III. ADMINISTRACIÓN LOCAL

AYUNTAMIENTO DE

39 ALCOBENDAS

OTROS ANUNCIOS

En virtud de las competencias previstas en el artículo 124.4 letras a), g), i) de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, y conforme a lo dispuesto en los artículos 22, 27, 33.4, 66 y 68 del Reglamento Orgánico de Gobierno y Administración (ROGA), vistos también los informes técnicos y jurídicos que obran en el expediente instruido al efecto,

HE RESUELTO

Aprobar el decreto número 2556, de fecha 13 de febrero de 2026, de Alcaldía Presidencia, como norma marco para establecer la Política General de Seguridad de la información aplicable a todos los sistemas TIC, personal y contratistas del Ayuntamiento cuyo anexo contiene el siguiente texto íntegro de dicha Política, que entrará en vigor el día de su publicación en el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID y en la sede electrónica municipal.

ANEXO POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. También estableció que el mismo debía mantenerse actualizado de manera permanente y, en desarrollo de este precepto, el Real Decreto 3/2010, de 8 de enero, establece que el Esquema Nacional de Seguridad se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de Administración electrónica, la evolución de la tecnología, los nuevos estándares internacionales sobre seguridad y auditoría, y la consolidación de las infraestructuras que le sirven de apoyo, manteniéndose actualizado de manera permanente.

Adicionalmente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados y recoge el Esquema Nacional de Seguridad en su artículo 156. Mientras que la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13 sobre derechos de las personas en sus relaciones con las Administraciones Públicas el relativo a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

En efecto, los ciudadanos confían en que los servicios públicos disponibles por el medio electrónico se presten en unas condiciones de seguridad equivalentes a las que encuentran cuando se acercan personalmente a las oficinas de la Administración.

Por otra parte, las ciberamenazas, que constituyen riesgos que afectan singularmente a la Seguridad Nacional, se han convertido en un potente instrumento de agresión contra las entidades públicas y los ciudadanos en sus relaciones con las mismas, de manera que la ciberseguridad figura entre los doce ámbitos prioritarios de actuación de la Estrategia de Seguridad Nacional como instrumento actualizado para encarar el constante y profundo cambio mundial en el que nos hayamos inmersos y como garantía de la adecuada actuación de España en el ámbito internacional. En particular, dicho ámbito de actuación de ciberseguridad se refiere a la garantía de la seguridad de

BOCM-20260302-39

los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas y a que se finalizará la implantación del Esquema Nacional de Seguridad, previsto en la Ley 11/2007, de 22 de junio. Profundizando en la cuestión, la Estrategia de Ciberseguridad Nacional «que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia» y en su línea de acción 2, titulada «Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas», se incluye la medida relativa a «Asegurar la plena implantación del Esquema Nacional de Seguridad y articular los procedimientos necesarios para conocer regularmente el estado de las principales variables de seguridad de los sistemas afectados».

El Ayuntamiento de Alcobendas, en el ámbito de sus competencias promueven actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de los vecinos del municipio. Los principios de la institución, misión, visión y valores publicados en la sede electrónica (https://www.alcobendas.org/es/transparencia/buen-gobierno) actúan como principios de calidad en la gestión que impulsa a alcanzar los objetivos y a adoptar los máximos estándares de calidad, entre los que se encuentran la seguridad. Esta prestación de servicios se fundamenta en el uso de Sistemas de Información que deben estar protegidos de una forma efectiva y eficiente

El Ayuntamiento de Alcobendas considera la información un activo esencial para el cumplimiento adecuado de sus funciones. Asume, por lo tanto, la seguridad de la información (incluyendo los sistemas que la procesa, la infraestructura tecnológica soporte, las instalaciones desde la que se realiza ese tratamiento y las propias personas) como una responsabilidad asociada a su protección frente a las amenazas que puedan afectar a su integridad, disponibilidad y/o confidencialidad fundamentalmente.

En cumplimiento de las Leyes 39/2015 de 1 de octubre del Procedimiento Administrativo común de las Administraciones Públicas, y 40/2015 de 1 de octubre del Régimen Jurídico del Sector Público, se hace necesario un marco de actuación en el que se desarrolle el procedimiento administrativo común para la gestión administrativa por medios electrónicos.

El Esquema Nacional de Seguridad (en adelante, ENS), establecido en el artículo 42.2 de la Ley 11/2007 de 22 de Junio, de acceso electrónico de los ciudadanos a los servicios públicos, y regulado por Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, el cuál deroga el Real Decreto 3/2010 de 8 de enero , proporciona el marco de gestión de la seguridad de la información en el ámbito de la administración electrónica, reconociendo como activos estratégicos la información y los sistemas que la soportan y asentando las bases sobre las cuales el Ayuntamiento de Alcobendas proporciona a las personas comprendidas en el ámbito de aplicación de esta Política de Seguridad de la Información y a los ciudadanos un entorno seguro de gestión para el acceso a los servicios, preservando sus derechos y anticipándose a sus necesidades.

Según lo mencionado en el artículo 12 del Real Decreto 311/2022: “cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente”.

La Política de Seguridad de la Información del Ayuntamiento de Alcobendas fue aprobada por Decreto de Alcaldía n.º 8474 de 23 de mayo de 2022, dejando sin efecto la anterior política aprobada por Decreto n.º 3709 de 18 de marzo de 2021. Esta política establece el marco normativo y organizativo para la protección de la información municipal, en cumplimiento del Esquema Nacional de Seguridad (ENS), la Directiva NIS2, el RGPD y la LOPD-GDD. El proceso de revisión y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) exige su actualización periódica para adaptarse a los cambios tecnológicos, normativos y a las recomendaciones derivadas de auditorías y análisis de riesgos. Asimismo, la reciente publicación de la Guía CCN-STIC 805 - Política de Seguridad de la Información (junio 2025) refuerza la necesidad de adaptar la política local a los nuevos requisitos y recomendaciones del ENS, estableciendo pautas y estructura para la política de seguridad aplicable a entidades públicas.

