I. Principado de Asturias

• Anuncios

CONSEJERÍA DE EMPLEO, INDUSTRIA Y TURISMO

CONSORCIO ASTURIANO DE SERVICIOS TECNOLÓGICOS (CAST)

APROBACIÓN de la Política de Seguridad de la información del CAST.

Se hace público que la Junta General del CAST en la sesión celebrada el día 20 de octubre de 2017, acordó por unanimidad la aprobación de la Política de Seguridad de la Información del Consorcio Asturiano de Servicios Tecnológicos, cuyo texto se transcribe en el siguiente anexo.

Anexo

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL CAST

1.—*Introducción.*

El Consorcio Asturiano de Servicios Tecnológicos (CAST) es una entidad de derecho público de carácter asociativo, con personalidad jurídica propia independiente de la de sus miembros, con patrimonio y tesorería propio, administración autónoma y tan amplia capacidad jurídica como requiera la realización de sus fines. El objeto del Consorcio es servir como mecanismo para encauzar la acción de soporte y apoyo entre el Principado de Asturias y los concejos asturianos de menos de 20.000 habitantes para contribuir a la plena integración de éstos en la sociedad de la información y en el aprovechamiento eficiente de las nuevas tecnologías.

El ámbito de actuación del Consorcio será el de los ayuntamientos consorciados sin perjuicio de que pueda prestar servicio a otras entidades locales siempre previa firma de un convenio de colaboración en el que se indique el coste de los servicios a prestar.

Forman el Consorcio Asturiano de Servicios Tecnológicos el Principado de Asturias y los concejos asturianos de menos de 20.000 habitantes que a continuación se relacionan: Allande, Aller, Amieva, Belmonte de Miranda, Bimenes, Boal, Cabrales, Cabranes, Candamo, Cangas del Narcea, Cangas de Onís, Caravia, Carreño, Caso, Castropol, Coaña, Colunga, Corvera de Asturias, Cudillero, Degaña, El Franco, Gozón, Grado, Grandas de Salime, Ibias, Illano, Illas, Laviana, Lena, Valdés, Llanes, Morcín, Muros de Nalón, Nava, Navia, Noreña, Onís, Parres, Peñamellera Alta, Peñamellera Baja, Pesoz, Piloña, Ponga, Pravia, Proaza, Quirós, Las Regueras, Ribadedeva, Ribadesella, Ribera de Arriba, Riosa, Salas, San Martín del Rey Aurelio, San Martín de Oscos, Santa Eulalia de Oscos, San Tirso de Abres, Santo Adriano, Sariego, Sobrescobio, Somiedo, Soto del Barco, Tapia de Casariego, Taramundi, Teverga, Tineo, Vegadeo, Villanueva de Oscos, Villaviciosa, Villayón y Yernes y Tameza.

El CAST se constituyó para el cumplimiento de los siguientes fines:

a) La prestación de los servicios de administración electrónica.

b) La gestión de servicios comunes relacionados con la difusión y formación de nuevas tecnologías y en general el desarrollo de la sociedad de la información de cualquier ámbito. En particular se consideran fines del Consorcio todos aquellos relacionados con la administración electrónica, teleformación, teletrabajo, alfabetización digital, accesibilidad, sistemas de información territorial y el desarrollo de la cultura, el ocio y el turismo por medios digitales.

c) La prestación de servicios a los concejos consorciados de una manera integrada y coordinada, apoyándolos en servicios de carácter técnico y tecnológico.

d) El asesoramiento, la formación, la colaboración económica, técnica y administrativa a los concejos consorciados.

e) Cualquier otra actividad relacionada con las TIC que puedan establecer de mutuo acuerdo la Administración del Principado de Asturias y los concejos consorciados.

Para el desarrollo de los fines citados, el Consorcio realizará las siguientes actividades:

a) Gestionar los recursos compartidos por los entes consorciados en la materia objeto del Consorcio.

b) Realizar estudios y propuestas en materia de fomento de las tecnologías de la información y la comunicación (TIC).

c) Apoyo a la informatización, soporte técnico y funcional de usuarios/as de los entes consorciados.

d) Asesoramiento en los fines señalados a los entes consorciados.

Cód. 2017-11732

e) Realizar toda clase de certámenes, convenciones, jornadas técnicas, y cualquier otro evento relacionado con los fines señalados.

f) Cualesquiera otras que tengan relación con los fines.

