——— ACUERDO DE LA MESA DE LA ASAMBLEA, SOBRE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA ASAMBLEA DE MADRID ———

La Mesa de la Asamblea, en sesión celebrada el día 25 de abril de 2024, en virtud de lo establecido en el artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en los artículos 48 y 49 del Reglamento de la Asamblea, acuerda aprobar la Política de Seguridad de la Información de la Asamblea de Madrid, ordenado su publicación en el Boletín Oficial de la Asamblea de Madrid.

Sede de la Asamblea, 25 de abril de 2024.
El Presidente de la Asamblea
ENRIQUE MATÍAS OSSORIO CRESPO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA ASAMBLEA DE MADRID

EXPOSICIÓN DE MOTIVOS

En virtud de lo dispuesto en los artículos 48 y 49 del Reglamento de la Asamblea de Madrid, corresponde a la Mesa, como órgano rector de la Asamblea, adoptar cuantas decisiones y medidas requiera la organización del trabajo y el régimen y gobierno interior de la Cámara.

La adopción de los principios generales y el establecimiento de la estructura organizativa que permitan garantizar la seguridad en la utilización de los medios electrónicos, configuran el núcleo de la Política de Seguridad de la Información de la Asamblea de Madrid, cuya finalidad es asegurar el acceso, disponibilidad, integridad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios, frente a los riesgos y amenazas que pueden comprometer el funcionamiento de la institución y su imagen derivados de incidentes relacionados con la seguridad de las redes y la información.

El contenido de la Política de Seguridad de la Información de la Asamblea de Madrid se ha adaptado a los requisitos mínimos establecidos con carácter general para las Administraciones Públicas y, en especial, a lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, cuyo objetivo es crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas que permitan garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, permitiendo el ejercicio de derechos y el cumplimiento de deberes a los ciudadanos y a las Administraciones Públicas.

Artículo 1. *Objeto y ámbito de aplicación.*

1. La presente Política establece las directrices que rigen la forma en que la Asamblea de Madrid gestiona y protege la información y los servicios que considera críticos.

2. La seguridad se entenderá como un proceso integral constituido por todos los elementos personales, técnicos, materiales y organizativos, relacionados con el sistema informático. Por ello, esta Política regula directamente la actividad de la Asamblea de Madrid y el uso del equipamiento hardware y software que la Asamblea facilita a los usuarios de su sistema informático, incluido, en su caso, cualquier tipo de dispositivo portátil, de telefonía o de comunicaciones. Afecta también a la actividad de terceros en su relación con esta.

3. A los efectos de esta Política de seguridad, el sistema informático de la Asamblea de Madrid comprende todo el hardware y/o software de:

a) Los dispositivos utilizados para procesar la información de la institución.

b) Los sistemas de almacenamiento de dicha información.

c) La red corporativa que interconecta los diversos dispositivos y sistemas.

d) Los sistemas de acceso a redes externas como internet.

e) Los sistemas de comunicaciones y telefonía.

f) Los sistemas de protección frente a intrusiones, virus o spam.

g) Los sistemas de respaldo y copia de seguridad.

h) Cualesquiera otros dispositivos o sistemas gestionados por la Asamblea de Madrid y relacionados con el tratamiento automatizado de la información de la institución.

4. Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos, para lo cual se elaborará una Política de gestión de documentos electrónicos.

Artículo 2. *Sistemas de información que traten datos personales.*

Todos los sistemas de información de la Asamblea de Madrid se ajustarán, en el tratamiento de datos de carácter personal, a los niveles de seguridad requeridos por la normativa vigente.

Artículo 3. *La seguridad como un proceso integral.*

1. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema.

2. La preservación de la seguridad de la información compete a todos los usuarios internos del sistema informático de la Asamblea de Madrid, siendo estos responsables del uso correcto de los dispositivos y servicios puestos a su disposición. La organización del mantenimiento y gestión de la seguridad de los datos y sistemas de información de la Asamblea de Madrid se realiza mediante la identificación y definición de las diferentes actividades y responsabilidades.