Habiéndose constituido el actual equipo de gobierno municipal en Alcobendas el 17 de junio de 2023; aprobadas las delegaciones por Decreto de Alcaldía 2585/2024, de 22 de febrero y vistas las modificaciones del mismo aprobadas por Decreto 4992/2024 de fecha 05 de abril sobre delegación de competencias en concejales y directores generales; y en virtud de las atribuciones propias de la Alcaldía en virtud de las competencias previstas en el Art. 124.4 letras a), g), i) de la Ley 7/1985, de 2 de abril, de Bases de Régimen Local (LRBRL); un nuevo proceso de revisión de la Política de Seguridad de la Información es necesario y justificado para garantizar la protección de los activos de información del Ayuntamiento de Alcobendas, cumplir con la normativa vigente y responder eficazmente a los nuevos retos en materia de ciberseguridad

Por todo lo expuesto; de conformidad con las competencias previstas legalmente y sin perjuicio de los informes jurídicos que se acumulen también en el expediente instruido al efecto, se aprueba el contenido siguiente de la POLITICA DE SEGURIDAD DE LA INFORMACION DEL AYUNTAMIENTO DE ALCOBENDAS:

BOCM-20260302-39

Primera. - Objeto

El Ayuntamiento de Alcobendas considera la información un activo esencial para el cumplimiento adecuado de sus funciones. Asume, por lo tanto, la seguridad de la información (incluyendo los sistemas que la procesa, la infraestructura tecnológica soporte, las instalaciones desde la que se realiza ese tratamiento y las propias personas) como una responsabilidad asociada a su protección frente a las amenazas que puedan afectar a su integridad, disponibilidad, confidencialidad, autenticidad y trazabilidad.

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, trazabilidad, autenticidad, 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.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

El Ayuntamiento de Alcobendas debe contemplar las acciones relativas a los aspectos de prevención, detección respuesta y conservación, frente a incidentes de seguridad, de acuerdo con el Artículo 8 del ENS.

Prevención

El Ayuntamiento de Alcobendas 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, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

Autorizar los sistemas antes de entrar en operación.

Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

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.

Respuesta

El Ayuntamiento de Alcobendas establece mecanismos para responder eficazmente a los incidentes de seguridad.

Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

BOCM-20260302-39

Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Conservación

El Ayuntamiento aplicará procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información.

Segunda. - Ámbito de aplicación

La presente Política aplica a todos los sistemas TIC y al personal laboral y funcionario del Ayuntamiento de Alcobendas, a sus contratistas y a todos los que desarrollen funciones para el Ayuntamiento de Alcobendas. En particular, el acceso a los sistemas de información estará condicionado a la adhesión a esta Política y a las Normativas asociadas existentes, siendo estas de obligado cumplimiento.

Tercera. - Objetivo

El Ayuntamiento de Alcobendas define, a través de este documento, una Política de Seguridad de la Información, de carácter obligatorio para todos aquellos comprendidos en el ámbito de aplicación, con el objetivo de garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a los incidentes que puedan ocurrir.

La Política de Seguridad de la Información velará por la seguridad de la información, siendo ésta de aplicación en todas las fases del ciclo de vida de la información y sus documentos: generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción; así como de los sistemas que los soportan: análisis, diseño, desarrollo, implantación, explotación y mantenimiento.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve la organización para desarrollar sus funciones, y se realicen, bajo garantías de seguridad, en sus distintas dimensiones:

- Disponibilidad: propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.
- Integridad: propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.
- Confidencialidad: propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.
- Autenticidad: propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.
- Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la Información serán:

- Aceptar como activos estratégicos la información y los sistemas que la soportan, manifestando su determinación en alcanzar los niveles de seguridad necesarios que certifiquen de forma rentable su protección, garantizando la seguridad de la información, en las distintas dimensiones antes descritas, y así mejorar la calidad de los servicios que ofrece a los ciudadanos.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de contingencias y continuidad de la actividad que se definan.
- Realizar una adecuada gestión de incidentes que afecten a la seguridad de la información.
- Concienciar con el fin de que la Política de Seguridad de la Información tenga la máxima repercusión dentro del Ayuntamiento, desarrollando metas a corto, medio y largo plazo e incorporando técnicas específicas de motivación.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.

BOCM-20260302-39

- Adoptar la Política de Seguridad de la Información como la principal herramienta de garantía de seguridad de la información y de los objetivos de negocio, promoviendo y asegurando su cumplimiento para todas las personas comprendidas en su ámbito de aplicación.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

Está Política de Seguridad:

Se revisará regularmente, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.

Se comunicará a todas las personas comprendidas en su ámbito de aplicación.

Está escrita a un nivel amplio, por lo que se complementará con documentos más precisos: Normativas de seguridad (nivel organizacional), ya sean generales o específicas, procedimientos de seguridad (nivel ejecutivo). Si se considera necesario, también podrán detallarse en instrucciones técnicas tareas específicas.

Cuarta. - Declaración de la Política de Seguridad de la Información

Es la política de esta organización asegurar que:

- La información y los servicios están protegidos contra pérdidas de disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad
- La información está protegida contra accesos no autorizados.
- Su cumplen los requisitos legales aplicables.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Los incidentes de seguridad son comunicados y tratados apropiadamente.

Se establecen procedimientos para cumplir con esta Política.

El responsable de Seguridad de la Información será el encargado de mantener esta política, los procedimientos y de proporcionar apoyo en su implementación.

El responsable de la Información y de los Servicios será el encargado de implementar esta Política y sus correspondientes procedimientos.

Cada persona comprendida en el ámbito de aplicación de esta Política de Seguridad es responsable del cumplimiento de la Política y sus procedimientos según aplique en su relación con el Ayuntamiento de Alcobendas.

El Ayuntamiento de Alcobendas implementa, mantiene y realiza un seguimiento del Esquema Nacional de Seguridad.

Esta Política está basada en los criterios del estándar Internacional ISO/IEC 27001 y en la guía del Centro Criptológico Nacional “CCN-STIC-805 Política De Seguridad de la Información”, y establece las medidas necesarias para garantizar el nivel de seguridad exigido por el marco legal vigente en materia de protección de datos de carácter personal.

Cualquier plan específico sobre Seguridad de la Información deberá ajustarse a las disposiciones y recomendaciones, de carácter más general y superior de esta Política.

Quinta. - Marco Normativo

Según la legislación vigente, en el momento de aprobación de esta Política de Seguridad las leyes aplicables al Ayuntamiento de Alcobendas en materia de Seguridad de la Información son:

Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.

Ley 34/2002, de 11 de Julio. De Servicios de Sociedad de la Información y de comercio electrónico.

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

BOCM-20260302-39

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.

Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

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.

