POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA, F.S.P. (FECYT)

El Esquema Nacional de Seguridad (ENS) está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, y entre ellas las entidades del sector público, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ámbito de sus competencias.

En el ámbito del ENS la Política de Seguridad de la Información de FECYT recoge la postura de la Fundación en cuanto a la seguridad de la información y establece los criterios generales en cuanto a seguridad que deben regir su actividad, especialmente la relacionada con la administración electrónica, tanto desde el punto de vista de los usuarios de los servicios, como desde el punto de vista interno de la gestión de la propia Fundación.

- ✓ La FECYT mantiene un compromiso prioritario con la seguridad de la Información para toda la organización, a la vez que quiere satisfacer determinadas necesidades de los agentes del Sistema Español de Ciencia, Tecnología e Innovación.

- ✓ La FECYT utiliza las tecnologías de la información y las comunicaciones para prestar sus servicios, por lo que es consciente de que estos sistemas deben estar administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información tratada o a los servicios prestados.

- ✓ La política de FECYT es la de contrarrestar las amenazas mencionadas anteriormente con los medios suficientes, teniendo en cuenta su disponibilidad presupuestaria. Para este fin, se establecerá una estructura de seguridad, junto con los mecanismos apropiados para su gestión, y un conjunto de instrumentos de apoyo de forma que se garantice:
  - El cumplimiento de los objetivos de su misión y de prestación de servicios.
  - El cumplimiento de la legislación y la normativa aplicables.

  Para ello,
  - Se preverán y desplegarán medidas para evitar incidentes de seguridad que pudieran afectar al cumplimiento de objetivos o poner en riesgo la información.
  - Se diseñarán medidas de respuesta ante incidentes de seguridad, física o lógica, de forma que se minimice el impacto de los mismos, en caso de que ocurrieran.

- ✓ Como norma general, el análisis de riesgos será la base a la hora de diseñar las medidas de seguridad necesarias, poniendo más foco y esfuerzo en la mitigación de lo que suponga un mayor riesgo.

- ✓ Las distintas áreas bajo cuya responsabilidad se encuentran los servicios prestados deberá contemplar la seguridad desde el mismo momento en que se concibe un nuevo sistema o servicio, aplicando para estos y para los ya existentes, las medidas de seguridad prescritas por el ENS para garantizar la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad de los servicios y de la información.

- ✓ Los requisitos de seguridad de los sistemas, las necesidades de formación de los usuarios, administradores y operadores y las necesidades de financiación deben ser identificados e incluidos en la planificación de los sistemas y en los pliegos de prescripciones utilizados para la realización de proyectos que involucren a las TIC.

- ✓ Se deben articular mecanismos de prevención, reacción y recuperación con objeto de minimizar el impacto de los incidentes de seguridad.

- ✓ En cuanto a la prevención, se debe evitar que los servicios y la información resulten afectados por un incidente de seguridad. Para ello FECYT implementará las medidas de seguridad establecidas en el Anexo II del ENS, así como aquellas medidas adicionales que pudieran ser identificadas en el proceso de análisis de riesgos.

- ✓ En cuanto a la reacción, se establecerán mecanismos de detección, comunicación y gestión de incidentes de seguridad, de forma que cualquier incidente pueda ser tratado en el menor plazo posible. Siempre que sea posible, se detectarán de forma automática los incidentes de seguridad, utilizando elementos de monitorización de los servicios o de detección de anomalías y poniendo en marcha los procedimientos de respuesta al incidente en el menor plazo posible. Para los incidentes detectados por los usuarios, ya sean internos o externos, se establecerán los pertinentes canales de comunicación de incidentes.

- ✓ En cuanto a la recuperación, para aquellos servicios que se consideren críticos, en base a la valoración que de los mismos realicen sus responsables, se deberán desarrollar planes que permitan la continuidad de dichos servicios en el caso de que, a raíz de un incidente de seguridad, quedaran indisponibles.

En una primera fase el alcance de la Política de Seguridad de FECYT comprenderá los siguientes servicios prestados por la Fundación:

- Convocatorias de ayudas públicas.
- Currículum Vitae Normalizado (CVN).
- Canal de infracciones.

