14. Política de Seguridad de la Junta General (BOJG/X/C/29).

(Acuerdo de la Mesa de la Cámara de 31 de enero de 2017)

Preámbulo

La implantación del e-Parlamento en la Junta General, regulada por las Normas de aplicación aprobadas por la Mesa en octubre de 2013 (BOJG IX/B/480), requiere reforzar los estándares y medidas de seguridad de las normas de 2007, teniendo en cuenta además lo establecido en el Esquema Nacional de Seguridad aprobado en el Real Decreto 3/2010, de 8 de enero.

CAPÍTULO I
NORMAS GENERALES

Artículo 1. Objeto y ámbito de aplicación

1. La presente Política establece las directrices que rigen la forma en que la Junta General gestiona y protege la información y los servicios que considera críticos.
2. Esta Política regula directamente la actividad de la Junta General y el uso del equipamiento hardware y software que la Junta General 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 Junta General 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 Junta General 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, en el marco de lo indicado en la Política de Gestión de Documentos Electrónicos.

Artículo 2. 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 3. Titularidad del equipamiento informático

El equipamiento de software y hardware que la Junta General 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.

CAPÍTULO II
RESPONSABILIDAD

Artículo 4. Responsables

1. El responsable de la información determina los requisitos de seguridad respecto a la información tratada en la Junta General. Esta función corresponde al Letrado Mayor o Letrado en quien delegue.
2. El responsable del servicio determina 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 Junta General. Esta función corresponde al Jefe del Servicio de Servicios Técnicos o funcionario de su Servicio en quien delegue.
3. El responsable de seguridad determina 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 Junta General. Esta función corresponde al Jefe del Servicio de Servicios Técnicos o funcionario de su servicio en quien delegue.
4. El administrador del sistema desarrolla, opera y mantiene el sistema de información de la Junta General. Esta función corresponde al Jefe del Servicio de Servicios Técnicos o funcionario de su servicio en quien delegue.
5. Las discrepancias en materia de seguridad serán resueltas atendiendo al criterio de mayor jerarquía.

Artículo 5. 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 Junta General 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 Junta General 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 6. La seguridad como 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. Todos los usuarios del sistema informático de la Junta General están 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.
3. 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 7. Información publicada
1. La información pública de la Junta General estará disponible en la sede electrónica www.jgpa.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 la sede electrónica 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 la sede electrónica, asignando responsables y pautas de actuación. En caso de publicación a través del Servicio de Servicios Técnicos, la información a publicar se facilitará ya elaborada y en el formato final. El Servicio de Servicios Técnicos se limitará a ponerla a disposición del público, sin intervenir en su contenido.

CAPÍTULO III
ADMINISTRACIÓN DEL SISTEMA

Artículo 8. Principios generales de administración
1. El responsable del servicio, el responsable de seguridad y el administrador 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 el Servicio de Servicios Técnicos 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 del mismo). 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 del Servicio de Servicios Técnicos, 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 del Servicio 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 9. Integridad del sistema

1. El sistema informático de la Junta General será diseñado y mantenido por el responsable del servicio bajo criterios técnicos, de eficiencia y de seguridad.
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 responsable del servicio, 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 Junta General, 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 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 del Servicio de Servicios Técnicos, mediante el procedimiento de solicitud establecido al efecto.

Artículo 10. 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 accidentales 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 11. Copias de seguridad y sistemas de respaldo

1. El responsable del servicio diseñará y establecerá las políticas de copia de seguridad de los datos alojados en los servidores corporativos.
2. La copia de seguridad y salvaguarda de los datos alojados en los dispositivos de la Junta General asignados a los usuarios es responsabilidad de cada usuario. El Servicio de Servicios Técnicos está facultado 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 Junta General.
3. 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 12. Sistemas ajenos a la Junta General

1. Las aplicaciones de proceso y almacenamiento de información implantadas por terceros y ajenas al control de la Junta General (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 Junta General.
2. En consecuencia, como norma general el responsable del servicio no 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 Junta General a la que se refiere el artículo 4.2.
b) El Servicio de Servicios Técnicos no ofrecerá soporte para las incidencias producidas en la aplicación.
c) Una vez concedida una autorización de uso, el responsable del servicio 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 Junta General, 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 Junta General. 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.).