Directiva NIS2 (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

Sexta. - Organización y Gestión de la Seguridad

El Comité de Seguridad de la Información coordina la seguridad de la información en el Ayuntamiento de Alcobendas y la designación inicial de sus miembros se realizará por Decreto de Alcaldía. El nombramiento se revisará cada dos años o cuando un puesto quede vacante. **En la DISPOSICION ADICIONAL de esta política de seguridad de la información se detalla su composición, las funciones, responsabilidades y tareas principales de sus miembros.**

Sin perjuicio de las funciones de coordinación, supervisión y gobierno de la seguridad atribuidas al Comité de Seguridad de la Información, el Ayuntamiento de Alcobendas podrá disponer de un Comité de Crisis de Ciberseguridad como órgano extraordinario y de carácter temporal, destinado a la dirección, coordinación y gestión de la respuesta ante incidentes de ciberseguridad de especial gravedad o impacto que comprometan, o puedan comprometer, la continuidad de los servicios municipales, la seguridad de los sistemas de información o la protección de los datos personales.

Dicho Comité se activará y actuará con carácter ejecutivo durante la situación de crisis y no sustituirá ni menoscabará las competencias del Comité de Seguridad de la Información. Finalizada la gestión del incidente, el Comité de Crisis remitirá al Comité de Seguridad de la Información la información, informes y propuestas necesarias para su análisis, valoración e incorporación, en su caso, al Sistema de Gestión de Seguridad de la Información, en el marco del principio de mejora continua establecido en el Esquema Nacional de Seguridad.

De acuerdo con el Principio de Jerarquía que rige en las administraciones públicas españolas, en caso de conflicto entre responsables y/o entre diferentes servicios de la entidad, sobre la seguridad de la información; éste será resuelto en primera instancia por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad, elevando aquellos casos en los que no tenga suficiente autoridad para decidir o resolver el conflicto.

Séptima. - Vigencia de la Política

La Política de Seguridad de la Información vigente propuesta por el Comité de Seguridad de la Información deberá ser aprobada por Decreto de Alcaldía.

BOCM-20260302-39

Cualquier modificación posterior requerirá nuevamente la supervisión del Comité de Seguridad de la Información y aprobación por Decreto de Alcaldía, previo a su entrada en vigor. Las versiones anteriores que hayan podido distribuirse constituyen borradores desarrollados temporalmente, y su vigencia queda anulada por la versión aprobada de este documento.

En el caso de que algún apartado de la Normativa de Seguridad del Ayuntamiento de Alcobendas entre en conflicto con esta Política, ésta última tendrá prioridad. Anualmente será revisada la vigencia y razonabilidad de la Política de Seguridad de la Información por parte del Comité de Seguridad de la Información, así como del enfoque con el que se aborda la protección de la información.

Octava. - Revisión de la política

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad como a la adaptación a los cambios en el marco legal, infraestructura tecnológica, organización general, etc. Entre los elementos a considerar se incluyen:

- Análisis y evaluación de riesgos.
- Resultados de auditorías o revisiones de terceros independientes o internas.
- Estado de las medidas preventivas o correctivas que pudieran estar planificadas.
- Análisis de cumplimiento por parte de las empresas que prestan los servicios en el Ayuntamiento.
- Tendencias asociadas a amenazas y vulnerabilidades.
- Información asociada a incidentes de seguridad identificados en el Ayuntamiento.
- Recomendaciones o directrices de órganos competentes.
- Cambios en el estándar adoptado como marco de referencia.

Se mantendrá un registro de las revisiones realizadas y se conservará, como evidencia, las actas aprobadas de las reuniones mantenidas con los cambios acordados en la Política de Seguridad de la Información. Las sucesivas revisiones de lo descrito en el ANEXO I no exige una aprobación de la política en su totalidad, sino que serán realizadas y entrarán en vigor cuando así lo acuerde el Comité de Seguridad.

Novena. - Difusión y custodia de la Política

El Ayuntamiento de Alcobendas, a través del Comité de Seguridad de la Información, potenciará el conocimiento y difusión de la presente Política en los niveles adecuados, dado que interpreta este factor como crítico para asegurar su implantación eficaz y un cumplimiento efectivo.

Corresponde al Comité de Seguridad de la Información impulsar de forma efectiva la implantación de la Política de Seguridad de la Información.

La distribución a las personas comprendidas en el ámbito de aplicación de esta Política de se realizará tan sólo en los casos que sean oportunos para salvaguardar la Política de Seguridad de la Información del Ayuntamiento. Será responsabilidad del centro gestor o servicio promotor de expedientes de contratación realizar esta difusión y vigilancia de su cumplimiento.

Una vez aprobada y publicada, el original firmado o el fichero correspondiente validado por firma electrónica, quedará bajo la custodia del responsable de Seguridad.

Décima. - Incumplimiento

El incumplimiento manifiesto por parte del personal laboral y funcionario del Ayuntamiento de Alcobendas de la Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

Undécima. - Gestión de documentación del SGSI

Todos los documentos que componen la documentación del Sistema de Gestión de Seguridad de la Información se gestionarán de acuerdo con lo descrito en el procedimiento de seguridad de gestión del SGSI.

BOCM-20260302-39

Duodécima. - Datos de carácter personal.

El Ayuntamiento de Alcobendas trata datos de carácter personal adecuados, pertinentes y no excesivos y sólo cuando se hallen en relación con el ámbito y las finalidades para los que se hayan obtenido. El Registro de Actividades de Tratamiento recoge las actividades de tratamiento y los responsables correspondientes.

El Ayuntamiento de Alcobendas debe evaluar los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado

El análisis de riesgos será reevaluado de forma periódica, contando con el asesoramiento y supervisión que realice el Delegado de Protección de Datos, y, en todo caso, cuando se detecte un tratamiento de alto riesgo, debiendo realizar, en su caso, una evaluación de impacto.

La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de datos personales.

Los sistemas de información del Ayuntamiento de Alcobendas (involucrados en servicios de administración electrónica) se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Registro.

Decimosegunda. - Gestión de riesgos

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

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal. La gestión de riesgos quedará documentada en el Informe de Análisis y gestión de riesgos.

Decimotercera. - Principios Básicos de la Seguridad

A continuación, se enuncian los principios básicos relacionados con la Seguridad de la Información, que rigen esta Política:

- Asegurar el punto más débil. La seguridad es una cadena, y dicha cadena es tan fuerte como su eslabón más débil. Un activo es tan seguro como su componente más débil.
- Defensa a fondo. Gestión de riesgos con distintas estrategias de seguridad, para el caso en que falle una de las capas de defensa o resulte inadecuada, otra capa prevenga la vulnerabilidad.
- Control de fallos. Los fallos son inevitables y se deben de tener en cuenta. Lo que sí se puede evitar son los problemas de seguridad causados por fallos. Es importante determinar exhaustivamente las causas de error que pueden afectar a un activo para que éste pueda ser recuperado ante cualquier eventualidad.

