DOCUMENTO DE POLITICA DE SEGURIDAD TIC EN "PARQUE CIENTÍFICO Y TECNOLÓGICO CARTUJA, S.A"

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
DOC SEG TIC PCT CARTUJA, S.A	0.00	Primera versión.	27/11/2019
DOC SEG TIC PCT CARTUJA, S.A	1.00	Se mejora el formato del documento. Se corrigen errores menores. Actualización del marco normativo. Se añaden otros principios y directrices. Se añade información de cargos, puestos y funcionamiento del Comité de Seguridad.	14/02/2020
DOC SEG TIC PCT CARTUJA, S.A	2.00	Actualización del marco normativo.	18/01/2024

1. INTRODUCCIÓN

"Parque Científico y Tecnológico Cartuja, S.A", en adelante, PCT CARTUJA, S.A, 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 los departamentos deben 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.

Los diferentes departamentos deben 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.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2. ALCANCE

Esta política se aplica a todos los sistemas TIC de PCT CARTUJA, S.A y a todos los miembros de la organización, sin excepciones.

3. MISIÓN

De acuerdo con la Guía de seguridad CCN-STIC-805, en la que se indica que en la política de seguridad TIC se hará referencia a la misión del organismo, le corresponde a PCT CARTUJA, S.A, fomentar la relación y generación de oportunidades de negocio y sinergias entre empresas y entidades del recinto, especialmente en temas relacionados con financiación empresarial y la generación de proyectos de I+D+i, favoreciendo el desarrollo, la capacidad competitiva y el progreso económico, cultural y social del entorno.

4. MARCO NORMATIVO

El marco normativo de las actividades del PCT CARTUJA en el ámbito de esta Política de Seguridad está integrado por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

5. PRINCIPIOS Y DIRECTRICES

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son la prevención, la detección, la respuesta y la recuperación, de manera que las amenazas existentes no se materialicen o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan.

5.1. 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.

5.2. 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 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 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.

5.3. 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).

5.4. 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.

5.5. OTROS PRINCIPIOS GENERALES:

- El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información del PCT CARTUJA deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas.
- La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el Esquema Nacional de Seguridad, así como las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

La gestión de la seguridad de la información va íntimamente ligada al establecimiento de una organización de seguridad, identificando las diferentes actividades y responsabilidades en materia de gestión de la seguridad y mediante su asignación formal a los agentes que correspondan, con arreglo al principio básico de función diferenciada recogido tanto en el ENS como en la política de seguridad TIC de la Junta de Andalucía.

Atendiendo a dicho principio, se creará un **Comité de Seguridad TIC,** que actuará como órgano no colegiado de dirección y seguimiento en materia de seguridad de los activos TIC de titularidad de PCT CARTUJA, S.A o cuya gestión tenga encomendada.

El Comité de Seguridad TIC estará compuesto por los siguientes miembros:

- Un presidente, que será la persona que ostente en cada momento la dirección general de la sociedad.
- Las vocalías, que serán dos, una por cada una de las personas que ostente en cada momento los puestos de Director/a Departamento de Innovación y Proyectos y, de Director/a Departamento Jurídico de la empresa.
- La secretaría la ostentará además la persona que ostente el cargo de Director/a Departamento Jurídico de la empresa.

La secretaría tendrá como funciones, convocar las reuniones del comité de seguridad; preparar los temas a tratar, aportando información puntual para la toma de decisiones y, levantar acta de cada reunión del mismo.

El Comité de Seguridad TIC tendrá las siguientes funciones:

a) Impulsar el cumplimiento de la política de seguridad TIC.

b) Definir, aprobar y realizar el seguimiento de los objetivos e iniciativas en materia de seguridad TIC. Además, le corresponde promover la mejora continua del sistema de gestión de la seguridad TIC.

c) Nombrar a la persona responsable de seguridad TIC y a la persona responsable del sistema.

d) Informar regularmente a la persona titular de la Consejería de Economía, Conocimiento, Empresas y Universidad del estado de la seguridad TIC de la sociedad.

e) Promover la formación y la concienciación de las medidas legales y organizativas relativas a la seguridad TIC entre el personal de PCT CARTUJA, S.A

f) Promover auditorías periódicas para verificar el correcto cumplimento de los procedimientos de seguridad.

g) Monitorizar los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto a ellos.

h) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto a ellos, velando, en particular, por la coordinación en la gestión de incidentes de seguridad TIC.

i) Priorizar las actuaciones en materia de seguridad TIC cuando los recursos sean limitados.

j) Velar para que la seguridad TIC se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en producción, procurando la creación y utilización de servicios horizontales que reduzcan duplicidades y permitan un funcionamiento homogéneo de todos los sistemas.

k) Resolver los conflictos de competencia que se puedan suscitar entre las diferentes personas responsables de la gestión de la seguridad TIC o elevar propuesta para resolverlos, en su caso.

l) Impulsar la determinación de los niveles de seguridad de la información tratada, en la que se valorarán los impactos que tendrían los incidentes que afectarán a la seguridad de la información, e impulsar los preceptivos análisis de riesgos, junto a las personas responsables de la información que correspondan, contando con el asesoramiento de la persona delegada de protección de datos.

m) Coordinar las medidas técnicas y organizativas establecidas en la normativa de protección de datos personales, de acuerdo con los correspondientes análisis de riesgos y, en su caso, las evaluaciones de impacto en la protección de datos, contando con el asesoramiento de la persona delegada de protección de datos.