3. Todos los usuarios del sistema informático de la Asamblea de Madrid deben estar comprometidos con la seguridad, deben conocer la presente Política y el Manual de procedimientos, y ejercitarán y aplicarán los principios de seguridad en el desempeño de su cometido. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos para que ni el desconocimiento, ni la falta de organización y coordinación, ni instrucciones inadecuadas sean fuentes de riesgo para la seguridad.

4. Cada usuario tratará con el debido celo profesional la información que maneja, observará el deber de sigilo y será especialmente cauto tanto en las modificaciones que afecten a la integridad de la

información como en cualquier proceso que pueda dar lugar a su publicación, en especial en lo que se refiere a datos de carácter personal.

Artículo 4. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado. El análisis se repetirá regularmente, al menos:

a) Cuando cambie la información manejada.

b) Cuando cambien los servicios prestados.

c) Cuando ocurra un incidente grave de seguridad.

d) Cuando se constaten vulnerabilidades graves.

2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos mediante la adopción de medidas de seguridad proporcionadas, adaptadas a la naturaleza de los datos y los tratamientos y al tipo de exposición.

3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas.

Artículo 5. *Prevención, detección, respuesta y conservación.*

1. Las medidas de prevención deben eliminar o, al menos, reducir la posibilidad de que las amenazas ocasionen daños al sistema. Estas medidas de prevención contemplarán, entre otras, el análisis, la evaluación de amenazas y riesgos, la disuasión y la reducción de la exposición.

2. Las medidas de control y las responsabilidades en materia de seguridad estarán definidas y documentadas.

3. Para garantizar el cumplimiento de esta política, de manera preventiva, se observarán las siguientes actuaciones:

a) Análisis de seguridad con carácter previo a la puesta en producción de los sistemas.

b) Evaluación regular de la seguridad de los elementos instalados y los eventuales cambios de configuración.

c) Revisión periódica de la aplicación efectiva de las medidas de seguridad establecidas. Esta revisión podrá realizarse mediante auditorías internas o externas.

4. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

5. Dado que los servicios afectados por incidentes de seguridad se pueden degradar rápidamente, se hará un seguimiento continuo para detectar anomalías. La información sobre los mecanismos de detección, así como los datos de seguimiento y análisis se comunicarán periódicamente al responsable de seguridad de la información y ciberseguridad y además, de forma singular, cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

6. Las medidas de detección estarán acompañadas de medidas de respuestas, de forma que se pueda responder eficazmente a los incidentes de seguridad. Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los canales de comunicación a las partes autorizadas y el registro de actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

7. Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

8. Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

9. El sistema garantizará la conservación en soporte electrónico de los datos y documentos y mantendrá disponibles los servicios durante todo el ciclo vital de la información con el fin de facilitar la preservación del patrimonio digital.

Artículo 6. *Manual de procedimientos de seguridad.*

1. Dentro del marco de la normativa aplicable, los procedimientos concretos relacionados con la seguridad o el uso de productos específicos pueden evolucionar por circunstancias de mercado, organizativas o técnicas.

2. Los aspectos sujetos a tales variaciones se plasmarán en un Manual de procedimientos de seguridad (en adelante Manual de procedimientos), que se mantendrá actualizado y a disposición de los interesados como complemento a la presente Política.

3. La Secretaría General es responsable de aprobar el Manual de procedimientos y cualquier actualización al mismo.

Artículo 7. *Titularidad del equipamiento informático.*

El equipamiento de software y hardware que la Asamblea de Madrid facilita a los usuarios de su sistema informático tiene la condición de herramienta de trabajo propiedad de la Cámara y debe serle reintegrado una vez concluya la relación parlamentaria o de servicio que haya determinado su adscripción al usuario, salvo acuerdo expreso adoptado por la Mesa de la Cámara.

Artículo 8. *Existencia de líneas de defensa.*

1. El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita:

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.

b) Minimizar el impacto final sobre el mismo.

