RESOLUCIÓN DE LA DIRECCIÓN GERENCIA POR LA QUE SE APRUEBA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN EL CONSORCIO PARQUE DE LAS CIENCIAS

I. EXPOSICIÓN DE MOTIVOS

El Consorcio Parque de las Ciencias de Granada se configura como el primer centro interactivo de ciencia y museo en el ámbito de la Comunidad Autónoma de Andalucía, cuyos principales objetivos son promover la divulgación de la ciencia; fomentar la cultura científica, tecnológica, sanitaria y ambiental; potenciar el desarrollo de la didáctica de la ciencia; mantener un permanente intercambio con centros homólogos; contribuir a la formación del alumnado, del profesorado y de otros profesionales de los centros docentes y a la formación integral y continuada de la ciudadanía en el ámbito de la ciencia; promover la actividad socioeconómica y la innovación en su entorno, así como el turismo científico.

En el contexto actual, el Consorcio depende de los sistemas de Tecnologías de la Información y Comunicaciones (TIC) para la consecución de estos objetivos estatutarios y la prestación de un servicio público de calidad. Estos sistemas deben ser administrados con la máxima diligencia, adoptando las medidas necesarias para protegerlos frente a daños accidentales o deliberados que puedan comprometer la disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad de la información tratada. La confianza de la ciudadanía, los visitantes y los colaboradores en los servicios digitales del Parque constituye un activo estratégico que debe ser preservado.

La seguridad de la información no puede entenderse como una acción puntual, sino como un proceso integral que abarca desde la concepción de los servicios hasta su retirada, exigiendo una estrategia capaz de prevenir, detectar y responder eficazmente ante incidentes de seguridad. La rápida evolución de las amenazas tecnológicas requiere que la entidad disponga de un marco normativo interno que garantice la resiliencia de los sistemas y la continuidad de las actividades de divulgación y gestión administrativa frente a cualquier contingencia.

Asimismo, el marco jurídico vigente, encabezado por el Real Decreto 311/2022, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), así como el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos, imponen al Consorcio la obligación de contar con una Política de Seguridad aprobada formalmente. Este documento de primer nivel sienta las bases organizativas, define roles y responsabilidades, y establece los principios de gestión de riesgos necesarios para asegurar el cumplimiento normativo.

De acuerdo con lo previsto en la letra w) del artículo 26 de los Estatutos del Consorcio -BOJA núm. 215, de 7 de noviembre de 2018- corresponde a la Dirección Gerencia adoptar en caso de urgencia, siempre que no puedan reunirse previamente los órganos colegiados de la entidad, las medidas adecuadas al caso que sean necesarias, dando cuenta inmediatamente de ello a los órganos de gobierno en la primera reunión que celebren.

En este caso, la circunstancia de la urgencia deriva de la inexistencia de esta política, resultando imprescindible que el Consorcio se dote de este instrumento para una mejor gestión.

Por todo ello, con el objetivo de dotar a la entidad de un marco de seguridad robusto, sistematizar la protección de los activos de información y dar cumplimiento a los requisitos legales del Sector Público, a propuesta del Comité de Seguridad Integral de la entidad adoptada en su reunión del día 13 de enero de 2026 y en uso de las facultades estatutariamente atribuidas, esta Dirección Gerencia

HA RESUELTO:

II. PARTE DISPOSITIVA

Primero. Aprobación de la Política de Seguridad. Se aprueba la Política de Seguridad de la Información del Consorcio Parque de las Ciencias, cuyo texto íntegro figura como Anexo I a la presente Resolución. Dicha Política constituye el documento de máximo nivel en la estructura documental de seguridad de la entidad.

Segundo. Ámbito de Aplicación. La Política de Seguridad será de obligado cumplimiento para todo el personal del Consorcio (funcionario, laboral o estatutario), así como para proveedores, colaboradores externos, becarios y cualquier tercero que acceda a los sistemas de información, servicios, redes o instalaciones físicas de la entidad. Abarca todos los activos, incluyendo equipos informáticos, bases de datos y documentación en cualquier soporte.

