Sección III. Otras disposiciones y actos administrativos

CONSEJO INSULAR DE EIVISSA

4211 ***Acuerdo del Consejo Ejecutivo del Consejo para la aprobación de la política de seguridad de las tecnologías de la información y las comunicaciones del Consell Insular d'Eivissa***

Por acuerdo del Consejo Ejecutivo Consejo Insular de Ibiza en sesión celebrada en fecha 24 de marzo de 2023, se ha aprobado por unanimidad la propuesta para la aprobación de la política de seguridad de las tecnologías de la información y las comunicaciones del Consell Insular d'Eivissa, del tenor literal siguiente:

"Atendido el Real Decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad (ENTE), que sustituye en el Real Decreto 3/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, el cual obliga al Consejo Insular de Ibiza a definir la política de seguridad en el ámbito de sus competencias para lograr los objetivos legales definidos al ENS.

Visto que el Esquema Nacional de Seguridad persigue los siguientes grandes objetivos:

- Crear las condiciones necesarias de seguridad en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes mediante estos medios.
- Definir las responsabilidades del personal del Consejo Insular de Ibiza
- Promover la gestión continuada de la seguridad.
- Promover la prevención, detección y corrección para una mejor resiliencia en el escenario de ciberamenaces y ciberataques.
- Promover un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios públicos digitales cuando participan varias entidades. Esto supone proporcionar los elementos comunes que tienen que guiar la actuación de las entidades del Sector Público y de sus proveedores tecnológicos en materia de seguridad de las tecnologías de la información.
- Servir de modelo de buenas prácticas, en línea con el apuntado a las recomendaciones de la OCDE Digital Security Risk Management for Economic and Social Prosperity OECD
- Recommendation and Companion Documento.

Vistos los artículos 11, 12 y 13 del RD 311/2022, donde se regula la diferenciación de las responsabilidades en materia de seguridad, así como el marco regulador de la política de seguridad que el Consejo Insular de Ibiza tiene que incorporar.

Atendida la propuesta del jefe de sección de Sistemas de Información y Seguridad de fecha 20 de marzo de 2023.

Por todo el anterior, en virtud de las facultades que tenc conferidas, por los Decretos de Presidencia de fecha 10 de julio de 2019 (publicados en el BOIB n.º 95 de 11 de julio de 2019) por el cual se regula la estructura orgánica del Consejo Insular de Ibiza, de fecha 16 de julio de 2019, por el que se determinan las atribuciones de los diferentes órganos de la Corporación (publicado en el BOIB n.º 98 de 17 de julio de 2019), elevo al Consejo Ejecutivo la siguiente,

PROPUESTA

Primero. Aprobar la política de seguridad de las tecnologías de la información y las comunicaciones del Consejo Insular de Ibiza, basada en el documento que se transcribe a continuación,

"Sumario

1. Introducción

El Consejo Insular de Ibiza depende de los sistemas TIC (Tecnologías de la Información y la Comunicación) para conseguir sus objetivos. Estos sistemas tienen que ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

El Esquema Nacional de Seguridad (ENS) tiene por objeto el establecimiento de los principios y requisitos de una política de seguridad en la utilización de los medios electrónicos que permita la adecuada protección de la información, a la vez que persigue fundamentar la confianza en que los sistemas prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control y sin que la información pueda llegar al conocimiento de personas no autorizadas.

La adaptación al ENS implica que el Consejo Insular de Ibiza y su personal tienen que aplicar las medidas mínimas de seguridad exigidas por este, 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 posibles incidentes que puedan surgir para garantizar la continuidad de los servicios prestados.

Los diferentes servicios de gestión del Consejo Insular de Ibiza tienen que asegurarse que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema.

2. La seguridad como proceso integral

La seguridad de la información es el resultado de un proceso que depende de todos y cada uno de los elementos humanos, técnicos, materiales y organizativos que intervienen en el tratamiento. Quienes participen en cualquier fase del tratamiento tendrán que responder, en la medida de sus responsabilidades, de la seguridad y buen uso de la información. De manera especial, tendrán que col•laborar en la prevención, detección y control de los riesgos derivados de actuaciones negligentes, ignorancia de las normas, fallos técnicos, de organización o de coordinación, o instrucciones inadecuadas.