Según lo anteriormente indicado, los fines del CAST están íntimamente ligados al desarrollo de la Administración Electrónica, lo que implica el tratamiento de gran cantidad de información por parte de los Sistemas de Tecnologías de la Información y de las Comunicaciones del CAST. De una parte de esta información el CAST no es el único responsable, pues en estos Sistemas se opera también con datos y con servicios de los ayuntamientos Consorciados y de otras Entidades a las que se pueda prestar servicio, pudiendo ser el CAST en estos casos encargado del tratamiento de datos personales y/o de la gestión de servicios comunes relacionados con la Administración Electrónica.

La Junta General del CAST es conocedora de los riesgos que pueden afectar a los sistemas de información del Consorcio, ya que la información está sometida a diferentes tipos de amenazas y de vulnerabilidades que pueden afectar a estos sistemas. Dichos Sistemas deben ser administrados con la suficiente diligencia y se deben de tomar las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, autenticidad, integridad, confidencialidad de la información tratada o de los servicios prestados.

Por otra parte, el Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiaran la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control y sin que la información pueda llegar a conocimiento de personas no autorizadas. 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 para detectar cualquier incidente y reaccionando con rapidez a los incidentes para recuperarse lo antes posible, acorde a lo establecido en el Artículo 7 del ENS.

2.—*Ámbito de aplicación.*

La presente Política se aplicará a los sistemas de información el CAST relacionados con sus competencias y que contribuyan a desarrollar el procedimiento administrativo y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con el CAST.

Todas las áreas del CAST deberán tener presente 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 todas las fases.

3.—*Objetivos en materia de seguridad de la información.*

El Consorcio Asturiano de Servicios Tecnológicos considera esencial que en el tratamiento de la información, en su almacenamiento y procesamiento, se garanticen los mayores niveles de seguridad y el máximo compromiso en su veracidad, disponibilidad y confidencialidad.

Igualmente el uso seguro y responsable de unos recursos que son corporativos, y en muchos casos compartidos, obliga a valorar la aplicación de medidas que contribuyan al mejor aprovechamiento tecnológico de los equipos, redes de comunicaciones, y aplicaciones y al desarrollo, cara al ciudadano, de una Administración electrónica eficaz y confiable.

Las medidas a tomar no pueden ser intuitivas o sobrevenidas sino bien calculadas, adaptadas a los niveles de riesgo asumidos, y correctamente procedimentadas, documentadas y aplicadas.

En materia de seguridad de la información se pretenden lograr los siguientes objetivos:

a. Establecer las bases de un modelo integral de gestión de la seguridad y los riesgos, que cubra en un ciclo de mejora continuo los aspectos técnicos, organizativos y procedimentales.

b. Implantar las más adecuadas medidas de seguridad física y lógica, desde una óptica técnica, normativa y organizativa para asegurar la integridad, confidencialidad y disponibilidad de los datos en el entorno específico del Consorcio Asturiano de Servicios Tecnológicos.

c. Garantizar a los usuarios de los sistemas TIC del Consorcio que sus equipos, recursos y datos están adecuadamente protegidos frente a cualquier tipo de acceso indebido o sustracción/manipulación de la información.

d. Concienciar a todos los niveles de la organización, sobre la necesidad de cumplir y hacer cumplir las normas relativas a la seguridad informática, tanto las emanadas desde esta Política de Seguridad como las generadas por normas y leyes de carácter estatal o supranacional.

e. Fomentar el conocimiento de la Política de Seguridad y de sus normas entre todos los usuarios, reiterando con la mayor frecuencia y de la forma más efectiva su contenido, sus implicaciones, y las causas que las justifican.

f. Convertir la seguridad en un eje transversal para la Organización y para sus sistemas de información de manera que junto al rendimiento y operatividad se valore la necesidad de aplicar y respetar restricciones de seguridad, especialmente cuando afecte a las garantías y derechos de trabajadores y usuarios.

g. Concienciar al conjunto de usuarios de la importancia de su participación y comportamiento para lograr la mejor protección y uso de la información y de los recursos corporativos, así como de la obligatoriedad en el cumplimiento de las normativas de seguridad.

h. Entender que la gestión de los riesgos y la imposición de una Política de Seguridad debe de hacerse desde una normativa clara, bien difundida, revisable periódicamente y estricta, pero a la par flexible ante circunstancias específicas y modelos tecnológicos y sociales cambiantes.