2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Artículo 9. *Vigilancia continua y reevaluación periódica.*

1. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

2. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

3. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Artículo 10. *Organización e implantación del proceso de seguridad.*

La estructura organizativa en materia de seguridad de la información de la Asamblea de Madrid es la siguiente:

1. Comité de Seguridad de la Información.

a) La composición del Comité de Seguridad de la Información estará integrada por:

i) Un miembro de la Mesa de la Asamblea, que actuará como presidente.

ii) El titular de la Secretaría General.

iii) El titular de la Dirección de Gestión Parlamentaria.

iv) El titular de la Dirección de Gestión Administrativa.

v) El titular de la Dirección de Informática, Tecnología y Transparencia, que actuará como secretario.

vi) El delegado de Protección de Datos.

vii) El responsable de Seguridad de la Información y Ciberseguridad.

viii) El titular de la Jefatura de Servicio de Proyectos y Soporte de las TIC.

ix) El titular de la Jefatura de Desarrollo y Gestión de las TIC.

b) Las funciones del Comité de Seguridad de la Información son las siguientes:

i) La elaboración de la estrategia de la Asamblea de Madrid sobre la seguridad de la información y la revisión de los informes periódicos en materia de seguridad de la información.

ii) Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

iii) En caso de discrepancia en el seno del Comité de Seguridad de la Información, resolverá su presidente.

2. Responsable de la información.

a) El responsable de la información es el titular de la Secretaría General y, por delegación los titulares de la Dirección de Gestión Parlamentaria y de la Dirección de Gestión Administrativa.

b) Sus funciones son:

i) Determinar los requisitos de seguridad respecto a la información tratada en la Asamblea de Madrid.

ii) La aprobación de los niveles de seguridad en el tratamiento de la información.

iii) La aprobación de instrucciones en materia de seguridad de la información, a propuesta del responsable de la Seguridad.

3. Responsable del Servicio:

a) El responsable del Servicio es el titular de la Dirección de Informática, Tecnología y Transparencia.

b) Sus funciones son:

i) Determinar la infraestructura hardware y software del sistema de información, los criterios de uso, los servicios ofrecidos, los formatos y cualquier otro aspecto del funcionamiento del sistema de información de la Asamblea de Madrid.

ii) La aprobación de los niveles de seguridad en el tratamiento de los servicios.

iii) La supervisión de la prestación, con los requisitos de seguridad adecuados, de los servicios basados en sistemas de información de la Asamblea de Madrid.

4. Responsable de Seguridad de las tecnologías de la información y de las comunicaciones:

a) El responsable de Seguridad de las tecnologías de la información y de las comunicaciones es el técnico informático de Seguridad y Control de Riesgos, puesto que deberá transformarse con la denominación de responsable de Seguridad de la Información y Ciberseguridad, bajo la dependencia directa de la Dirección de Informática, Tecnología y Transparencia.

b) Sus funciones son:

i) Determinar cómo satisfacer los requisitos de seguridad, tanto de la información como de los servicios ofrecidos, incluyendo la definición de procedimientos de seguridad. y, en su

caso, la adopción de medidas de urgencia ante posibles deficiencias o amenazas en la Asamblea de Madrid.

ii) Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el responsable del Sistema.

iii) Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.

iv) Gestionar las revisiones externas o internas del sistema.

v) La planificación y coordinación de las diferentes áreas para asegurar la eficaz implantación de la Política de Seguridad de la Información y evitar duplicidades.

vi) La planificación de auditorías.

vii) La propuesta de normas e instrucciones en materia de seguridad de la información y planificación de su ejecución.

viii) El mantenimiento del sistema de gestión de la seguridad de la información y de los procedimientos que lo componen.

ix) La coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

x) La vigilancia de las medidas de seguridad ante incidentes de seguridad establecidas para proteger la información y garantizar la disponibilidad y correcto funcionamiento de los servicios prestados por los sistemas de información y de los mecanismos de continuidad.

xi) Vigilancia de las autorizaciones concedidas a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

xii) La vigilancia del cumplimiento de los controles de seguridad y los procedimientos operativos de seguridad establecidos.

xiii) Vigilancia de la configuración y estado de actualización, en su caso, del hardware y software que soportan los mecanismos y servicios de seguridad del sistema de información.

xiv) La vigilancia del estado de seguridad del sistema y supervisión de las instalaciones de hardware y software.

xv) La comunicación a los responsables del Sistema de cualquier anomalía o vulnerabilidad relacionada con la seguridad.

xvi) La colaboración en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

xvii) El soporte y asesoramiento al personal técnico de la Dirección de Informática, Tecnología y Transparencia en materias relacionadas con la seguridad.

xviii) La elaboración de informes periódicos en materia de seguridad de la información.

xix) Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.

xx) Elaborar el documento de Declaración de Aplicabilidad.

xxi) Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.

xxii) Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información.