El Consejo Insular de Ibiza, mediante los diversos agentes con responsabilidades específicas en materia de seguridad de la información, se encargará de proporcionar los canales de participación adecuados que hagan efectiva la colaboración mencionada en el párrafo anterior. Del mismo modo, se encargará de mantener permanentemente informados a todos los destinatarios de esta política, del propósito de la misma, así como de los documentos que la desarrollan y de los canales de participación habilitados.

El proceso de gestión de la seguridad de la información tendrá que estar sometido a monitorización, control y mejora continuos para confirmar su eficiencia ante la constante evolución de los riesgos y de los sistemas de protección

2.1. Prevención

El Consejo Insular de Ibiza tiene que evitar o, al menos, prevenir en la medida que sea posible que la información o los servicios se vean perjudicados por incidentes de seguridad. Para lo cual, se tienen que implementar 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 así como los roles y responsabilidades de seguridad de todo el personal tienen que estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, la organización tiene que:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Suele licitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se tiene que monitorizar l'operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, según el establecido en el artículo 9 del ENS.

La monitorización es especialmente relevando cuando se establecen líneas de defensa de acuerdo con el artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y repuerto que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. Respuesta

El Consejo Insular de Ibiza tiene que:

- Establecer mecanismos para responder de manera eficaz a los incidentes de seguridad.
- Designar puntos de contacto por las comunicaciones en relación a incidentes detectado a áreas de la entidad o a otros organismos relacionados con el Consejo Insular de Ibiza.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en los dos sentidos, con los Equipos de Respuesta a Emergencias (CERT) reconocidos a nivel nacional como Iris-CERT, CCN-CERT y otros equivalentes.

2.4. Recuperación

Para restaurar la disponibilidad de los servicios, se tendrán que desarrollar planes de contingencia de los sistemas TIC que incluyan actividades de recuperación de la información que contribuyan a la continuidad del servicio.

3. Alcance

El Consejo Insular de Ibiza aplicará la presente Política de Seguridad sobre aquellos sistemas que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

4. Marc normativo

El marco normativo que afecta al desarrollo de las actividades y competencias del Consejo

Insular de Ibiza está constituido por normas jurídicas estatales y autonómicas, si procede, orientadas a la administración electrónica, a la seguridad de la información y los servicios que la manejan, así como a la protección de datos de naturaleza personal.

Las normas que constituyen este marco se encuentran recogidas en un registro creado a tal efecto, el cual se mantiene actualizado según señala el correspondiente procedimiento de gestión de requisitos legales.

También podrán formar parte de este marco, aquellas normas aplicables a la Administración Electrónica del Consejo que se hayan desarrollado a partir de las anteriores o estén relacionadas, pudiendo ser adicionalmente publicadas a las sedes electrónicas comprendidas dentro del ámbito de aplicación de esta Política.

5. Misión y objetivos

El Consejo Insular de Ibiza, para la gestión de sus intereses y de las funciones y competencias que tiene encomendadas, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población.

Por este motivo, pose a disposición de la misma la realización de trámites en línea con el objetivo de impulsar la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la eficacia de la acción pública. Se pretende potenciar, por otro lado, el uso de las nuevas tecnologías en el Consejo y entre la propia ciudadanía.

Los principales objetivos que se persiguen, entre otros, son: fomentar la relación electrónica de la ciudadanía con el Consejo y crear la confianza necesaria entre ciudadano y Consejo.

6. Organización de la seguridad

Pueden distinguirse tres niveles al organigrama del Consejo Insular de Ibiza:

- Nivel 1 – Órganos de Gobierno: alta dirección que entiende la misión de la organización, determina los objetivos que se propone conseguir y responde que se consigan.
  Este nivel corresponde a la figura del **Responsable de la Información ENS**, que asumirá la presidencia de la Corporación y que podrá delegar en el consejero ejecutivo responsable del área TIC, junto con el **Comité de Seguridad de la Información** como órgano consultivo, asistidos por todas las direcciones de Área del Consejo.
- Nivel 2 – Dirección Ejecutiva: responsables de los servicios que entienden qué hace cada unidad de gestión y como las diferentes unidades se coordinan entre ellas para conseguir los objetivos marcados por la Dirección.
  Este nivel corresponde a la figura del **Responsable de la Seguridad y el Responsable de los Servicios**.
- Nivel 3 – Operacional que se centra en una actividad concreta y controla como se hacen las cosas.
  Este nivel corresponde a la figura del **Responsable de los Sistemas de Información**, asistido por los responsables de sistema delegados y por los administradores de la seguridad del sistema que se nombren.