Cód. 2017-11732

i. Crear una Comisión Asesora sobre Seguridad de la Información, con capacidad para cooperar en el diseño de procedimientos operativos de seguridad y con los objetivos y funciones que determine la Junta de Administración del CAST. La composición y las funciones de dicha Comisión se deberán publicar en la Sede Electrónica del CAST y en el Portal de Transparencia, de acuerdo con lo indicado en el artículo 6 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

j. Auditar la calidad de la seguridad de los sistemas de información, fomentando la consecución de la Certificación de Conformidad con el Esquema Nacional de Seguridad.

k. Asegurar que los responsables de los diferentes roles relacionados con la Seguridad de la Información y la Protección de Datos de Carácter Personal cumplan con las competencias requeridas para obtener las certificaciones pertinentes.

4.—*Seguridad de la información. Fases.*

Para lograr los objetivos fijados en el apartado anterior, se adoptarán una serie de medidas encaminadas a conseguir un ciclo de mejora continua.

4.1.—Prevención.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, el CAST implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

Para garantizar el cumplimiento de la política, el CAST a través de los órganos competentes, según el caso:

— Autorizará los sistemas antes de entrar en operación.

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

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

4.2.—Detección.

El CAST establecerá controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuará en consecuencia según lo establecido en el Artículo 9 del ENS (reevaluación periódica). Cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 8 del ENS. Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

4.3.—Respuesta.

El CAST establecerá las siguientes medidas:

— Mecanismos para responder eficazmente a los incidentes de seguridad.

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

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

4.4.—Recuperación.

Para garantizar la disponibilidad de los servicios, el CAST dispondrá de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

5.—*Marco normativo.*

El marco normativo en que se desarrollan las actividades del CAST, y, en particular, la prestación de sus servicios electrónicos proporcionados la ciudadanía, está integrado por las siguientes normas:

— Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

— Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

— 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.

— Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

— Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

— Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Cód. 2017-11732

— Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

— Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

— Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.

— Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.

— Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

— Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

— Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

— Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

— Ley 59/2003, de 19 de diciembre, de firma electrónica.

— Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

— Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.

— Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

— 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.

— Texto refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre, y su normativa de desarrollo.

— Estatutos vigentes del Consorcio Asturiano de Servicios Tecnológicos.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del CAST derivadas de las anteriores comprendidas dentro del ámbito de aplicación de la presente Política.

6.—*Organización de la seguridad.*

Para la redacción de esta política de seguridad, se han tenido presentes las Guías del Centro Criptográfico Nacional (CCN-CERT), teniendo en cuenta que el Real Decreto 3/2010 promueve la elaboración y difusión de guías de seguridad de las TIC por parte del CCN-CERT para facilitar un mejor cumplimiento de los requisitos establecidos en el ENS.

La Guía de Seguridad CCN-STIC-801 crea un marco de referencia que establece las responsabilidades generales en la gestión de la seguridad de los sistemas de información y propone unas figuras o roles de seguridad que asuman dichas responsabilidades.

En la Guía se consideran tres estructuras de la organización de la seguridad en función de la dimensión de las mismas:

— Estructura mínima para los organismos de pequeña dimensión.

— Estructura intermedia para los organismos de dimensión intermedia.

— Estructura de máximos para grandes organizaciones.

Teniendo en cuenta la estructura de los órganos de gobierno del CAST fijada en el artículo 6 de sus Estatutos, así como la estructura administrativa, fijada en la relación de puestos de trabajo tanto de personal funcionario como laboral del CAST, se considera que el Consorcio es un organismo de dimensión intermedia.

6.1.—Estructura organizativa.

En el CAST los roles y responsabilidades identificadas en el ENS se reducen a tres roles (Dirección, Supervisión y Operación).

En cuanto a las funciones relacionadas con estos tres roles son las siguientes:

Dirección: una figura integrando las siguientes funciones:

— Responsable de la información.

— Responsable del servicio.

Supervisión: una figura reportando a Dirección.

— Responsable de seguridad.

Cód. 2017-11732

Operación: una figura reportando a Dirección, e integrando las funciones de:

— Responsable del sistema.

— Administrador de seguridad.

La estructura de la Organización en relación a la Seguridad de la Información en el CAST será la siguiente:

— Dirección: Junta de Administración del CAST.

— Supervisión: Dirección-Gerencia del CAST.

— Operación: Jefatura de Área de Gestión Municipal y Dinamización Tecnológica.

6.2.—Responsabilidades asociadas al Esquema Nacional de Seguridad.

6.2.1.—Responsabilidad general.