5. Responsables del Sistema.

a) Son responsables del sistema el titular de la Jefatura de Servicio de Proyectos y Soporte de las TIC y el titular de la Jefatura de Desarrollo y Gestión de las TIC.

b) Sus funciones son:

i) El desarrollo, operación y mantenimiento del sistema de información durante todo su ciclo de vida.

ii) La definición de la topología y gestión del sistema de información.

iii) La revisión de la adecuada integración de las políticas y medidas de seguridad en los sistemas.

iv) Los análisis de riesgos.

v) La decisión sobre la suspensión o interrupción temporal de un servicio, cuando se detecten deficiencias graves de seguridad, informando con carácter inmediato de la situación al responsable de seguridad. La decisión final, que será tomada por la Secretaría General, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad.

vi) La propuesta de planes de mejora, así como de planes de formación del personal en materia de seguridad.

vii) La elaboración de planes de continuidad.

viii) Elaborar los procedimientos operativos necesarios.

ix) Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

x) Llevar a cabo las funciones del administrador de la seguridad del sistema:

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

Artículo 11. *Gestión de personal.*

1. El personal, propio o ajeno, relacionado con los sistemas de información, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

2. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por el Comité de Seguridad.

Artículo 12. *Profesionalidad.*

1. La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida.

2. El personal de la Asamblea de Madrid que atiende, revisa y audita la seguridad de los sistemas recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables.

3. La Asamblea de Madrid exigirá, de manera objetiva y no discriminatoria, que los prestadores de servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

Artículo 13. *Autorización y control de los accesos.*

1. El acceso al sistema informático de la Asamblea de Madrid estará controlado y limitado a los usuarios, procesos y dispositivos debidamente autorizados. Este acceso estará restringido a las

funciones permitidas. Dichas funciones serán las mínimas necesarias para que la organización alcance sus objetivos.

2. En la medida en que sea técnicamente posible, respetando los principios generales de administración y de acuerdo con la normativa aplicable (incluido, en su caso, el Manual de procedimientos), se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

3. Los medios de identificación para acceder al sistema son personales e intransferibles. Todo usuario que disponga de ellos está obligado a:

a) Hacerse responsable de las acciones que se realicen.

b) Velar por la confidencialidad y seguridad de dichos medios.

c) Aplicar lo establecido al respecto en el Manual de procedimientos.

d) Avisar inmediatamente al administrador del sistema si considera que sus medios de identificación pueden haberse visto comprometidos.

Artículo 14. *Protección de las instalaciones.*

Los sistemas se instalarán en áreas separadas cuyos accesos estarán dotados de un procedimiento de identificación y control que se regulará mediante instrucción de la Dirección de Informática, Tecnología y Transparencia. Como mínimo, las salas deberán estar cerradas y disponer de un control de llaves.

Artículo 15. *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

En la adquisición de productos de seguridad será exigible la certificación de la funcionalidad de seguridad relacionada con el objeto de dicha adquisición, según el criterio del responsable de seguridad y aplicando el principio de proporcionalidad. Para la contratación de servicios de seguridad se estará a lo dispuesto en el artículo 12.

Artículo 16. *Mínimo privilegio.*

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

1. El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.

2. Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

3. Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

4. Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Artículo 17. *Integridad y actualización del sistema.*

1. El sistema informático de la Asamblea de Madrid será diseñado y mantenido, mediante prestación directa o indirecta, bajo criterios técnicos, de eficiencia y de seguridad de la Dirección de Informática, Tecnología y Transparencia.

2. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. También requerirá autorización formal previa cualquier alteración de la configuración de hardware y software de los equipos o cualquier desinstalación de programas de la plataforma de uso predefinida. Dicha autorización será otorgada en su caso por el titular de la Dirección de Informática, Tecnología y Transparencia, o bien estará recogida de forma general en el Manual de procedimientos.