El Comité de Seguridad TIC reportará al Consejo de Administración de PCT CARTUJA, S.A, al menos, cuando requiera autorización para la adopción de cualquier acuerdo que exceda del límite económico de poder del Director/a General de la sociedad, y se reunirá con carácter ordinario, al menos una vez cada 6 meses, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores, cuando lo decida la persona titular de la presidencia de oficio o, a propuesta de cualquiera de sus miembros y, siempre que se produzcan algunos de estos sucesos:

a) Incidencias graves de seguridad que afecten a cualquier sistema.
b) Surjan nuevas necesidades de seguridad que requieran la participación del Comité.

En caso de vacante, ausencia o enfermedad, la presidencia y las vocalías podrán ser sustituidas por la persona suplente que la titular designe mediante acto documentado que remitirá al Comité de Seguridad TIC. La persona titular de la secretaría podrá ser sustituida por el trabajador/a de la sociedad que designe la presidencia del Comité.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Según lo previsto en la Orden de 12 de julio de 2019, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería de Economía, Conocimiento, Empresas y Universidad y sus entidades adscritas, PCT CARTUJA, S.A deberá contar con, al menos, los siguientes agentes responsables:

- **Persona responsable de la información.**
- **Persona responsable del servicio.**
- **Persona responsable de la seguridad TIC**
- **Persona delegada de la protección de datos.**
- **Persona responsable del sistema.**

A continuación, y en base a lo previsto en la guía CCN-STIC 801 se concretan las funciones y responsabilidades del Responsable de la Información, de la persona Responsable de Sistemas, y su relación con el Comité de Seguridad TIC. Debido a la estructura de la sociedad, las funciones del **responsable de la información y del responsable del servicio** podrán recaer sobre una misma persona, unidad o departamento.

- **Funciones de la persona Responsable de la Información.**

Es quien tiene la información y determina sus niveles de seguridad dentro del marco establecido en el Anexo I del Real Decreto 3/2010, de 8 de enero.

No puede coincidir con la persona responsable de la Seguridad TIC.

Los deberes y responsabilidades principales de este perfil de responsabilidad, sin perjuicio de otras previstas en el ENS y en la guía CCN-STIC 801, son las que se determinan a continuación:

a) Ayudar a determinar los requisitos de seguridad de la información, identificando los niveles de seguridad de dicha información, mediante la valoración del impacto sobres esta de los incidentes que pudieran producirse.

b) Con ayuda de la persona responsable del sistema, proporcionar la información necesaria para la realización de los análisis de riesgos, con la finalidad de establecer salvaguardas a implantar.

c) En relación con los análisis de riesgos de los sistemas de información, aceptar los riesgos residuales de las informaciones manejadas que sean de su competencia.

Será responsable de la Información en PCT CARTUJA, S.A la persona que ostente el puesto de la dirección general de la sociedad.

- **Funciones de la persona Responsable del Servicio.**

En lo relativo al ENS, es la persona que determinará los niveles de seguridad de los servicios dentro del marco establecido en el Anexo I del Real Decreto 3/2010, del 8 de enero. Los deberes y responsabilidades principales de este perfil de responsabilidad, dentro de su ámbito de actuación y sin perjuicio de otras previstas en el ENS y la guía CCN-STIC-801, son los siguientes:

a) Ayudar a determinar los requisitos de seguridad de los servicios a prestar, identificando los niveles de seguridad de los mismos mediante la valoración del impacto sobre éstos de los incidentes que pudieran producirse.

b) En el ámbito de cada servicio, proporcionar la información necesaria para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello, contará con la ayuda de la persona responsable del sistema.

La figura de responsable del Servicio corresponderá a la persona titular del puesto de la dirección general de la sociedad.

- **Funciones de la persona Responsable de la Seguridad TIC.**

La persona responsable de seguridad TIC será la encargada de velar por la armonización de la seguridad de la información y tendrá las siguientes funciones y responsabilidades:

a) Elaborará la normativa de seguridad que se presentará al Comité de Seguridad TIC para su aprobación.

b) Será responsable de:

1.) Conocer los cambios tecnológicos que puedan afectar a los sistemas de información, pudiendo tener consecuencias para la organización. En este caso deberá alertar al Comité de Seguridad TIC y proponer las medidas oportunas.