La organización de la seguridad de la información está basada en la siguiente estructura:

A. Estructura de supervisión, que es la encargada de verificar la correcta implantación y operación de los requisitos de seguridad establecidos, de cara a mantener la alineación con los objetivos y de cumplir con las normas y legislación aplicable.
   Forman parte de la estructura de supervisión:
   - La Dirección General.
   - El Responsable de Seguridad de la Información.
   - El Comité de Seguridad de la Información.
   - Los Responsables de la Información y del Servicio.

B. Estructura de operación, que debe asumir la administración operativa de la seguridad de los sistemas de información, implantando en dichos sistemas las medidas necesarias para satisfacer los requisitos de seguridad establecidos por la estructura de especificación.
   Forman parte de la estructura de operación:
   - El Responsable del Sistema de Información.
   - El Responsable de Infraestructura IT.
   - El Responsable de la seguridad física.
   - Los usuarios de los sistemas.

Formación y concienciación:
Anualmente se realizará al menos una acción de formación y concienciación en materia de seguridad, con el doble objetivo de, por un lado, mantener informado al personal sobre los procedimientos existentes en seguridad, riesgos, medidas de protección, planes de protección, etc., y, por otro lado, concienciar, en general, de la importancia de la seguridad y de los procedimientos básicos de manejo e intercambio de información.

Gestión de riesgos:
Los servicios e infraestructuras bajo el alcance de la Política de Seguridad deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos.
Como metodología base para la realización de los análisis de riesgos se utilizará Magerit, siendo esta metodología la más recomendable para el sector público estatal. Se utilizará, como punto de partida, el catálogo de amenazas de seguridad previsto en la metodología.
El análisis se realizará: (i) regularmente, una vez al año; (ii) cuando haya cambios significativos en la información manejada; (iii) cuando haya cambios en los servicios esenciales prestados o

cambios significativos en las infraestructuras que los soportan; (iv) cuando ocurra un incidente grave de seguridad; y (v) cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de seguridad implantadas.

Datos de carácter personal:

La FECYT en su política de protección de datos mantiene un compromiso de cumplimiento de la legislación vigente en materia de tratamiento de datos personales con el objeto de garantizar que el tratamiento de los datos de carácter personal se realiza conforme al Reglamento (UE) 2016/679 General de Protección de Datos (RGPD), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), así como la jurisprudencia existente en materia de protección de datos de carácter personal, y de los informes y resoluciones de la Agencia Española de Protección de Datos (AEPD).

La FECYT aplicará medidas de seguridad para garantizar el derecho fundamental a la protección de datos garantizando la confidencialidad, la integridad y la disponibilidad de los datos personales. Para garantizar estos tres factores de la seguridad la FECYT aplicará las medidas de seguridad necesarias adecuadas al nivel de los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas conforme al artículo 32 del RGPD.

En relación con las medidas de seguridad en el ámbito del sector público, la FECYT cumplirá con la disposición adicional primera de la LOPDGDD, que se señala que los responsables enumerados en el artículo 77.1 de la citada ley orgánica, entre los que se encuentran las fundaciones del sector público como la FECYT, deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

La FECYT dispondrá de un Registro de Actividades del Tratamiento de datos de carácter personal que incluirá los contenidos regulados en el artículo 30 del RGPD y lo hará público en su portal de transparencia en aplicación del artículo 31.2 de la LOPDGDD.

Desarrollo de la Política de Seguridad:

Esta Política de Seguridad de la Información se desarrollará mediante la elaboración de otras políticas o normativas de seguridad que aborden aspectos específicos. A raíz de dichas políticas y normativas se podrán desarrollar procedimientos que describan la forma de llevarlas a cabo.

La documentación de políticas y normativas de seguridad, así como esta Política de Seguridad de la Información se encontrará a disposición de todo el personal de la Fundación que necesite conocerla y, en particular, el personal que utilice, opere o administre los sistemas de información y comunicaciones o la información misma albergada en dichos sistemas o los servicios prestados por FECYT.