3. Con carácter general, no se instalará software salvo que se disponga de la correspondiente licencia de uso, bien por haberlo adquirido la Asamblea de Madrid, o bien por tratarse de software libre con una licencia aplicable. En todo caso, será el administrador del sistema quien instale el software una vez se autorice.

4. Como corresponsables que son de la seguridad del sistema, los usuarios comunicarán al responsable del servicio cualquier conflicto entre sus necesidades funcionales y las medidas de seguridad, de modo que el responsable del servicio y el de seguridad de la información puedan estudiar una solución.

5. El sistema ha de proteger el perímetro, en particular en lo referente a su conexión con redes públicas.

6. Toda intervención, modificación o reparación que sea preciso realizar en un dispositivo del sistema informático deberá canalizarse a través de la Dirección de Informática, Tecnología y Transparencia, mediante el procedimiento de solicitud establecido al efecto.

Artículo 18. *Protección de información almacenada y en tránsito.*

1. En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

2. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

3. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se

aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Artículo 19. *Prevención ante otros sistemas de información interconectados.*

Se protegerá el perímetro del sistema de información, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión.

Artículo 20. *Registro de actividad y detección de código dañino.*

1. Con el propósito de satisfacer con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Artículo 21. *Incidentes de seguridad.*

1. Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos se reflejarán en el Manual de procedimientos.

2. Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Artículo 22. *Continuidad de la actividad.*

1. Se desarrollarán planes de continuidad de los sistemas de tecnologías de la información y de las comunicaciones para garantizar la disponibilidad de los servicios críticos.

2. El titular de la Dirección de Informática, Tecnología y Transparencia diseñará y establecerá las políticas de copia de seguridad de los datos alojados en los servidores corporativos con el previo asesoramiento del responsable de seguridad de la información y ciberseguridad.

3. Las copias de seguridad y las medidas de recuperación que se implanten permitirán la restauración de la información y los servicios, de forma que sea posible hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

4. La copia de seguridad y salvaguarda de los datos alojados en los dispositivos de la Asamblea de Madrid asignados a los usuarios es responsabilidad de cada usuario. La Dirección de Informática,

Tecnología y Transparencia está facultada para borrar el contenido de estos dispositivos en caso de avería que así lo requiera o en el momento en que termine la relación entre el usuario y la Asamblea de Madrid.

5. Atendiendo al principio de proporcionalidad, y en la medida en que lo permitan los medios disponibles, se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Artículo 23. *Mejora continua del proceso de seguridad.*

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Estas modificaciones se reflejarán en el Manual de procedimientos.

Artículo 24. *Información publicada.*

1. La información pública de la Asamblea de Madrid estará disponible en el sitio web www.asambleamadrid.es en los términos que, de acuerdo con la legislación aplicable, determine la Mesa de la Cámara y ejecute la Secretaría General.

2. Asimismo, en el sitio web se podrá publicar otras informaciones que la Presidencia de la Cámara considere de interés.

3. En el Manual de procedimientos se recogerán los procedimientos de publicación en el sitio web, asignando responsables y pautas de actuación. En el caso excepcional de publicación a través de la Dirección de Informática, Tecnología y Transparencia, la información a publicar se facilitará ya elaborada y en el formato final. La Dirección de Informática, Tecnología y Transparencia se limitará a ponerla a disposición del público, sin intervenir en su contenido.

Artículo 25. *Principios generales de administración.*

1. El responsable del servicio, el responsable de seguridad de tecnologías de la información y comunicaciones y los responsables del sistema deberán, en todo caso, respetar el principio de proporcionalidad en la adopción de medidas que demanden la seguridad e integridad del sistema y observar el sigilo profesional en el tratamiento de cualquier tipo de información que se gestione, en función de las tareas asignadas a cada usuario.

2. A fin de poder garantizar la seguridad e integridad del sistema, el responsable del servicio arbitrará los mecanismos y herramientas oportunos para la prestación eficaz del mismo, incluyendo la definición de políticas globales de administración de los equipos, copias de seguridad o sistemas de intervención remota o sin presencia del usuario.