Siguiendo el mismo esquema y, de acuerdo con el ENS, se estructura un organigrama de seguridad en el Consejo Insular de Ibiza en tres niveles:

- Nivel 1:
  - -Comité de Gestión y Coordinación de la Seguridad de la Información.
  - -Responsable de la Información ENS.
- Nivel 2:
  - -Responsable de la Seguridad de la Información.
  - -Responsable del Servicio.
- Nivel 3:
  - -Técnico de Seguridad de los Sistemas.
  - -Responsables de los Sistemas de Información.

La especificación de requisitos de seguridad (Nivel 1) corresponde a los responsables de la información y de los servicios. La operación (nivel 3) corresponde a los responsables de los sistemas, mientras que la supervisión corresponde al responsable de la seguridad (nivel 2) y al técnico de seguridad (nivel 3).

Por encima de todos ellos existe el Comité de Coordinación y Gestión de la Seguridad (nivel 1).

6.1. Comité de Gestión y Coordinación de la Seguridad de la Información

El Comité de Gestión y Coordinación de la Seguridad de la Información, de ahora en adelante Comité de Seguridad, coordina la seguridad de la información a nivel de organización.

De acuerdo con el ENS, las funciones indicadas que corresponden al Comité de Seguridad son:

- Elaborar (y revisar periódicamente) la Política de Seguridad de la información para que sea aprobada por el responsable de la información.
- Aprobar y divulgar los procedimientos de seguridad del Consejo Insular de Ibiza.
- Promover la mejora continua de la gestión de la seguridad de la información del Consejo Insular de Ibiza.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos sean consistentes, alineados con la estrategia decidida en la materia y evitar duplicidades.
- Evaluar los principales riesgos residuales asumidos por el Consejo Insular de Ibiza y recomendar posibles actuaciones respecto a ellos.
- Evaluar el cumplimiento de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto a 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 las auditorías periódicas y evaluar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Priorizar las actuaciones en materia de seguridad de acuerdo con los recursos disponibles.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en marcha. En particular, se tendrá que velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y soporten un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas del Consejo Insular de Ibiza, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Evaluar las necesidades de recursos requeridos para el cumplimiento de los planes de actuación derivados de la aplicación de la Política de Seguridad.
- Elaborar un informe anual del estado de la seguridad de los sistemas de información.

El Comité de Seguridad estará formado por las personas titulares, o aquellas en que deleguen, de los siguientes cargos:

- Presidente: El Responsable de la información.
- Vocales:
  - El Delegado de Protección de Datos del Consejo Insular de Ibiza.
  - El Responsable de los servicios ENS.
  - El Responsable de Seguridad de la Información, actuando también como Secretar del Comité.
  - El Responsable de los Sistemas de Información.

A requerimiento del presidente, podrán incorporarse a los trabajos y sesiones del Comité otros miembros del Consejo, incluidos grupos de trabajo especializados, ya sean estos de carácter interno, externo o mixto.

El Comité de Seguridad no es un comité técnico, pero recaudará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones. El Comité de Seguridad se asesorará en los temas sobre los cuales tenga que decidir o emitir una opinión.

La Secretaría del Comité lo asume el Responsable de la Seguridad de la Información, al cual como tal le corresponde:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar a las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.
- El comité de seguridad se reunirá con carácter ordinario dos veces en el año y, con carácter extraordinario por acuerdo de la Presidencia, a iniciativa propia o previa solicitud motivada de uno de sus miembros.

6.2. Responsable de la Información

El Responsable de la Información establecerá los requisitos sobre la información proporcionada por medios electrónicos a través de los servicios del Consejo Insular de Ibiza y, por lo tanto, tendrá la último palabra en la hora de decidir el tipo de información accesible y el uso que se le pueda dar, en virtud de la reglamentación vigente y de las buenas prácticas en materia de Protección de Datos.

Le corresponden las siguientes funciones:

- Establecimiento de los requisitos de la información en materia de seguridad.
- Trabajo en colaboración con el responsable de seguridad y los responsables de los sistemas en el mantenimiento de los sistemas catalogados segundos el Anexo Y del Esquema Nacional de Seguridad.

El Responsable de la Información será el presidente del Consejo Insular de Ibiza que podrá delegar en el consejero responsable de los servicios TIC.