BOCM-20260302-39

- Asignación del mínimo privilegio. Se facilitará el mínimo acceso necesario para la realización de una operación, y únicamente el tiempo necesario. Cada usuario comprendido en el ámbito de aplicación de esta Política de Seguridad con derecho de acceso, así como las credenciales empleadas en los procesos deberán tener un conjunto de derechos de acceso mínimo y suficiente para desempeñar sus tareas.
- Separación de privilegios. Se minimizará el daño que se puede ocasionar a un activo mediante la división del activo en unidades más pequeñas, mientras se aísla el proceso mediante privilegios de seguridad.
- Simplicidad. La complejidad aumenta el riesgo de problemas. El diseño debe ser lo más directo posible. Diseños complejos no son fáciles de entender. Una topología compleja tiende a ser más difícil de mantener, y suele ser más propensa a tener errores.
- Practicidad vs complejidad. Los controles de seguridad deben ser fáciles de usar, de manera que sean realmente utilizados en la práctica y no evitados y falseados.
- Promover la privacidad. Se debe evitar cualquier hecho que pueda comprometer la privacidad de la información de los ciudadanos, actuando lo más diligentemente posible con cualquier tipo de información personal facilitada.
- Utilización y reutilización de componentes de confianza. Se debe promover la reutilización de componentes ya probados y consolidados. El uso repetitivo sin fallos promueve la confianza.
- Se recomienda “no reinventar la rueda” y, por defecto, se usarán los mecanismos de seguridad presentes en las propias aplicaciones (ejemplo: autenticación de servidores Web, algoritmos criptográficos, etc.).
- Principio de lectura hacia abajo. Las personas comprendidas en el ámbito de aplicación de esta Política de Seguridad que hayan sido autorizadas a acceder a información con un cierto nivel de clasificación deben ser autorizadas a acceder a información de más bajo nivel; aplicándose el criterio de “lectura hacia abajo”.
- Principio de necesidad de conocer. La autorización de acceso a la información estará basada en la “necesidad de conocer”. Se autorizará el acceso a información clasificada como no pública, estrictamente a la persona que necesite conocer dicha información.
- Auditabilidad. La realización de auditorías periódicas servirá al Ayuntamiento para mantener sus sistemas al día en cuestión de amenazas internas o externas.
- Control de activos. Por medio de pruebas específicas en los activos se medirá el grado de seguridad de estos. El control de los sistemas es un tema fundamental a la hora de implantar un ciclo de mejora continua.
- Colaboración. El acceso a los recursos, por parte de contratistas, está condicionado a la adhesión a la Política de Seguridad de la Información y a las Normativas asociadas existentes en el Ayuntamiento de Alcobendas, siendo estas de obligado cumplimiento.
- Seguridad por defecto. Los sistemas se configurarán de forma que sean seguros por defecto, es decir, de forma que los usuarios realicen un uso seguro, salvo que conscientemente reduzcan la seguridad o se expongan a riesgos.

Decimocuarta. - Política de uso aceptable

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición. Las políticas de uso aceptable se definen en la Normativa General de Utilización de los recursos y sistemas de información, así como en las Normativas particulares relacionadas.

Decimoquinta. - Gestión de activos

Es un objetivo primordial la protección de los activos de información del Ayuntamiento de Alcobendas. En adelante, por activo se entiende cualquier elemento con valor para el Ayuntamiento.

Todos los activos de información deberán tener un Propietario, siendo este en última instancia el responsable sobre el activo. Las tareas necesarias para adoptar las medidas de seguridad oportunas sobre los activos, así como la implantación de controles para protegerlos, podrán ser delegadas en el personal apropiado (personal técnico, por ejemplo).

BOCM-20260302-39

Deberá existir normativa específica que establezca las directrices sobre el uso apropiado de los activos.

Los activos de información deberán estar clasificados en función de los niveles establecidos en relación con la sensibilidad y criticidad de la información contenida, así como convenientemente identificados para su correcto manejo.

Decimosexta. - Seguridad Ligada a toda persona comprendida en el ámbito de aplicación de esta Política de Seguridad.

Es un objetivo del Ayuntamiento de Alcobendas garantizar que se conozcan las responsabilidades sobre la seguridad de la información a la que se tiene acceso, siendo conscientes de los riesgos potenciales, así como de los procedimientos de actuación adecuados para preservar la seguridad de la información.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente.

Se deberán implantar los controles necesarios que garanticen la seguridad en relación con la definición del trabajo y los procesos.

Dentro de la relación laboral o contractual, se deberán desempeñar siempre las funciones asignadas con profesionalidad, es decir, realizar un ejercicio adecuado de la profesión con capacidad y eficacia.

Se deberá impartir una adecuada formación en los procedimientos de seguridad y en el uso correcto de los servicios y procesos de información, concienciando de las amenazas y riesgos en el ámbito de la seguridad de la información.

Se tendrá que conocer los procedimientos para informar de los distintos tipos de incidentes que puedan tener impacto en la seguridad de los activos. Los incidentes que afecten a la seguridad de la información deberán ser comunicados por los canales adecuados establecidos, de forma rápida y fiable.

A la finalización de las funciones desempeñadas se debe aplicar un procedimiento gestionado y fiable que garantice la devolución de los activos y la revocación de los permisos de acceso que tuviera. La responsabilidad de su aplicación deberá estar determinada. Cuando se termine la relación laboral o contractual, se les retirarán los permisos de acceso a las instalaciones y la información, y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

En el caso de contratistas, la seguridad de la información deberá garantizarse y mantenerse mediante acuerdos o cláusulas en el contrato entre las partes, los cuales deberán contemplar los riesgos, los controles seguridad y los procedimientos para el uso de los Sistemas de Información del Ayuntamiento de Alcobendas.

Decimoséptima. - Seguridad Física y del Entorno

La información y los sistemas que la soportan, deberán ubicarse en áreas seguras adecuadamente protegidas de amenazas físicas o ambientales, ya sean estas intencionadas o accidentales. Será necesario establecer las suficientes garantías físicas de seguridad, a fin de reducir los riesgos de daños o pérdidas de datos.

Los sistemas o equipamiento de soporte a los procesos de información deberán estar protegidos razonablemente de potenciales amenazas del entorno (fuego, humedad, accidentes, etc.) y convenientemente de amenazas intencionadas (robo, copia, etc.).