Tercero. Organización y Responsabilidades. La estructura organizativa de la seguridad reside en el Comité de Seguridad Integral (CSI), cuya composición y funciones se rigen por su acuerdo de creación. Se designan como roles clave para la gestión de la seguridad a las figuras detalladas en el apartado "Procedimiento de Designación" de la Política adjunta.

Cuarto. Revisión y Actualización. El Comité de Seguridad Integral revisará anualmente la Política de Seguridad de la Información para asegurar su adecuación a la evolución de los

riesgos y la normativa, proponiendo a esta Dirección Gerencia su mantenimiento o modificación según proceda.

Quinto. Difusión y Publicidad. La presente Política se publicará en el Portal de Transparencia y se pondrá a disposición de todos los miembros de la organización. Es responsabilidad del Comité de Seguridad Integral disponer los medios necesarios para que su contenido sea conocido por todas las partes afectadas.

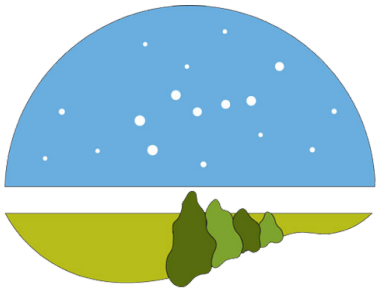
Sexto. Entrada en Vigor. La Política de Seguridad que se aprueba entrará en vigor el día siguiente al de su firma y mantendrá su vigencia hasta su derogación expresa o sustitución por una nueva versión.

Séptimo. Dar cuenta de esta Resolución al Consejo Rector de la entidad en la próxima reunión que celebre.

Granada, a fecha de la firma electrónica.

Alfonso Peres Osia
Director Gerente

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



PARQUE de las CIENCIAS

ANDALUCÍA - GRANADA

Consorcio Parque de las Ciencias
Avd. del Mediterráneo s/n. 18006 Granada. España
Telf: 958 131 900 - info@parqueciencias.com
www.parqueciencias.com

JUNTA DE ANDALUCÍA
AYUNTAMIENTO DE GRANADA
DIPUTACIÓN PROVINCIAL DE GRANADA
UNIVERSIDAD DE GRANADA
CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS

ÍNDICE

CONTROL DE REVISIONES

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	ELABORADO	REVISADO	APROBADO
1.0	Primera versión del documento	20/12/2025		
2.0	Segunda Versión del documento	28/01/2025		

1 APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información es efectiva desde su entrada en vigor y hasta que sea reemplazada por una nueva Política.

2 INTRODUCCIÓN

El Consorcio PARQUE DE LAS CIENCIAS DE GRANADA, en adelante CPC, 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, confidencialidad, autenticidad o trazabilidad 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 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.

El CPC 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.

El CPC debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

2.1 Prevención

El CPC 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 implementará 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, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, se 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

PARQUE DE LAS CIENCIAS DE GRANADA:

- Establecerá mecanismos para responder eficazmente a los incidentes de seguridad.
- Designará un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecerá 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 Recuperación

Para garantizar la disponibilidad de los servicios críticos, el CPC dispondrá de planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

3 PRINCIPIOS BÁSICOS

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información.

Se establecen los siguientes:

- **Alcance estratégico:** La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos del CPC, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.
- **Responsabilidad determinada**: En los sistemas TIC se identificará el Responsable de la Información, que determina los requisitos de seguridad de la información tratada; el Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios y el Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- **Seguridad integral:** La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- **Gestión de Riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

- **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
- **Seguridad por defecto:** Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad adaptada a la política de seguridad del CPC y al ENS.

4 ALCANCE

La presente Política de Seguridad es de aplicación a todos los sistemas de información, servicios, redes, equipos físicos e instalaciones propiedad del CONSORCIO PARQUE DE LAS CIENCIAS o bajo su responsabilidad, que den soporte a las funciones de divulgación científica, gestión educativa, administración y venta de entradas.

