo de fomentar la 'Cultura de la seguridad', el Comité de Seguridad de la Información promoverá un programa de concienciación continúa para formar a todo el personal. El incumplimiento de la Política de Seguridad y su normativa de desarrollo dará lugar al establecimiento de medidas preventivas y correctivas encaminadas a salvaguardar y proteger las redes y sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria.

12. Relaciones con terceros

Cuando Circular Universe preste servicios o ceda información a terceras partes, se les hará partícipe de esta Política de Seguridad de la Información y de las normas e instrucciones derivadas.

Asimismo, cuando Circular Universe utilice servicios de terceros o ceda información a terceros se les hará igualmente partícipe de esta Política de Seguridad de la Información y de la normativa e instrucciones de seguridad que ataña a dichos servicios o información. Los terceros quedarán sujetos a las obligaciones y medidas de seguridad establecidas en dicha normativa e instrucciones, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de detección y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad de la información, al menos al mismo nivel que el establecido en esta Política de Seguridad de la Información.

En concreto, los terceros deberán garantizar el cumplimiento de la política de seguridad de la información basadas en estándares auditables que permitan verificar el cumplimiento de estas políticas. Asimismo, se garantizará mediante auditoría o certificado de destrucción/borrado que la tercera cancela y elimina los datos pertenecientes a Circular Universe a la finalización del contrato.

Cuando algún aspecto de la Política de la Seguridad de la Información no pueda ser satisfecho por una tercera parte, se requerirá un informe del Responsable de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el Responsable de la Información y de los Servicios afectados antes de seguir adelante.