Basado en un análisis de riesgos que atienda a la sensibilidad o criticidad de la información y los procesos que se llevan a cabo, se deberán proteger mediante controles más restrictivos aquellas zonas que presenten mayores riesgos (controles de acceso, protecciones ambiéntales, etc.). En cualquier caso, la protección suministrada deberá ser proporcional al riesgo y en función de la criticidad de la información.

Se deberán acometer las revisiones de mantenimiento requeridas por los equipos (aires acondicionados, suministros eléctricos, cableado, equipos, etc.).

Deberá existir una normativa específica en relación con el tratamiento de la información y los equipos fuera de las instalaciones. En cualquier caso, se deberán cumplir las mismas garantías de seguridad que aplican dentro de las dependencias del Ayuntamiento.

En cumplimiento de la ley de riesgos laborales, deberá existir un plan de emergencia y evacuación del edificio para riesgos que pongan en peligro la seguridad de las personas.

BOCM-20260302-39

Decimoctava. - Áreas seguras

El Ayuntamiento de Alcobendas tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las áreas restringidas de las instalaciones.

La totalidad de las instalaciones del Ayuntamiento de Alcobendas cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen.

Los lugares donde se ubican los servidores y el cableado estarán protegidos con sistemas de control de acceso y sólo tendrán acceso las personas autorizadas y los contratistas cuando vayan acompañados por alguien autorizado.

Las ventanas y puertas deberán permanecer cerradas cuando las instalaciones estén vacías.

Se prohíbe expresamente a todas las personas comprendidas en el ámbito de aplicación de esta Política de Seguridad comer y beber cerca de los servidores y equipos informáticos. Así mismo, se tendrá especial cuidado con el manejo de cualquier producto que pueda verterse sobre activos de información.

Para la prevención de fugas de agua e inundaciones será necesaria la revisión periódica de la grifería, sanitarios y demás instalaciones que puedan causar daños de este tipo.

Decimonovena. - Seguridad de los equipos

Los equipos informáticos son un activo importante del que depende la continuidad de las actividades, por lo que serán protegidos de manera adecuada y eficaz.

Los equipos informáticos del Ayuntamiento de Alcobendas están protegidos contra posibles fallos de energía u otras anomalías eléctricas, para ello se han instalado equipos de alimentación ininterrumpida.

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado de forma para que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información. Para ello deben someterse a las revisiones recomendadas por el suministrador. Sólo las personas debidamente autorizadas podrán acceder al equipo para proceder a su reparación. También será necesario adoptar las medidas de precaución necesarias en caso de los equipos deban abandonar las instalaciones para su mantenimiento.

La eliminación de equipos sólo se llevará a cabo por el Responsable de Seguridad o por la persona en quien éste delegue.

Vigésima. - Gestión de operaciones y comunicaciones

Se establecerá las responsabilidades y procedimientos para la gestión y operación de los sistemas de información e infraestructura tecnológica soporte del Ayuntamiento de Alcobendas, garantizándose la adecuada segregación de funciones que minimice el riesgo de comportamientos negligentes o malintencionados.

Los cambios sobre los sistemas y tecnologías de la información estarán identificados y aprobados de forma previa a su puesta en explotación. En este sentido, los entornos de desarrollo y/o prueba estarán separados del entorno productivo o real para evitar incidentes que puedan afectar a la integridad y/o disponibilidad de la información.

Se garantizará el cumplimiento de los requerimientos y niveles de servicio acordados con los contratistas del Ayuntamiento de Alcobendas, estableciendo mecanismos de monitorización, seguimiento o reporte periódicos.

La capacidad de los sistemas se adecuará a los requerimientos presentes, pero anticipándose a las expectativas de crecimiento, a fin de reducir los riesgos de sobrecarga de los sistemas, garantizar su disponibilidad y minimizar el riesgo de fallos.

Los sistemas de información considerarán la opción de registrar información asociada a actividades especialmente sensibles o realizadas por determinados usuarios. Estos logs o registros de auditoría podrán ser revisados de forma periódica para identificar problemas o incidentes de seguridad.

Vigesimoprimera. - Procedimientos operativos y responsabilidades

El Ayuntamiento de Alcobendas 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 del Ayuntamiento de Alcobendas y otras redes, los mecanismos adecuados de acceso y autenticación en el Sistema de Información para usuarios y equipos.

BOCM-20260302-39

Para evitar un uso malicioso de la red del Ayuntamiento de Alcobendas existirán mecanismos para cubrir 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.

Todas las personas comprendidas en el ámbito de aplicación de esta Política de Seguridad autorizadas 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.

Para asegurar la operación correcta y segura de los sistemas de información, se considerará la creación de Instrucciones Técnicas detallando las tareas a realizar.

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

Vigesimosegunda. - Protección frente a código malicioso y código móvil

Queda totalmente prohibida la instalación de otro software que no sea el permitido y necesario para el correcto desarrollo de las funciones encomendadas por el Ayuntamiento de Alcobendas.

Todo software adquirido por la organización sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias.

Cualquier software que requiera ser instalado para trabajar sobre la red deberá ser evaluado por el responsable del Sistema.

El responsable del Sistema velará por la correcta instalación de las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

Vigesimotercera. - Copias de seguridad

Los datos deben ser guardados en los servidores para asegurar que se realizan copias de seguridad habitualmente. Si la información se guarda en el disco duro de un PC, la persona comprendida en el ámbito de aplicación de esta Política de Seguridad asignada a dicho PC es la responsable de realizar las copias de seguridad.

Habrá procedimientos para la realización de copias de seguridad que se archivarán para recuperar los datos en caso de incidencia. Estas copias estarán claramente identificadas y se guardarán en sitio seguro.

También se desarrollarán procedimientos para recuperar los datos a partir de las copias de seguridad. Hay que asegurarse periódicamente de que la información se guarda correctamente y permite recuperar un nivel mínimo de servicio en caso necesario.

Si se corrompe la información en operación, hay que comprobar el software, el hardware y las comunicaciones implicadas antes de utilizar las copias de seguridad, para asegurarse de que no se pueda corromper la información contenida en ellas también.

Vigesimocuarta. - Gestión de la seguridad de la red

Se establecerán los controles necesarios para garantizar la seguridad de la información de las amenazas potenciales del uso de las redes de comunicaciones. Será necesaria una adecuada actividad de gestión de las redes, así como monitorización de la actividad registrada por los dispositivos.

Se controlará el intercambio de información y software entre organizaciones, siendo consecuentes con la legislación aplicable. Se deberán establecer procedimientos para proteger la información y los medios en tránsito considerando las implicaciones comerciales y de seguridad relacionadas con el intercambio electrónico de datos, considerando principalmente la necesidad de reducir los riesgos de seguridad creados por el comercio y el correo electrónicos.