Específicamente, este alcance vincula a:

- Personas: Todo el personal del Consorcio (funcionario, laboral o estatutario), así como proveedores, colaboradores externos, becarios y cualquier tercero con acceso a la información o instalaciones de la entidad.
- Activos: Todos los equipos informáticos (servidores, puestos de trabajo, dispositivos móviles), software, bases de datos y documentación en cualquier soporte (papel o digital).
- Ubicaciones: Las instalaciones físicas del CPC, incluyendo las áreas de oficinas, CPD, exposiciones, taquillas y el BioDomo.

El cumplimiento de esta política es obligatorio para todos los sujetos mencionados anteriormente.

5 MISIÓN

La misión de la Seguridad de la Información del CPC es garantizar el desarrollo seguro y continuo de sus actividades de divulgación científica, educación y gestión administrativa, protegiendo los servicios prestados y la información gestionada frente a amenazas internas y externas, ya sean accidentales o deliberadas.

Esta estrategia de protección tiene como fines fundamentales:

- Asegurar la confianza de la ciudadanía, visitantes y colaboradores en los sistemas digitales del Consorcio.
- Garantizar el cumplimiento del marco legal vigente, con especial atención al Esquema Nacional de Seguridad (ENS) y la normativa de Protección de Datos.
- Preservar los activos esenciales (integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad) necesarios para el cumplimiento de los fines estatutarios de la entidad.

6 MARCO NORMATIVO

Según la legislación vigente, las leyes aplicables CPC en materia de Seguridad de la Información son:

- Real Decreto 311/2022, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS).
- 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.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.
- Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad TIC de la Junta de Andalucía.

7 ORGANIZACIÓN DE LA SEGURIDAD

La estructura organizativa de la seguridad del CPC reside en el Comité de Seguridad Integral (CSI).

La composición, funcionamiento, régimen de convocatorias y funciones de gobierno de dicho Comité se rigen por lo establecido en el 'Acuerdo de Creación del Comité de Seguridad Integral y su Reglamento de Funcionamiento', aprobado por el Consejo Rector el 15 de diciembre de 2025.

Dicho reglamento se considera parte integrante del marco normativo de seguridad de la entidad.

8 PROCEDIMIENTO DE DESIGNACIÓN

Se designan las siguientes responsabilidades:

- **Responsable del Servicio:** Responsable de Seguridad de la Información del Comité de Seguridad Integral.
- **Responsable de la Información:** Responsable de Seguridad de la Información del Comité de Seguridad Integral.
- **Responsable de Seguridad:** Responsable de Seguridad de la Información del Comité de Seguridad Integral.
- **Delegado de Protección de Datos:** Responsable de Asuntos Jurídicos y Delegado de Protección de Datos del Comité de Seguridad Integral
- **Responsable del Sistema:** Responsable de Informática de Sistemas del Comité de Seguridad Integral.

Los nombramientos se revisarán según lo establecido en la normativa del Comité de Seguridad Integral.

9 REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad Integral 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 la Dirección-Gerencia y publicada en el portal de transparencia para que la conozcan todas las partes afectadas.

10 REQUISITOS MÍNIMOS DE SEGURIDAD

A continuación, se enuncian los principios básicos relacionados con la seguridad de la información, que rigen la política de seguridad de la información de la organización.

a) Organización e implantación del proceso de seguridad. Se desarrolla en el punto 6 de la presente política.
b) Análisis y gestión de los riesgos. Se desarrolla en el apartado gestión de riesgos.
c) Gestión de personal. Se desarrolla en el apartado Obligaciones del Personal.
d) Profesionalidad. Se desarrolla en el apartado Obligaciones de personal