2.) La correcta ejecución de las instrucciones emanadas del Comité de Seguridad TIC, transmitiendo dichas instrucciones directamente o a través de la Unidad de Seguridad TIC.

3.) La presentación regular de informes sobre el estado de seguridad de los servicios TIC al Comité de Seguridad TIC.

4.) La preparación de informes en caso de incidentes excepcionalmente graves y en caso de desastres.

5.) La elaboración del Análisis de Riesgos de los sistemas, análisis que será presentado al Comité de Seguridad TIC para su aprobación. Este análisis deberá actualizarse regularmente dependiendo de la criticidad del sistema.

6.) La inspección de las verificaciones regulares de seguridad aprobadas por el Comité. El resultado de estas inspecciones se presentará al Comité de Seguridad TIC para su conocimiento y aprobación. Si como resultado de la inspección aparecen incumplimientos, propondrá medidas correctoras que presentará al Comité de Seguridad TIC para su aprobación, responsabilizándose de que sean llevadas a cabo.

7.) La elaboración y seguimiento del Plan de Seguridad que será presentado al Comité de Seguridad TIC para su aprobación.

c) Determinará, para su aprobación por el Comité de Seguridad TIC, los requisitos de formación y calificación de las personas con perfiles de personas administradoras, operadoras y usuarias desde el punto de vista de la seguridad de las TIC.

La persona responsable de la Seguridad TIC, en el caso de que no forme parte del Comité de Seguridad de la sociedad como vocal o ejerciendo la secretaría, asistirá en calidad de persona asesora.

Aunque las actividades de esta persona son delegables en una organización externa, la responsabilidad última la tendrá siempre la persona física responsable de seguridad TIC de la sociedad. A estos efectos, será responsable de la Seguridad TIC en PCT CARTUJA, S.A, la persona que ostente el puesto de la dirección del Departamento de Innovación y Proyectos de la sociedad.

- **Funciones de la persona Responsable del Sistema.**

La persona responsable del sistema tendrá las siguientes atribuciones:

a) Gestionar el sistema durante todo su ciclo de vida, desde la especificación, la instalación, hasta el seguimiento de su funcionamiento.

b) Definir los criterios de uso y los servicios disponibles en el sistema.

c) Elaborar los procedimientos operativos de seguridad para su aprobación por la persona responsable de seguridad TIC.

d) Determinar la configuración autorizada de hardware y software a utilizar en el sistema y aprobar las modificaciones importantes de dicha configuración.

e) Implantar y controlar las medidas específicas de seguridad del sistema.

f) Elaborar, junto con la persona responsable de seguridad TIC, los planes de mejora continua de la seguridad que deberá aprobar el Comité de Seguridad TIC.

g) Elaborar planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

h) Suspender el manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con las personas responsables de la información afectada, del servicio afectado y la persona responsable de seguridad TIC, antes de ser ejecutada.

Será responsable del Sistema en PCT CARTUJA, S.A la persona que ostente el puesto de la dirección general de la sociedad.

- **Persona delegada de la protección de datos.**

La persona delegada de protección de datos asesorará y supervisará la elaboración y mantenimiento del registro de actividades de tratamiento a que se refiere el artículo 30 del RGPD, y entregará un listado actualizado del citado registro al Comité de Seguridad TIC en cada una de sus reuniones, con indicación expresa de las personas u órganos que asumen las figuras de responsable del tratamiento, encargada del tratamiento, así como de las deficiencias que en su caso se produzcan, de modo que el Comité disponga de la información completa y pueda arbitrar los mecanismos necesarios para la subsanación de aquellas.

El Delegado de Protección de Datos puede ser una persona interna o externa a la organización.

La dirección general de PCT CARTUJA, S.A deberá nombrar una persona delegada de protección de datos que se comunicará a la Agencia Española de Protección de Datos y al Comité de Seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad. La persona delegada de protección de datos, que deberá estar en posesión de una titulación superior, será designada atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de Derecho y la práctica en materia de protección de datos, de conformidad con el artículo 35 de la Ley Orgánica 3/2018, de 5 de diciembre.

Son funciones de la persona que ostente la condición de delegada de protección de datos, además de las que le corresponden de conformidad con el artículo 39 del Reglamento General de Protección de Datos, artículos 36 y 37 de la Ley Orgánica 3/2018, de 5 de diciembre, y demás normativa de aplicación, las siguientes:

a) El asesoramiento y la supervisión:

1.) De los principios relativos al tratamiento de datos, como la limitación de finalidad, minimización o exactitud de los datos.

2.) En la identificación de las bases jurídicas de los tratamientos de datos.