BOCM-20260302-39

Los elementos de red (switch, router...) permanecerán fuera del acceso de personas no autorizadas para evitar usos malintencionados que puedan poner en peligro la seguridad del sistema. Se deberán implementar los medios y métodos necesarios para un mantenimiento adecuado de la red.

Vigesimoquinta. - Gestión de soportes

Deberá estar formalizada la gestión de los soportes de almacenamiento de información, de modo que se prevenga la divulgación, modificación, sustracción o eliminación no autorizada. Así, serán necesarios controles organizativos y de protección física para la gestión de los soportes.

Se aplicarán las mismas medidas de seguridad a los soportes que contengan información sensible que a los ficheros de donde han sido extraídos.

Los soportes (tanto papel como lógicos) que contengan información sensible deben permanecer en cajones o armarios cerrados bajo llave. Cuando cualquier persona comprendida en el ámbito de aplicación de estas Política de Seguridad deba utilizarla para realizar alguna gestión relacionada con las labores propias del Ayuntamiento de Alcobendas, ésta se hará responsable del buen cuidado de los soportes. No los dejará encima de su mesa cuando abandone su puesto de trabajo ni los colocará en cualquier otro lugar donde cualquier persona no autorizada pueda verlos o apropiarse de ellos.

Los soportes reutilizables cuya información ya no se necesite deberá borrarse, siempre que se cuente con la autorización precisa. Esta eliminación debe hacerse de forma segura para que los datos que contiene no se filtren a otras personas. Algunos procedimientos de destrucción que se consideran adecuados son la incineración, el triturado o vaciamiento de los soportes para uso posterior.

Siempre será necesario registrar la eliminación de soportes que contengan información sensible para mantener una pista de auditoría.

Vigesimosexta. - Intercambio de información

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, fax, etc.).

Vigesimoséptima. - Seguimiento

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.

Vigesimoctava. - Control de Acceso

Es un objetivo del Ayuntamiento de Alcobendas garantizar el adecuado control de acceso a la información y los recursos que la soportan.

Se deberán garantizar los adecuados niveles de control de acceso en las diferentes capas de acceso a la información (red, sistema operativo y aplicaciones), evitando así el acceso no autorizado. Los controles tendrán en cuenta, entre otros, las necesidades específicas de cada sistema, siendo el nivel de control coherente con la clasificación de la información gestionada; se hará uso de distintos perfiles de usuario que los sistemas operativos y aplicativos permitan y se tendrá en cuenta la segregación de funciones cuando se requiera; se seguirán los procedimientos de autorización, revocación y revisión de permisos y de gestión de contraseñas.

En relación con los accesos a través de redes, se deberán establecer controles específicos para garantizar que no se compromete la seguridad de la información, especialmente con la interconexión entre redes de otras organizaciones o redes públicas (Internet).

BOCM-20260302-39

Se deberá mantener un adecuado nivel de concienciación de las personas comprendidas en el ámbito de aplicación de esta Política de Seguridad en relación con sus responsabilidades acerca del mantenimiento de las medidas de control de acceso, particularmente en el uso de sus credenciales y en la seguridad de la información que manejan.

El uso de dispositivos móviles e instalaciones de trabajo remotas deberá disponer de las medidas necesarias para garantizar la seguridad de la información. La protección requerida será proporcional al riesgo que implique la modalidad del trabajo.

Se deberá monitorizar el adecuado funcionamiento de los controles implantados, mediante los reportes generados automáticamente, analizando los posibles accesos no autorizados y desviaciones respecto de la política de control de accesos.

Vigesimonovena. - Responsabilidades del usuario

Los puestos de trabajo deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado, así como otros posibles daños. Éstos deberían guardarse en espacios cerrados adecuados, especialmente fuera del horario laboral.

De igual forma, el usuario debe bloquear el equipo que tenga asignado cuando se va a ausentar de su puesto de trabajo de forma que sea necesario introducir una contraseña para acceder a los datos que se almacenan en el terminal.

También debe recordarse retirar los documentos de las impresoras de forma que se prevenga que puedan ser accedidos por personal no autorizado.

Trigésima. - Control de acceso a la red

No se permitirá el acceso a la red, a los sistemas, aplicaciones o información a personas que no estén formalmente autorizadas para ello.

En el caso de contratistas o de personas que desarrollen funciones para el Ayuntamiento de Alcobendas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con el Ayuntamiento de Alcobendas para mantener el mismo nivel de seguridad que si fueran personal laboral o funcionario del Ayuntamiento de Alcobendas.

El Área de Informática gestionará las altas y bajas de todos los usuarios de las aplicaciones o sistemas de administración electrónica.

Trigésima primera. - Desarrollo y Mantenimiento de los Sistemas

El Ayuntamiento de Alcobendas, consciente de la mayor eficiencia de los controles automáticos, tiene como objetivo estratégico la integración, dentro de las propias aplicaciones o sistema de información, de mecanismos de validación respecto a la exactitud y razonabilidad de los datos de entrada, correcto procesamiento de la información y realidad y regularidad de los resultados obtenidos. Cuando sea necesario, las aplicaciones incluirán medidas para la generación de pistas de auditoria o los registros de actividad necesarios.

Además, los sistemas de información estarán desarrollados de forma que prevengan la pérdida, modificación o acceso no autorizado de la información que almacenan y procesan. Estos requerimientos de seguridad se considerarán en el documento de diseño funcional de la aplicación y estarán basados en la necesidad de identificación y autenticación para acceder a los sistemas y en medidas de control de acceso que determinen el alcance de los privilegios. Además, por su especial importancia, el acceso al código fuente de la aplicación estará especialmente restringido.

En este sentido, se desarrollarán directrices esenciales para garantizar que la seguridad es incorporada en el desarrollo y mantenimiento de los sistemas, incluyendo las infraestructuras, aplicaciones y los desarrollos propios, mediante el análisis y especificación de requerimientos de seguridad, designando controles apropiados, a fin de prevenir pérdidas, modificación o usos no autorizados.

Por otra parte, en los entornos tecnológicos utilizados para el desarrollo de nuevos sistemas o el mantenimiento de las aplicaciones existentes se minimizará la información sensible o los datos reales con los que deberán de realizarse las pruebas.

Cuando una información sea crítica y tenga un alto riesgo, deberá usar sistemas y técnicas criptográficas para proteger la información, con el fin de proteger la confidencialidad, autenticidad e integridad de la información.