CAPÍTULO IV
USO DEL SISTEMA

Artículo 13. Uso adecuado

1. El uso del sistema informático de la Junta General 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 usuarios (tales como el tráfico masivo de información, el uso intensivo de la capacidad de proceso de los servidores o la ocupación injustificada de sesiones y licencias), salvo que sea imprescindible para el desarrollo de las funciones propias del trabajo administrativo o parlamentario y así se recoja explícitamente en el Manual de procedimientos.

Artículo 14. Acceso al sistema informático

1. El acceso al sistema informático de la Junta General 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 (contraseñas, certificados digitales o cualesquiera otros que se establezca) son personales e intransferibles. Todo usuario que disponga de ellos está obligado a:
a) Hacerse responsable de las acciones que se realicen usando sus medios de identificación.
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.
4. Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas deberán estar cerradas y disponer de un control de llaves.

Artículo 15. Dispositivos personales

1. Los dispositivos personales (que no sean propiedad de la Junta General) no se consideran parte del sistema informático de la Junta General.
2. Los dispositivos personales, como principio general, no tendrán acceso a la red corporativa. No obstante, circunstancialmente podrán arbitrarse procedimientos que permitan su acceso a la misma, sujeto a las condiciones y requisitos mínimos que se determine en el Manual de procedimientos.

3. En caso de que estén vigentes procedimientos de acceso a la red corporativa mediante dispositivos personales, y en la medida en que sea estrictamente necesario para cumplir las condiciones de acceso impuestas, el Servicio de Servicios Técnicos podrá intervenir en dichos dispositivos, si su propietario así lo requiere, únicamente a efectos de configuración de las herramientas de trabajo que se haya dispuesto. Estas intervenciones:
a) Solamente se realizarán en dispositivos que cumplan las condiciones y requisitos establecidos en el Manual de procedimientos.
b) Se limitarán a la mera configuración de los mismos según lo indicado en el procedimiento correspondiente.
c) En ningún caso supondrán ningún tipo de reparación o mejora genérica del dispositivo.
4. Si un usuario utiliza un dispositivo personal en un procedimiento de acceso autorizado a la red corporativa, estará obligado a observar las mismas pautas de seguridad y a someterse implícitamente a la misma normativa que si realizase el acceso con un dispositivo propiedad de la Junta General.

Artículo 16. Confidencialidad y cifrado
1. La confidencialidad en el contenido de documentos y comunicaciones gestionadas mediante el sistema informático de la Junta General está protegida por las medidas de seguridad dispuestas en el mismo, así como por los principios generales de administración y la deontología que vinculan al responsable del servicio, al responsable de seguridad y al administrador del sistema.
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 17. Fin de la relación de un usuario con la Junta General
1. Cuando termina la relación de un usuario con la Junta General, dicho usuario debe restituir los medios que esta le haya facilitado.
2. Desde el momento mismo en que termina la relación, el Servicio de Servicios Técnicos 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 en razón de su desempeño en la Junta General, los usuarios cuya relación con esta termine estarán sujetos a lo que establezca la normativa aplicable.

CAPÍTULO V
OTROS PROCEDIMIENTOS

Artículo 18. Mejora continua
El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Estas modificaciones se reflejarán en el Manual de procedimientos.

Artículo 19. 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 se reflejarán en el Manual de procedimientos.

Artículo 20. Análisis y gestión de riesgos
1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.
3. La periodicidad y características del análisis y gestión de riesgos se detallarán en el Manual de procedimientos.

Artículo 21. 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 5.

Disposición adicional
Se establecen los siguientes datos identificativos para la presente Política:

Nombre:	Política de seguridad de la Junta General del Principado de Asturias
Versión:	1.0
Identificador de la Política:	I00000141_PS
URI de referencia de la Política:	http://www.jgpa.es/ps
Año de publicación:	2017
Ámbito de aplicación:	Directrices que rigen la forma en que la Junta General gestiona y protege la información y los servicios que considera críticos.
Identificador del gestor de la Política:	Nombre del gestor: Junta General del Principado de Asturias. Secretaría General. DIRECCIÓN: C/ CABO NOVAL Nº 9, 33007. OVIEDO Identificador del gestor: I00000141

Disposición derogatoria

Quedan derogadas las Normas de Uso del Sistema Informático de la Junta General aprobadas por Acuerdo de la Mesa de 4 de diciembre de 2007 (BOJG/VII/C/12) y modificadas por Acuerdo de la Mesa de 27 de septiembre de 2011 (BOJG/VIII/C/15).

Disposición final

La presente Política entrará en vigor desde su publicación en el Boletín Oficial de la Junta General.