3. Cuando la Dirección de Informática, Tecnología y Transparencia realice una intervención en un equipo podrá optar por una intervención remota (durante la cual el técnico que la realiza no está presente físicamente en la ubicación del equipo, sino que la realiza a distancia) y/o sin presencia del usuario (durante la cual el usuario del equipo no está presente físicamente en la ubicación de este). En el caso de una intervención remota o sin presencia del usuario, el personal técnico velará por la privacidad y la salvaguarda de los derechos de los usuarios afectados de acuerdo con el principio de proporcionalidad y en los términos establecidos en el Manual de procedimientos.

4. La producción y, en su caso, modificación de expedientes electrónicos, documentos electrónicos, publicaciones oficiales o cualquier otra información electrónica será realizada exclusivamente por los usuarios y Servicios competentes y observando los procedimientos legales. Cuando para realizar una modificación sea precisa la intervención de la Dirección de Informática, Tecnología y Transparencia, esta tendrá lugar previa solicitud, de la que quedará constancia escrita, realizada por el canal que se establezca en el Manual de procedimientos. La intervención se ajustará a lo detallado en dicha solicitud.

5. Las funciones de administración estarán convenientemente protegidas para evitar el acceso a las mismas de usuarios no autorizados.

Artículo 26. *Almacenamiento en servidores corporativos.*

1. Los servidores corporativos podrán ofrecer espacios comunes de almacenamiento para compartir información y trabajar en equipo. El responsable del servicio diseñará dichos espacios de acuerdo con las necesidades planteadas y los recursos disponibles, asignará dichos espacios a los usuarios o grupos de usuarios y diseñará el sistema de permisos para su utilización.

2. Es responsabilidad de los usuarios realizar un uso adecuado de dichos espacios, teniendo en cuenta los recursos disponibles y la finalidad para la que se les facilita el acceso. En particular, evitarán almacenar en ellos información ajena a los fines a los que se destinan, y pondrán especial atención cuando manejen la información de los servidores a fin de prevenir la destrucción o degradación accidental de la misma.

3. Los usuarios de esos espacios deberán seguir las instrucciones de sus respectivos jefes de Servicio respecto a la organización, nomenclatura e integridad de la información que almacenan en ellos, así como eliminar convenientemente los datos obsoletos o innecesarios de acuerdo con tales instrucciones. Los jefes de Servicio, a su vez, tendrán en cuenta las directrices del responsable del servicio.

Artículo 27. *Sistemas ajenos a la Asamblea de Madrid.*

1. Las aplicaciones de proceso y almacenamiento de información implantadas por terceros y ajenas al control de la Asamblea de Madrid (incluidos sistemas de almacenamiento en redes externas, herramientas de sincronización o compartición de ficheros, herramientas colaborativas y sociales, cuentas de correo de terceros y cualesquiera otras que operen en circunstancias similares) no pertenecen al sistema informático de la Asamblea de Madrid y no tendrán acceso a la red corporativa.

2. En consecuencia, como norma general desde la Dirección de Informática, Tecnología y Transparencia no se facilitará el acceso a tales aplicaciones ni resolverá incidencias relacionadas con las mismas.

3. Excepcionalmente, el responsable del servicio puede decidir autorizar la instalación y uso de alguna de estas aplicaciones ajenas. En tal caso:

a) Esta autorización no supondrá en ningún caso la incorporación de la aplicación a la cartera de servicios ofrecidos por la Asamblea de Madrid.

b) La Dirección de Informática, Tecnología y Transparencia no ofrecerá soporte para las incidencias producidas en la aplicación.

c) Una vez concedida una autorización de uso, la Dirección de Informática, Tecnología y Transparencia podrá revocar dicha autorización en cualquier momento por razones técnicas o de seguridad, tanto con carácter general como para dispositivos concretos. En caso de conflicto entre una aplicación ajena y el sistema informático de la Asamblea de Madrid, se resolverá a favor de este último desinstalando la aplicación.

d) El usuario que haga uso de tal autorización observará las mismas pautas de seguridad y se someterá implícitamente a la misma normativa que cuando utiliza aplicaciones del sistema informático de la Asamblea de Madrid. Será asimismo el único responsable en relación con el uso de la aplicación (confidencialidad, seguridad, protección de datos personales, jurisdicción de los servidores, propiedad intelectual, cambios en los términos de uso de la aplicación, etc.).