6.3. Responsable del Servicio.

El Responsable del Servicio establecerá los requisitos de seguridad aplicables a los servicios proporcionados por el Consejo Insular de Ibiza a través de medios electrónicos y, en este sentido, tendrá como funciones:

- Establecimiento de los requisitos de los servicios TIC en materia de seguridad.
- Trabajo en colaboración con el Responsable de Seguridad y los responsables de los sistemas donde se englobe/n el/s servicio/s para el mantenimiento de los sistemas catalogados segundos el Anexo Y del Esquema Nacional de Seguridad.

Será ejercido por el **Secretario** del Consejo Insular de Ibiza, sin prejuicio que se designen responsables delegados, los cuales podrán ser convocados al Comité de Seguridad de la información con voz pero sin voto.

6.4. Responsable de Seguridad de la Información

El Responsable de Seguridad de la Información del Consejo Insular de Ibiza tiene por funciones las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC.
- Promover la formación y concienciación de la seguridad de la información dentro de su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Aprobar toda la documentación relacionada con la seguridad de los sistemas.
- Verificar los informes de motorización y auditoría de los estados de seguridad de los sistemas.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.

- Elaborar el informe periódico de seguridad para el Comité de Seguridad incluyendo los incidentes más relevantes del periodo a informar.
- Aprobación de los procedimientos de seguridad elaborados por los responsables de los sistemas cuando, en virtud del contenido, no requiera la aprobación del Comité de Seguridad.
- Proponer la redacción de aquella normativa de seguridad del Consejo Insular de Ibiza que considere necesario formalizar.
- Determinar la categorización de los sistemas y los requisitos de seguridad con carácter previo a la puesta en marcha de un nuevo servicio vinculado al ENTE.
- Será desarrollado por el **jefe de sección de los Sistemas de Información y Seguridad** del Consejo Insular de Ibiza

6.5. Responsable de los Sistemas de información

El Responsable de los Sistemas de Información tiene por funciones:

- Velar por el correcto funcionamiento del sistema durante todo su ciclo de vida, de sus especificaciones e instalación, incorporando los requisitos de seguridad necesarios para la operativa en el sistema.
- Definir la tipología y política de gestión del sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el sistema.
- Proponer al Responsable de Seguridad los cambios que afecten a la seguridad del sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del sistema en las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del sistema y asegurarse que estas se integren adecuadamente en el marco general de seguridad.
- Determinar los requisitos de la configuración autorizada del hardware y software a utilizar en el sistema, en aquello que afecte a su seguridad.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema que afecte a la seguridad y disponibilidad del servicio.
- Llevar a cabo el preceptivo proceso de revisión periódica del análisis y gestión de riesgos en el sistema.
- Elaborar y aprobar la documentación de seguridad del sistema.
- Delimitar las actuaciones que afecten a la Política de Seguridad de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del sistema.
- Investigar los incidentes de seguridad que afecten al sistema y, en su caso, comunicarlo al Responsable de Seguridad o a quién este determine.
- Establecer planes de contingencia y emergencia.
- Además, el responsable del sistema puede acordar la suspensión del manejo de una información determinada o la prestación de un servicio determinado si es informado de graves deficiencias de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión tiene que ser acordada con los responsables de la información afectada, del servicio afectado y con el Responsable de Seguridad, antes de ser ejecutada.

6.6. Delegado de Protección de Datos

El Delegado de Protección de Datos será único para todos los servicios que presta la entidad.

Esta figura tiene que estar registrada a lo Agencia Española de Protección de Datos.

Las funciones del Delegado de Protección de Datos serán las indicadas al mencionado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y otras disposiciones reguladoras de la materia.

6.7. Procedimientos de designación

El desarrollo de las responsabilidades definidas en esta Política de Seguridad venderá determinada por el acceso a los diferentes cargos que se han vinculado a ellas. En el supuesto de que desapareciera o cambiara de denominación de alguno de estos cargos será competencia del Consejo Insular de Ibiza asignar el nuevo lugar al que quedará vinculada la figura.

7. Datos de carácter personal

El Consejo Insular de Ibiza realiza tratamientos en los que hace uso de datos de carácter personal sometidas al que se dispone en el 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 aquello que respeta al tratamiento de datos personales y en conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

Las políticas de seguridad aplicables a los tratamientos se rigen por las medidas de seguridad implantadas de acuerdo con el Anexo II

(Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Seguridad al ámbito de la Administración Electrónica. Al RAT (Registro de actividades del tratamiento, del sistema de gestión de la privacidad) se indexan los diferentes tratamientos de datos afectados por la normativa.

Todos los sistemas de información del Consejo Insular de Ibiza se ajustarán a los niveles de seguridad requeridos por la normativa por la naturaleza y finalidad de los datos de carácter personal.