3.) Del diseño e implantación de medidas de información a los afectados por los tratamientos de datos, así como el asesoramiento en la confección de modelos de formularios de recogida de datos personales.

4.) Para el establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de las personas interesadas.

5.) De la valoración de las solicitudes de ejercicio de derechos por parte de las personas interesadas.

6.) En la contratación de las personas encargadas del tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-persona encargada.

7.) En la identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.

8.) Del diseño e implantación de políticas de protección de datos.

9.) De la auditoría de protección de datos.

10.) En el establecimiento y gestión de los registros de actividades de tratamiento.

11.) Del análisis de riesgo de los tratamientos realizados.

12.) De la implantación de las medidas de protección de datos desde el diseño y la protección de datos por defecto adecuadas a los riesgos y a la naturaleza de los tratamientos.

13.) De la implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.

14.) En el establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de las personas afectadas y los procedimientos de notificación a las autoridades de supervisión y a esas personas.

15.) Sobre la determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.

16.) En la realización de evaluaciones de impacto sobre la protección de datos.

17.) En la implantación de programas de formación y sensibilización del personal en materia de protección de datos.

b) La valoración de la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.

c) El asesoramiento sobre la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específico, distintas de las establecidas por la normativa general de protección de datos.

La persona delegada de protección de datos, en el caso de que no forme parte del Comité de Seguridad TIC de la sociedad como vocal o ejerciendo la secretaría, asistirá en calidad de persona asesora.

La figura de la persona Delegada de Protección de Datos de la sociedad, la ostenta actualmente la persona responsable del Departamento de Asesoría Jurídica de PCT CARTUJA, S.A

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

Los nombramientos de los responsables del Servicio, de la Información y del Sistema, así como del Responsable de la Seguridad TIC y del Delegado de Protección de Datos se revisarán cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el director general de la sociedad, y difundida para que la conozcan todas las partes afectadas.

7. ASESORAMIENTO ESPECIALIZADO EN MATERIA DE SEGURIDAD

7.1. ASESORAMIENTO ESPECIALIZADO.

El Responsable de la Seguridad será el encargado de coordinar los conocimientos y las experiencias disponibles en el PCT CARTUJA con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos.

7.2. COOPERACIÓN ENTRE ORGANISMOS Y OTRAS ADMINISTRACIONES PÚBLICAS.

A efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de seguridad, el PCT CARTUJA mantendrá contactos periódicos con organismos y entidades especializadas en temas de seguridad.

7.3. REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN.

El Responsable de la Seguridad propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la Política de Seguridad con el fin de garantizar que las prácticas en el PCT CARTUJA reflejan adecuadamente sus disposiciones.

8. DATOS DE CARÁCTER PERSONAL

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo establecido en el 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como lo establecido en la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales.

9. FORMACIÓN Y CONCIENCIACIÓN

Periódicamente se realizarán acciones de formación y concienciación en materia de seguridad.

El objetivo de las acciones formativas y de concienciación es doble:

- mantener informado al personal más directamente relacionado con el manejo de información y los sistemas que la tratan sobre los procedimientos existentes de seguridad, riesgos, medidas de protección, planes de protección, etc.

- concienciar al personal, en general, de la importancia de la seguridad y de los procedimientos básicos de manejo e intercambio de información.

El primer objetivo se asocia a Formación y el segundo a Concienciación.

El Responsable de la Seguridad determinará el formato de las acciones de Formación y Concienciación, así como sus contenidos.

10. GESTIÓN DE RIESGOS

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

- 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 TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

11. RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de la Seguridad.

12. OBLIGACIONES DEL PERSONAL

Todos los trabajadores de PCT CARTUJA, S.A 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 TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los trabajadores de PCT CARTUJA, S.A atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de PCT CARTUJA, S.A, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será 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.

13. TERCERAS PARTES

Cuando PCT CARTUJA, S.A preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando PCT CARTUJA, S.A utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará 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 requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

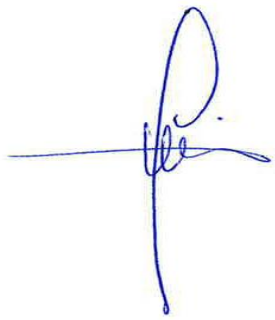
14. APROBACIÓN Y ENTRADA EN VIGOR

La presente Política de Seguridad de la Información fue aprobada el **27 de noviembre de 2019** por el director general de la sociedad y modificada el 14 de febrero de 2020 y el 18 de enero de 2023.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y será revisada, al menos, cada dos años.

15. PUBLICACIÓN DE LA POLÍTICA DE SEGURIDAD

La presente Política será publicada en la página web del PCT CARTUJA (https://www.pctcartuja.es/).



_____

Fdo. Luis Pérez Díaz.
Director General "Parque Científico y Tecnológico Cartuja, S.A"