Artículo 28. *Uso adecuado.*

1. El uso del sistema informático de la Asamblea de Madrid obedece a fines profesionales. El uso personal deberá ser moderado y no deberá interferir con el funcionamiento normal del sistema.

2. En todo caso, no están permitidas acciones que puedan incidir negativamente en el rendimiento global del sistema o entorpecer su uso por el resto de los usuarios, salvo que así se recoja explícitamente en el Manual de procedimientos.

Artículo 29. *Dispositivos personales.*

1. Los dispositivos personales que no sean propiedad de la Asamblea de Madrid no se consideran parte del sistema informático de la Asamblea de Madrid.

2. Los dispositivos personales no tendrán acceso a la red corporativa.

Artículo 30. *Confidencialidad y cifrado.*

1. La confidencialidad en el contenido de documentos y comunicaciones gestionadas mediante el sistema informático de la Asamblea de Madrid está protegida por las medidas de seguridad dispuestas en el mismo, así como por los principios generales de administración y la deontología que vinculan a todo el personal adscrito a la Dirección de Informática, Tecnología y Transparencia.

2. En caso de que un usuario plantee necesidades adicionales de confidencialidad respecto a las garantías ofrecidas por las medidas de seguridad y los principios generales de administración, puede utilizar herramientas de cifrado de modo que solamente el emisor y el receptor puedan acceder a esos contenidos.

Artículo 31. *Fin de la relación de un usuario con la Asamblea de Madrid.*

1. Cuando termina la relación de un usuario con la Asamblea de Madrid, dicho usuario debe restituir los medios que esta le haya facilitado, salvo acuerdo expreso adoptado por la Mesa de la Asamblea.

2. Desde el momento mismo en que termina la relación, la Dirección de Informática, Tecnología y Transparencia procederá a la eliminación de todos los datos almacenados en los dispositivos adscritos al usuario, la revocación de todos los medios de identificación y permisos de acceso, la cancelación de

sus cuentas y eliminación de los mensajes almacenados en servidores (en particular los de correo electrónico o similares), y cualquier otra información que se haya asociado al usuario a efectos de uso del sistema de información.

3. Es responsabilidad del usuario haber realizado, con anterioridad al fin de la relación, las copias de seguridad de toda la información que desee conservar.

4. En lo que se refiere a la confidencialidad de la información a la que hayan accedido debido a su desempeño en la Asamblea de Madrid, los usuarios cuya relación con esta termine estarán sujetos a lo que establezca la normativa aplicable.

Artículo 32. *Obligaciones de los usuarios.*

1. Todos los usuarios del sistema informático de la Asamblea de Madrid tienen la obligación de conocer y cumplir la Política de Seguridad de la Información, así como las instrucciones y procedimientos que se aprueben en su desarrollo.

2. Será obligatorio asistir a los programas formativos y a las sesiones de concienciación en materia de seguridad que se programen, cuando así se establezca.

3. Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación adaptada para garantizar el manejo seguro de los sistemas. La asistencia a dicha formación será obligatoria.

4. Las actuaciones que realiza el personal relacionado con la gestión de la información y los sistemas podrán ser supervisadas para verificar que se cumplan los procedimientos establecidos.

Artículo 33. *Relación con terceros.*

1. Cuando la Asamblea de Madrid utilice servicios de terceros o ceda información a terceros, se les informará de la obligatoriedad del cumplimiento de esta Política de Seguridad de la Información y de las instrucciones y procedimientos de desarrollo que pudieran afectarles.

2. Se establecerán procedimientos específicos de comunicación y resolución de incidencias.

Disposición adicional. Desarrollo de la Política de Seguridad de la Información de la Asamblea de Madrid.

La Política de Seguridad de la Información se desarrollará a través de instrucciones y procedimientos de seguridad que se elaborarán con participación del Comité de Seguridad y que estarán a disposición de todos los usuarios internos que utilicen, operen o administren los sistemas de información y comunicaciones.

Disposición final. Entrada en vigor.

La Política de Seguridad de la Información de la Asamblea de Madrid entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de la Asamblea de Madrid.