e) Autorización y control de los accesos. El acceso del sistema de información debe ser controlado y limitado. En el apartado control de accesos, se definen unas líneas básicas en la materia.
f) Protección de las instalaciones. Se desarrolla en el apartado Seguridad Física y del entorno.
g) Adquisición de productos. Se desarrolla en el apartado terceras partes.
h) Integridad y actualización del sistema. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.
i) Protección de la información almacenada y en tránsito. La protección de la información almacenada se desarrolla en el apartado Protección de información almacenada.
j) Prevención ante otros sistemas de información interconectados. Se desarrolla en el apartado Gestión de comunicaciones y operaciones.
k) Registro de actividad. Se desarrolla en el apartado Seguimiento y monitorización.
l) Incidentes de seguridad. Se desarrolla en el apartado Gestión de incidencias de seguridad.
m) Mínimo privilegio. Se desarrolla en el apartado Gestión de la configuración.
n) Continuidad de la actividad. Se desarrolla en el apartado Gestión de la continuidad del servicio.
o) Mejora continua del proceso de seguridad. Tal como se especifica en esta política, el comité de seguridad integral promoverá la mejora continua, de forma que se planifiquen y realicen objetivos y acciones de mejora (Apartado Organización de la Seguridad).

Estos requisitos mínimos de seguridad podrán ser ampliados por normativas superiores, así como los procedimientos que se pudieran establecer en el Esquema Nacional de Seguridad para el CPC.

11 DATOS DE CARÁCTER PERSONAL

El CPC trata datos de carácter personal.

Todos los sistemas de información del CPC se ajustarán a los niveles de seguridad requeridos por la normativa vigente en materia de Protección de Datos de Carácter Personal, identificada en el apartado 6. Marco Normativo, de la presente Política de Seguridad de la Información.

12 GESTIÓN DE RIESGOS

Para todos los sistemas sujetos a esta Política de Seguridad de la Información debe realizarse periódicamente una evaluación de los a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información gestionada
- 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 Integral establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados. El Comité de Seguridad Integral dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

13 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta política de seguridad de la Información complementa las políticas de seguridad del CPC en materia de protección de datos de carácter personal.

Esta Política de Seguridad de la Información se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará 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.

14 GESTIÓN DE LA CONTINUIDAD DEL SERVICIO

Es imprescindible para el CPC establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades del negocio por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad del negocio en estos casos, el CPC establecerá planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del servicio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La gestión de la continuidad del servicio se incorporará a los procesos del CPC y será responsabilidad de una o varias personas dentro de la empresa.

15 SEGURIDAD FÍSICA Y DEL ENTORNO

Para que una seguridad lógica sea efectiva, es primordial que las instalaciones mantengan una correcta seguridad física para evitar los accesos no autorizados, así como cualquier otro tipo de daño o interferencia externa.

El CPC cuenta con un Plan de Seguridad Interior que desarrolla todos los aspectos relacionados con la seguridad física y del entorno.

16 OBLIGACIONES DEL PERSONAL

Todos y cada uno de los usuarios de los sistemas de información CPC son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros CPC 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 Integral disponer los medios necesarios para que la información llegue a los afectados.

Los miembros del CPC recibirán formación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros CPC, 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.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

17 GESTIÓN DE COMUNICACIONES Y OPERACIONES

El CPC controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red CPC y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red existirán mecanismos para limitar los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los empleados autorizados para el manejo de información automatizada deberán estar registrados como usuarios del dominio. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal. Esta contraseña caducará periódicamente.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo a estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

En algunos casos será necesario que distintas áreas estén lógicamente separadas del resto para evitar accesos no autorizados.

18 SEGUIMIENTO Y MONITORIZACIÓN

Se definirá una estrategia global de monitorización de sistemas y actividades, identificando los sistemas más críticos y estableciendo los controles oportunos para registrar cualquier evento que debe ser detectado (actividades no autorizadas o funcionamientos inadecuados de sistemas). Los registros deberán ser almacenados convenientemente protegidos contra su modificación o eliminación.

Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades de proceso de información no autorizadas. Esto implicará realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos así como para recomendar cualquier cambio que se estime necesario.

19 CONTROL DE ACCESOS

La información debe estar protegida contra accesos no autorizados. El Comité de Seguridad Integral definirá las necesidades de acceso a la información a dos niveles, para el conjunto de áreas y las de cada usuario dentro del conjunto. Sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.

Cada usuario deberá estar asociado a un perfil, de acuerdo a las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá de unos determinados permisos y verá restringido su acceso a información y sistemas que no le son necesarios para las competencias de su trabajo.

No se permitirá el acceso a la red, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.

