

| | | |
|---|--|--|
| DOCUMENTO Otros: 2022.MC.12_Memoria justificativa | IDENTIFICADORES | |
| OTROS DATOS Código para validación: FCPIS-PNTPJ-LYM5W Página 1 de 2 | FIRMAS El documento ha sido firmado o aprobado por : 1.- BEATRIZ DURAN HERNANDEZ, Gerente, de IASS. Firmado 10/05/2022 11:49 | ESTADO FIRMADO 10/05/2022 11:49 |



Esta es una copia impresa del documento electrónico. El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://www.iass.es/verificador



GERENCIA

MEMORIA JUSTIFICATIVA

Nos encontramos en una etapa de transformación digital que impacta toda nuestra actividad, tanto la personal como la empresarial, desde la forma en la que nos comunicamos y trabajamos hasta la manera en cómo tomamos decisiones. Esta revolución trae aparejados nuevos retos que debemos afrontar. Si toda la información y las comunicaciones están digitalizadas, es un deber y obligación proteger tanto los datos como las vías de transmisión utilizadas, y el no hacerlo puede tener un impacto muy elevado para la sociedad desde todos los puntos de vista, el derecho a la privacidad de la información, a la honra y el buen nombre, derechos de propiedad intelectual, entre tantos otros. Las administraciones públicas gestionan datos de los ciudadanos a los que sirven, y en un elevado porcentaje, son datos de carácter personal, por lo que se exige que dispongan y apliquen las medidas necesarias para su protección y seguridad.

Las medidas necesarias para fortalecer la ciberseguridad han crecido, lógicamente, de manera proporcional a la evolución de este proceso de digitalización, que junto con el procesamiento automático de los servicios y las capacidades de interconexión han elevado el riesgo y el aumento de ciberataques. Si, además, acompañamos esta nueva época digital con factores adicionales, como el conflicto bélico actual, el peligro aumenta. A diferencia de otros enfrentamientos previos, el actual contempla la ciberguerra. De hecho, la OTAN ha definido el ciberespacio como un dominio bélico e incluso ha reconocido que un impacto significativo de un ataque cibernético mal intencionado puede ser considerado, en situaciones particulares, un ataque armado.

Una herramienta de apoyo al cumplimiento de la seguridad de la información es la aplicación de la normativa vigente en la materia. Tanto el Reglamento de Protección de Datos como el Esquema Nacional de Seguridad son de obligado cumplimiento y proporcionan instrucciones, instrumentos y metodología para facilitar esta labor de custodia y protección.

El Cabildo Insular de Tenerife (CIT) y el Centro Criptológico Nacional del Centro Nacional de Inteligencia (CCN-CNI) han suscrito con fecha 28 de octubre de 2020 un Convenio de Colaboración en materia de ciberseguridad que tiene por objeto fijar los términos y el alcance de la colaboración entre el CIT y el CNI-CCN en el ámbito de la gestión y prevención de la seguridad de los sistemas, servicios y redes TIC de la Administración. Dicho Convenio, en su cláusula PRIMERA contempla la posibilidad de extender el ámbito subjetivo a los entes del Sector Público Insular dependientes del Cabildo Insular de Tenerife, conforme al procedimiento de adhesión previsto en su cláusula SEXTA.

Trasladado al ECIT el interés del IASS en incorporarse al citado convenio, para afianzar y mejorar las medidas de seguridad actualmente implantadas, así como para fortalecer la aplicación de normativa vigente, y reunida la Comisión de Seguimiento del citado Convenio, el pasado 11 de marzo de 2022, en los términos expuestos en la cláusula SEXTA del mismo, se ha aprobado la incorporación del IASS al Convenio de referencia.

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE22e00020043323

CSV

GEISER-2dc9-f171-2e17-4995-a88b-6789-18e8-e25d

DIRECCIÓN DE VALIDACIÓN

https://sede.administracionespublicas.gob.es/valida

FECHA Y HORA DEL DOCUMENTO

23/05/2022 09:09:05 Horario insular

Validez del documento

Copia Electrónica Auténtica





Esta es una copia impresa del documento electrónico. El documento está FIRMADO. Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://www.iasa.es/verificador

| | | |
|--|--|--|
| DOCUMENTO Otros: 2022.MC.12_Memoria justificativa | IDENTIFICADORES | |
| OTROS DATOS Código para validación: FCPIS-PNTPJ-LYM5W Página 2 de 2 | FIRMAS El documento ha sido firmado o aprobado por : 1.- BEATRIZ DURAN HERNANDEZ, Gerente, de IASS. Firmado 10/05/2022 11:49 | ESTADO FIRMADO 10/05/2022 11:49 |

El alcance del acuerdo de colaboración contempla dos líneas de trabajo principal, cuyos hitos se distribuirán durante su período de vigencia actual, esto es, durante 3 años:

1. La adecuación al Esquema Nacional de Seguridad, generando los procedimientos, auditorías de certificación y documentación necesarios, así como recibiendo la colaboración necesaria para la implementación de dichos procedimientos y configuraciones. El objetivo en una primera fase será la certificación del IASS en nivel MEDIO, y a partir de ahí, continuar la fase de evolución continua que permita una total adecuación a la normativa en el menor plazo de tiempo.
2. Implantación y mantenimiento del funcionamiento de un Centro Virtual de Operaciones de Ciberseguridad (vSOC), con cobertura sobre los servicios y usuarios de sistemas de información del IASS

Los costes que se deriven de la incorporación del IASS al Convenio de referencia, con el alcance indicado en el Anexo I del documento de adhesión, será financiado por el IASS, y los mismos tendrán el carácter de costes de compensación para resarcir los gastos al CNI-CCN que genera la actuación de colaboración consistente en la implementación y funcionamiento del Centro Virtual de Operaciones de Ciberseguridad (vSOC), y para asumir la sostenibilidad funcional y técnica del mismo, así como la asistencia y apoyo específico en las tareas de adecuación al Esquema Nacional de Seguridad. La distribución anual del gasto sería la siguiente:

- 2022 (Año 1): 80.000 €
- 2023 (Año 2): 100.000 €
- 2024 (Año 3): 100.000 €
- El importe anual para una posible prórroga del Convenio será también de 100.000 €.

Para la tramitación del citado gasto, en el Presupuesto actual de este Organismo no existe crédito a nivel de vinculación jurídica en la aplicación presupuestaria 2022.4A.231.421.11, por lo que se hace necesaria la habilitación de la misma para el presente ejercicio,

Santa Cruz de Tenerife a, fecha de firma electrónica.

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE22e00020043323

CSV

GEISER-2dc9-f171-2e17-4995-a88b-6789-18e8-e25d

DIRECCIÓN DE VALIDACIÓN

https://sede.administracionespublicas.gob.es/valida

FECHA Y HORA DEL DOCUMENTO

23/05/2022 09:09:05 Horario insular

Validez del documento

Copia Electrónica Auténtica