8. Gestión de riesgos

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

- Regularmente, al menos una vez en el año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando tenga lugar un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

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

9. Desarrollo de la Política de Seguridad

Esta Política se desarrollará por medio de una **Normativa de Seguridad** que afronte aspectos específicos. La Normativa de Seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular, por aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Otros documentos que complementan esta Política de Seguridad son:

- La normativa de seguridad, la cual estará disponible a la intranet del Consejo Insular de Ibiza.

10. Obligaciones del personal

Todos los miembros del Consejo Insular de Ibiza tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a las personas afectadas, teniendo siempre en cuenta las disponibilidades presupuestarias del Consejo Insular de Ibiza.

Todos los trabajadores y trabajadoras del Consejo Insular de Ibiza, bajo el alcance del ENTE, atenderán a una acción de concienciación en materia de seguridad TIC, al menos una vez cada dos años. Se establecerá un programa de acciones en concienciación continua para atender a todos los miembros del Consejo Insular de Ibiza relacionados con servicios de administración electrónica, en particular a los de nueva incorporación, teniendo en cuenta siempre las disponibilidades presupuestarias del Consejo Insular de Ibiza. Se realizará una acción de concienciación durante los dos años siguientes a la aprobación de esta Política de Seguridad y, de manera continuada, para el personal de nueva incorporación.

En su caso, si se requiere formación específica por el manejo seguro de los sistemas, las personas con responsabilidad en la operación o administración de sistemas TIC la recibirán en la medida en que la necesiten para realizar su tarea.

11. Terceras partes

Cuando el Consejo Insular de Ibiza preste servicios a otros organismos o maneje información otros organismos, se los hará partícipe de esta Política de Seguridad de la Información. Por eso, se establecerán canales por información y coordinación de los respectivos Comités de Seguridad del ENS y se establecerán procedimientos de actuación ante posibles incidentes de seguridad.

Cuando el Consejo Insular de Ibiza utilice servicios de terceros o ceda información a terceros, se los hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que implique a los mencionados servicios o información. Esta tercera parte quedará sujeto a las obligaciones establecidas a la mencionada normativa, teniéndose que incorporar a los pliegos y encomiendas del Consejo Insular de Ibiza. De este modo, el proveedor tendrá que garantizar que su personal está adecuadamente formado en materia de seguridad de acuerdo con los requerimientos del Consejo Insular de Ibiza.

12. Entrada en vigor

Esta Política de Seguridad de la Información es efectiva desde el día siguiente al de su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

El Consejo Insular de Ibiza dispondrá de los medios para publicar, dar a conocer y facilitar el cumplimiento de esta política y de los documentos que la desarrollan, así como para verificar su aplicación y efectividad. Así mismo, habilitará canales de participación que permitan a los destinatarios de esta política y de los documentos complementarios, participar en su revisión y mejora.

Anexo A. Glosario de términos

- Análisis de riesgos: Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.
- Datos de carácter personal: Cualquier información que se refiere a personas físicas identificadas o identificables.
- Gestión de incidentes: Plan de acción para atender a las incidencias que se den. Además de resolverlas tiene que incorporar medidas de desarrollo que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en problemas grandes. ENS.
- Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización respecto a los riesgos. ENS.
- Incidente de seguridad: Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información. ENS.
- Información: Caso concreto de cierto tipo de información.
- Política de seguridad: Conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos. ENS.
- Principios básicos de seguridad: Cimientos que tienen que regir toda acción orientada a asegurar la información y los servicios. ENS.
- Responsable de la información: Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.
- Responsable de la seguridad: Persona que determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Responsable del servicio: Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.
- Responsable del sistema: Persona que se encarga de la explotación del sistema de información.
- Servicio: Función o prestación desarrollada por alguna entidad oficial destinada a cuidar los intereses o satisfacer las necesidades de los ciudadanos.
- Sistema de información: Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Anexo B. Abreviaturas

- CCN: Centro Criptològic Nacional
- CIERTO: Computer Emergency Reaction Team
- ENTE: Esquema Nacional de Seguridad
- STIC: Seguridad Tecnologías de la Información y las Comunicaciones
- TIC: Tecnologías de la Información y las Comunicaciones”

Segundo. Publicar este acuerdo en el boletín oficial de las Islas Baleares.

Tercero. Comunicarlo a los diferentes responsables."

Eivissa, 4 de mayo de 2023

El jefe de servicio de Transportes
Antonio Montero Guasch