En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con el CPC para mantener el mismo nivel de seguridad que si fueran empleados de la propia organización.

Cuando los equipos o la información propiedad CPC están fuera de las instalaciones, es el empleado que los está utilizando el que debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento.

20 GESTIÓN DE LA CONFIGURACIÓN

La gestión, configuración y actualización del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información se realizará siempre siguiendo los principios de seguridad por defecto y mínimo privilegio.

21 GESTIÓN DE INCIDENTES

Cualquier empleado que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Responsable de Seguridad para que tome las medidas oportunas y registre la incidencia.

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.

22 PROTECCIÓN DE INFORMACIÓN ALMACENADA

El CPC implantará medidas físicas y lógicas para proteger la información allí donde se encuentre almacenada, tanto si se encuentra en un soporte físico o digital. Se realizarán copias de seguridad que aseguren la posibilidad de recuperación en caso de incidente.

23 TERCERAS PARTES

Las empresas y organizaciones externas que con ocasión de su colaboración con el CPC para la prestación de un servicio, accedan o gestionen activos de información CPC o de sus usuarios, directa o indirectamente (en sistemas propios o ajenos), comparten la responsabilidad de mantener la seguridad de los sistemas y activos del CPC, por lo que deberán asumir las siguientes obligaciones:

- No difundir ninguna información relativa a los servicios proporcionados al CPC sin autorización expresa para ello.
- Informar y difundir a su personal las obligaciones establecidas en esta Política.

- Aplicar las medidas estipuladas por RGPD en el tratamiento de los datos personales responsabilidad CPC que traten por razón de la prestación del servicio.
- Aplicar los procedimientos para la gestión de seguridad relacionados con los servicios proporcionados CPC. Especialmente se deben aplicar los procedimientos relacionados con la gestión de usuarios, tales como notificaciones de altas y bajas, identificación de los usuarios, gestión de contraseñas, etc., en el sentido descrito en la presente política y normativa reguladora que sea de aplicación.
- Notificar cualquier incidencia o sospecha de amenaza a la seguridad de algún sistema o activo CPC a través de los mecanismos que se determinen, colaborando en la resolución de las mismas relacionados con los sistemas, servicios o personal de la propia entidad.
- Implantar medidas en sus propios sistemas y redes para prevenir la difusión de virus y/o código malicioso a los sistemas del CPC. Específicamente, cualquier equipo conectado a la red corporativa del CPC debe disponer de un antivirus actualizado preferiblemente de forma automática.
- Implantar medidas en sus propios sistemas y redes para prevenir el acceso no autorizado a los sistemas del CPC desde otras redes. Entre otros, se deben aplicar las actualizaciones de seguridad en sus sistemas y se debe mantener un sistema cortafuegos para proteger las conexiones desde Internet y otras redes no confiables.

El CPC se reserva el derecho de revisar la relación con la entidad externa en caso de incumplimiento de las anteriores obligaciones.

24 ESTRUCTURA DE LA DOCUMENTACIÓN DE SEGURIDAD

Todos los documentos que componen la documentación del Sistema de Gestión de Seguridad de la Información se gestionarán de acuerdo a lo descrito en los procedimientos del Esquema Nacional de Seguridad.

Se ha establecido un marco normativo en materia de seguridad de la información estructurado en diferentes niveles, de forma que los principios y los objetivos marcados en la política de seguridad de la institución tengan un desarrollo específico:

- **Primer nivel:** la presente Política de Seguridad de la Información, que debe ser aprobada por la Dirección-Gerencia a propuesta del Comité de Seguridad Integral.
- **Segundo nivel:** la normativa de seguridad de la información aprobada por el Comité de Seguridad Integral en desarrollo de la Política de Seguridad de la Información. En

ella se establecerán unas normas de uso aceptable de los sistemas de información Esta normativa será aprobada por el Comité de Seguridad Integral.

- **Tercer nivel:** los procedimientos de seguridad de la información, en los que se detallará la manera correcta de realizar determinados procesos de modo que se proteja en todo momento la seguridad y la información. Estos procedimientos han de ser aprobados por el Comité de Seguridad Integral.