Por último, existirán procedimientos de control de cambios que permitan asegurar que las modificaciones a realizar sobre las aplicaciones están identificadas, se verifican para comprobar su correcto funcionamiento y son debidamente aprobadas.

BOCM-20260302-39

Trigésima segunda. - Informática Móvil y Teletrabajo

Debido a los problemas de inseguridad de Internet, no se debe transferir información por este medio de la organización a los domicilios particulares. En caso de teletrabajo, se solicitará autorización al Área de Informática para teletrabajar utilizando redes privadas virtuales (VPN). Antes de usar cualquier información hay que asegurarse de que el equipo en el que va a ser tratada está libre de virus o código malicioso.

Cuando los equipos o la información propiedad del Ayuntamiento de Alcobendas están fuera de las instalaciones, el responsable de su seguridad es quien los está utilizando y debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento.

Trigésima tercera. - Videoconferencias

La Normativa General de Utilización de Recursos y Sistemas de Información recoge pautas para garantizar que las reuniones online, mediante voz, vídeo o a través de servicios web, sean un espacio de trabajo eficaz y seguro, evitando incidentes que puedan llegar a constituir una brecha de seguridad. Cabe destacar que solo podrá utilizarse la herramienta corporativa aprobada por la Dirección General de Informática.

Trigésima cuarta. - Gestión de incidentes

La identificación de incidentes de seguridad que puedan afectar a la información y/o a los sistemas es considerada un instrumento efectivo que facilita la gestión de estos problemas o debilidades y puede prevenir su ocurrencia en el futuro.

En este sentido, se desarrollará e implantará un procedimiento formal que considere los mecanismos para la identificación y escalado de incidentes, permitiendo una respuesta apropiada.

Los incidentes se clasificarán en función de criterios que consideren su naturaleza y los planes de respuesta considerarán, al menos, el análisis para la identificación de la causa, la planificación de medidas correctivas para evitar su ocurrencia, la comunicación a aquellos que puedan verse afectados y la inclusión, en un registro, de la información relevante para la caracterización del incidente de seguridad.

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

Toda persona con acceso a los sistemas de información del Ayuntamiento tiene la responsabilidad de reportar mediante los canales adecuados cualquier incidente o indicio que haya podido detectar.

Trigésima quinta. - Continuidad de Servicio

Se establecerá un proceso de gestión de la continuidad de la operativa del Ayuntamiento de Alcobendas que permita la recuperación de los procesos y sistemas críticos. Con el fin de reducir el tiempo de indisponibilidad a niveles aceptables se combinarán controles de carácter organizativo, tecnológico y asociados a procedimientos, tanto preventivos como de recuperación.

En este sentido, estará disponible una infraestructura de respaldo (en una ubicación alternativa a la que, habitualmente, ubica los sistemas de información principales y considerando la problemática asociada a la conectividad y direccionamiento en la red de comunicaciones) que permita la recuperación de la operativa dentro de un marco temporal razonable a través de procedimientos, adecuadamente formalizados (incluyendo la asignación de responsabilidades), de invocación y recuperación.

Trigésima sexta. - Conformidad

El diseño, operación, uso y administración de los sistemas de información deberá estar sujeto a requisitos de seguridad legal, normativa y contractual. Se deberán impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

De esta manera se entiende que:

El Ayuntamiento de Alcobendas adquiere el compromiso de velar por el cumplimiento de la legislación vigente en materia de protección y seguridad de la información y de los sistemas de información, aplicable a todos sus procesos.

BOCM-20260302-39

El Ayuntamiento de Alcobendas y las personas comprendidas en el ámbito de aplicación de esta Política de Seguridad se comprometen al uso y tratamiento de los datos personales adoptando las precauciones necesarias para garantizar el nivel de seguridad exigido por el marco legal vigente en materia de Datos de Carácter Personal.

El Ayuntamiento de Alcobendas y las personas comprendidas en el ámbito de aplicación de esta Política de Seguridad se comprometen al uso y explotación de los servicios de información, adoptando las medidas necesarias para cumplir con la legislación vigente en materia de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Las personas comprendidas en el ámbito de aplicación de esta Política de Seguridad deberán cumplir todas sus obligaciones considerando en todo momento las directrices marcadas por el Ayuntamiento de Alcobendas con el fin de no incumplir la legislación, informando a los responsables a través de las vías reglamentarias.

Con el fin de evaluar y conseguir la conformidad de los sistemas con las políticas, normas de seguridad y requerimientos legales, se asignarán las responsabilidades oportunas para velar por el cumplimiento normativo en el Ayuntamiento de Alcobendas, de modo que se identifique la legislación aplicable y se realicen regularmente las revisiones y auditorias necesarias sobre los sistemas de información.

Se establecerán controles para salvaguardar los sistemas operativos y las herramientas de auditoria durante las auditorias del sistema.

Trigésima séptima. - Obligaciones de las personas comprendidas en el ámbito de aplicación de esta Política de Seguridad

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 de la Información disponer los medios necesarios para que la información llegue a los afectados.

Los precitados recibirán periódicamente concienciación en materia de seguridad TIC y formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

Trigésima octava. - Terceras partes, prestadores de servicios, proveedores de soluciones/productos

Cuando el Ayuntamiento de Alcobendas preste servicios a otros organismos, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando el Ayuntamiento de Alcobendas utilice servicios de terceros o ceda información a terceros, se hará partícipes a los contratistas de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dichos contratistas quedarán sujetos a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el contratista está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Se deberá desarrollar un procedimiento de seguridad en relación con la gestión de proveedores donde se documentarán las consideraciones en materia de seguridad de la información en cuanto a la adquisición de nuevos componentes, la contratación de proveedores y la gestión de dichos contratos.

Cuando la entidad adquiera, desarrolle o implante un sistema de Inteligencia Artificial de terceros, además de cumplir con lo establecido en la normativa vigente en la materia, así como política de uso de Inteligencia Artificial del Ayuntamiento, deberá contar con el informe del Responsable de Seguridad, que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Delegado de Protección de Datos emitir su parecer.

Trigésima novena. - Órgano Resolutor

El órgano resolutor superior competente para todos los ámbitos será la Alcaldía-Presidencia del Ayuntamiento de Alcobendas.

BOCM-20260302-39

DISPOSICIÓN DE APROBACIÓN Y ENTRADA EN VIGOR

La Política de Seguridad de la Información del Ayuntamiento de Alcobendas (en adelante PSI) tendrá validez en el momento de aprobación de la PSI y estará en vigor en tanto no se derogue la mencionada PSI.