El artículo 12 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), establece que la seguridad deberá comprometer a todos los miembros de la organización. En este sentido, la preservación de la seguridad de los Sistemas de Información y el seguimiento de las normas específicas que desarrollarán esta Política, serán considerados objetivos comunes para todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con el CAST, especialmente para aquellos que participen en cualquier fase del tratamiento de la información o tengan acceso a los locales y Centros de Datos donde se custodie o se realice dicho tratamiento.

Las responsabilidades generales de los usuarios de los sistemas de información incluyen el uso correcto y coherente de los activos de tecnologías de la información y comunicaciones puestos a su disposición por el Consorcio Asturiano de Servicios Tecnológicos para el desarrollo de sus funciones, y la notificación de cualquier incidencia de seguridad de la que tengan conocimiento, todo ello respetando el principio de proporcionalidad y el deber de sigilo profesional.

6.2.2.—Responsabilidades particulares.

Adicionalmente a las responsabilidades generales indicadas, el Esquema Nacional de Seguridad y la normativa relacionada con la protección de datos personales identifican una serie de roles, a los cuales asignan unas responsabilidades particulares en materia de seguridad de la información. En relación al ENS las responsabilidades son las siguientes:

— El Responsable de la Información. En el marco del Esquema Nacional de Seguridad, es la persona, órgano o unidad administrativa que tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección. Es el propietario de los riesgos sobre la información y por consiguiente el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

  El Responsable de la información, al objeto de protegerla, tiene la potestad de determinar el nivel de seguridad requerido por la información de la cual es responsable atendiendo especialmente a los requisitos de integridad y confidencialidad.

— El Responsable del Servicio. Según el Esquema Nacional de Seguridad, es la persona, órgano o unidad administrativa que tiene la potestad de establecer los requisitos del servicio en materia de seguridad.

— El Responsable de Seguridad. En el marco del Esquema Nacional de Seguridad, el Responsable de Seguridad es la persona, órgano o unidad administrativa que define las medidas necesarias para garantizar la seguridad del sistema de información durante todo su ciclo de vida y vela porque los sistemas de información efectivamente responden a los requisitos de seguridad establecidos.

— El Responsable del Sistema ENS. En el marco del Esquema Nacional de Seguridad, es la persona, órgano o unidad administrativa encargada de implantar las medidas necesarias para garantizar la seguridad del sistema de información durante todo su ciclo de vida, siguiendo las recomendaciones del Comité de la Seguridad de la Información y notificando a éste cualquier cambio en el sistema que pueda suponer una alteración previsible en los riesgos que afectan a dicho sistema.

6.3.—Procedimientos de designación.

La designación de estructura de la Organización de la Seguridad de la Información del CAST está ligada a la los Órganos de Gobierno y de administración del CAST, por lo que los cambios de composición o de titularidad de los mismos no afecta a dichas designaciones. En el caso de modificación de los Estatutos o de la Relación de Puestos de Trabajo (RPT) del CAST que afecte a la estructura de la Organización en relación a la Seguridad de la Información en el CAST será competencia de la Junta General la fijación de la nueva estructura.

La designación de nuevos roles de Seguridad de la Información, en caso de ser necesario, pasará a ser responsabilidad del Presidente del CAST, dando cuenta a la Junta General del Consorcio y a la Junta de Administración del CAST.

6.4.—Resolución de conflictos.

Si hubiera conflicto entre los diferentes Responsables, en el caso de que una parte del conflicto sea el Responsable de la información o el Responsable del servicio será resuelto por la Junta General del Consorcio, caso contrario por la Junta de Administración.

Cód. 2017-11732

7.—*Datos de carácter personal.*

El CAST solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativa necesarias para el cumplimiento de la normativa de Protección de Datos:

1. Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

2. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

8.—*Concienciación y formación.*

El CAST desarrollará actividades específicas en materia de formación y concienciación de Seguridad de la Información así como sensibilización de los riesgos a los que están expuestos los Sistemas de Información, cuyos destinatarios deben ser todas las personas con responsabilidades asociadas al ENS.

No obstante, aunque la presente Política se aplicará a los sistemas de información el CAST y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con el CAST, en el caso de prestadores de Servicio, será responsabilidad de los mismos la formación y concienciación de sus empleados.

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

Desde el CAST se dispondrá de los medios necesarios para publicar, difundir y facilitar el conocimiento de esta política de seguridad así como de sus documentos de desarrollo.

9.—*Gestión de riesgos.*

Todos los sistemas afectados por esta Política estarán sujetos a un análisis periódico de riesgos con el objetivo de evaluar las amenazas a las que puedan estar expuestos.

El Responsable de Seguridad será el encargado de que se realice el análisis de riesgos y una vez identificadas las carencias y debilidades deberá tomar las medidas necesarias para minimizarlas hasta niveles aceptables.

El proceso de gestión de riesgos comprenderá las siguientes fases:

1. Categorización de los sistemas.

2. Análisis de riesgos.

3. Selección de medidas de seguridad a aplicar, que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

Se seguirá preferentemente la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información recomendada por el CCN-CERT.

10.—*Desarrollo de la política de seguridad de la información.*

Corresponde a la Junta de Administración, la revisión de la Política proponiendo, en caso de que sea necesario mejoras de la misma a la Junta General.

La Junta de Administración deberá aprobar y hacer públicos los programas y la planificación temporal del desarrollo de este reglamento.

10.1.—Documentos de seguridad.

Esta Política de seguridad será desarrollada por diversos documentos que aprobará la Junta de Administración tales como normas, protocolos, procedimientos, instrucciones técnicas, guías, estándares de seguridad, buenas prácticas. Estos documentos, en atención a su clasificación se difundirán o facilitarán a sus destinatarios, a través de un repositorio de documentos en que se fijarán diferentes niveles de acceso.

Todo ello adecuándolo a los medios materiales y personales del Consorcio.

10.2.—Herramientas de Ciberseguridad.

Se priorizará el uso de las herramientas que ponga a disposición al efecto el CCN-CERT para garantizar la seguridad de los sistemas y contribuyan a una mejor gestión de la ciberseguridad y permitan una mejor defensa frente a los ciberataques.

11.—*Terceras partes.*

Teniendo en cuenta que el CAST presta servicios a otras Entidades y que maneja como encargado de tratamiento información de las mismas, se deberá hacer partícipes de esta Política de Seguridad de la Información a dichas Entidades. Dicha participación se concreta en que cada Ayuntamiento tiene un representante en la Junta General y en que la mitad de los miembros de la Junta de Administración son representantes de Entidades Locales. Además se hará partícipes a estas Entidades por medio de la difusión de la Política así como de los documentos que la desarrollen indicados anteriormente.

Cód. 2017-11732

Además, se establecerán canales para el reporte y de coordinación con el Responsable de Seguridad de cada Entidad.

El mismo criterio indicado anteriormente, se deberá tener en cuenta en el caso de firma de Convenios de Colaboración en los que en virtud del mismo, el tercero deba o pueda acceder a datos responsabilidad del CAST.

El CAST para la consecución de sus fines celebra contratos administrativos con varias empresas por lo que dichas empresas en el ámbito de estos contratos tienen acceso a los Sistemas de Información del CAST que albergan información del Consorcio y de los Ayuntamientos y otros Entes a los que presta Servicio el CAST. Por lo tanto, será necesario velar porque durante todo el proceso de relación con estas empresas, incluyendo la elaboración de los Pliegos Administrativos y Técnicos, la celebración del contrato, la ejecución del mismo se tengan presentes los requisitos de esta política y de la normativa vigente en relación a la Seguridad de los Sistemas de Información. En este sentido, será requisito de solvencia técnica para la adjudicación de estos contratos que el servicio a contratar disponga del Certificado de Conformidad o de la Declaración de Conformidad con el ENS, según aplique en cada caso, de acuerdo a la valoración que de los Sistemas se realice por los responsables de los servicios que se prestan desde los Sistemas de Información del CAST.

Además el CAST realizará una adecuada supervisión y control de las actividades que hayan sido contratadas o convenidas, al objeto de minimizar los riesgos derivados de una gestión externalizada (incumplimientos, pérdida de control, limitaciones de acceso, dificultades para implantar cambios, etc.).

Disposición transitoria

A la vista de la entrada en vigor, el día 25 de mayo de 2018, del 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), se deberán ir adoptando las medidas oportunas a fin de que antes de tal fecha estén realizados el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos.

Disposición final

La presente política se publicara en el *Boletín Oficial del Principado de Asturias*, así como en la Sede Electrónica y en el Portal de Transparencia del CAST.

Entrará en vigor el día siguiente al de su publicación en el *Boletín Oficial del Principado de Asturias*.

En Oviedo, a 20 de octubre de 2017.—El Presidente del Consorcio Asturiano de Servicios Tecnológicos.—Cód. 2017-11732.

Cód. 2017-11732