Las sucesivas modificaciones a las funciones/tareas aquí descritas no requieren aprobación de una nueva PSI, serán aprobadas y entrarán en vigor a propuesta del Comité de Seguridad descrito en la PSI.

DISPOSICIÓN ADICIONAL- Organización y Gestión de la Seguridad

Comité: Composición, funciones y responsabilidades

El Comité de Seguridad de la Información lo presidirá la Alcaldía-Presidencia; o en su caso, el Concejal delegado competente en materia de seguridad de la información, con la asistencia como vicepresidente del director general de Informática. El secretario del Comité será el Responsable de Seguridad de la Informática o funcionario municipal en quien éste delegue, y tendrá como funciones:

- Proponer a la Presidencia la convocatoria que ésta haga de las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, asistido por los restantes miembros del Comité, que deberán aportar información puntual que se les demande para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de impulsar la ejecución directa o delegada de las decisiones del Comité.

El Comité de Seguridad de la Información estará integrado también por:

- Responsable de la Información, de los Servicios y las actividades de tratamiento de datos personales. Directores de las distintas Áreas del Ayuntamiento.
- Responsable de Seguridad.
- Responsable del Sistema y de la seguridad de actividades de tratamiento de datos personales. Jefe de Sistemas Informática.
- Delegado de Protección de Datos.

Las responsabilidades y funciones de los miembros del comité de seguridad de la información serán las descritas en la “Guía de Seguridad de las TIC CCN-STIC 801”, tal y como se encuentra definido en el artículo 2 del Real Decreto 311/2022, de 3 de mayo.

Según se indica en la Política de Seguridad de la Información del Ayuntamiento de Alcobendas, el Comité de Seguridad de la Información es un órgano que coordina la seguridad de la información en el Ayuntamiento de Alcobendas. A tal efecto, el Comité de Seguridad de la Información reportará al órgano superior competente y tendrá las siguientes funciones:

- Informar regularmente del estado de la seguridad de la información al órgano superior competente.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución del Ayuntamiento de Alcobendas en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por el Ayuntamiento de Alcobendas y recomendar posibles actuaciones respecto de ellos.

BOCM-20260302-39

- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información del Ayuntamiento de Alcobendas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en los proyectos TIC relacionados con la Administración electrónica desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC involucrados en servicios de Administración electrónica.
- Resolver conflictos de responsabilidad que puedan aparecer entre diferentes responsables, elevando los casos en los que no tenga suficiente autoridad para decidir.

Roles: Funciones y Responsabilidades

Responsable de Información, de los servicios y actividades de tratamiento de datos personales.

Los responsables de la Información, de los servicios y de las actividades de tratamiento de datos personales, en lo sucesivo responsable de la Información (information owner) serán las personas que ocupan el cargo de director/subdirector de cada área y se ocupan de velar por el buen uso de la información y, por tanto, de su protección; así como ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

El ENS asigna al 'responsable de la Información' la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información.

El responsable de la Información puede recabar una propuesta al responsable de Seguridad y conviene que se escuche la opinión del responsable del Sistema.

Establecer los requisitos del servicio en materia de seguridad, incluyendo requisitos de interoperabilidad, accesibilidad y disponibilidad.

Determinar los niveles de seguridad de los servicios. Puede recabar una propuesta al responsable de la Seguridad y conviene que se escuche la opinión del responsable del Sistema.

Responsable de Seguridad

Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.

Promover el mantenimiento de un inventario de activos y la asignación de responsabilidades sobre la protección de estos.

Promover la formación y concienciación en materia de seguridad de la información.

Además de las funciones descritas en el apartado "Segunda. -Tareas" de este anexo.

Responsable de velar por el cumplimiento de la normativa en materia de Seguridad de la Información y de la Seguridad de las actividades de tratamiento de datos personales.

Supervisar el Sistema de Información durante todo su ciclo de vida, sus especificaciones, instalación y verificación de su correcto funcionamiento.

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

Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

BOCM-20260302-39

Delegado de Protección de Datos.

Será responsabilidad del delegado de Protección de Datos y el Responsable del Tratamiento velar por el cumplimiento de la Normativa de Protección de Datos, en particular, el Reglamento Europeo de 2016/679 de 27 abril de 2016, así como cualquier otra legislación aplicable en el ámbito de datos de carácter personal que pueda surgir, siempre de acuerdo con lo dispuesto en el presente procedimiento.

Implantación de las normas contenidas en el RGPD relativas a cumplimiento de normas jurídicas y de tratamiento de datos.

Diseño e implantación de políticas de protección de datos y de medidas de seguridad adecuadas a los riesgos de los tratamientos.

Auditoría continua de protección de datos.

Implantación de programas de formación/sensibilización del personal sobre protección de datos.

Tareas:

RINFO – Responsable de la Información y de los Servicios.

RSEG – Responsable de la Seguridad.

RSIS – Responsable del Sistema.

DPD – Delegado de Protección de Datos.

TAREA	RESPONSABLE
Determinación de los niveles de seguridad requeridos en cada dimensión.	RINFO o el Comité de Seguridad de la Información.
Determinación de la categoría del sistema.	RSEG
Análisis de riesgos.	RSEG, DPD
Declaración de aplicabilidad.	RSEG
Medidas de seguridad adicionales.	RSEG
Configuración de seguridad.	Elabora y aplica: RSEG
Implantación de las medidas de seguridad.	RSEG
Aceptación del riesgo residual.	RINFO
Documentación de seguridad del sistema.	RSEG, DPD
Política de seguridad.	Elabora: Comité de Seguridad de la Información. Aprueba: Decreto de Alcaldía
Normativa de seguridad.	Elabora y aprueba: Comité de Seguridad de la Información.
Procedimientos de seguridad.	Elabora y aprueba: RSEG Aplica: RSEG
Estado de la seguridad del sistema.	RSEG
Planes de mejora de la seguridad.	Elabora: RSIS + RSEG + DPD Aprueba: Comité de Seguridad de la Información.
Planes de concienciación y formación.	Elabora: RSEG Aprueba: Comité de Seguridad de la Información.
Planes de continuidad.	Elabora: RSIS Valida: RSEG Coordina y aprueba: Comité de Seguridad de la Información Ejercicios: RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios.	Elabora: RSIS Aprueba: RSEG

En Alcobendas a 18 de febrero de 2026.—La alcaldesa-presidenta, Rocío García Alcántara.

(01/2.665/26)

BOCM-20260302-39