



## **POLÍTICA DE USO DE MEDIOS TECNOLÓGICOS Y SEGURIDAD DE LA INFORMACIÓN**



## 1. FINALIDAD

El Patronato de la Fundación de la Comunitat Valenciana Centro de Estudios Ambientales del Mediterráneo ha aprobado en su sesión de fecha 12 de diciembre de 2024 la presente Política de Seguridad de la Información (en adelante, también la **“Política”**), que establece los principios y directrices con los que la FUNDACIÓN DE LA COMUNITAT VALENCIANA CENTRO DE ESTUDIOS AMBIENTALES DEL MEDITERRÁNEO (CEAM) (en adelante, también la **CEAM**) protegerá su información, de conformidad con la normativa aplicable y con sus valores éticos, definidos en el Código de Conducta y Prácticas Responsables (en adelante, el **“Código de Conducta”**) y en otra normativa interna que resulte de aplicación.

**FUNDACIÓN CENTRO DE ESTUDIOS AMBIENTALES DEL MEDITERRÁNEO (CEAM)** velará por la protección de la información, independientemente de la forma en la que esta se comunique, comparta, proyecte o almacene esta (en adelante, la **“Información”**). Esta protección afecta tanto a la información existente dentro de la entidad como a la información compartida con terceros.

A los efectos de la presente Política, se definen los Sistemas de la Información como el conjunto de tecnologías o medios tecnológicos, propios o de terceros que gestionen, almacenen o transmitan Información.

## 2. ÁMBITO DE APLICACIÓN.

La presente Política se aplicará a la entidad, y vinculará a todo su personal, independientemente de la posición y función que desempeñe. Igualmente, podría hacerse extensiva, total o parcialmente, a cualquier otra persona física y/o jurídica vinculada con la entidad por cualquier relación cuando ello sea posible por la naturaleza de esta y resulte conveniente para el cumplimiento de la finalidad de aquella.

De conformidad con la Política, **CEAM**, podrá desarrollar procedimientos e instrucciones para implementar y dar cumplimiento a las obligaciones asumidas, así como para adaptar la misma a las diversas legislaciones.

Asimismo, la aplicación de esta Política es complementaria a otras normas internas de obligado cumplimiento.

## 3. OBJETIVOS

La presente Política constituye y tiene los siguientes objetivos:

- Garantizar el grado de confidencialidad necesario a cada clase de Información.
- Mantener la integridad de la información, de modo que no sufra alteraciones con respecto al momento en que haya sido generada.

- Asegurar la disponibilidad de la Información, en todos los soportes y siempre que sea necesaria, asegurando la continuidad del negocio y el cumplimiento de cuantas obligaciones sean exigibles.

#### 4. PRINCIPIOS GENERALES

La consecución de los objetivos descritos en el apartado anterior se articula a través de los siguientes **principios generales**:

- Clasificación de la Información. Se clasificará en función de su valor e importancia para la entidad, de forma que las medidas de protección se adecúen al nivel de clasificación de cada activo de información.
- Uso de los Sistemas de la Información. Estará limitado a fines lícitos y exclusivamente profesionales, para la realización de tareas relacionadas con el puesto de trabajo, no pudiendo ser destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.
- Retención de la Información. Se establecerán, cuando resulte necesario o conveniente, períodos de retención de la Información por categorías atendiendo a las necesidades operativas o de cumplimiento regulatorio, así como los correspondientes procedimientos de destrucción de la información.
- Acceso a la Información por parte de terceros. Se desarrollarán los procedimientos de control de puesta a disposición y acceso por terceros a la información relativa a CEAM.
- Seguridad de la Información en los Sistemas. Los entornos de desarrollo y producción se mantendrán en sistemas independientes. Igualmente, el desarrollo y mantenimiento de los Sistemas de la Información deben incluir los controles y registros necesarios para garantizar la correcta implementación de las especificaciones de seguridad.
- Continuidad. Se establecerá un proceso de gestión de continuidad que permita garantizar la recuperación de la información de la compañía en caso de accidente, reduciendo el tiempo de indisponibilidad a niveles aceptables.
- Cumplimiento. Los Sistemas de Información y comunicaciones deberán estar adecuados de forma permanente a las exigencias de la legislación vigente en todas las jurisdicciones en la que opera, así como la normativa interna de desarrollo que resulte de aplicación.

#### 5. RESPONSABILIDADES

La responsabilidad de la protección de la Información y de los Sistemas que la tratan, almacenan, transmiten o se extienden a todos los niveles organizativos y funcionales de CEAM, como se detalla a continuación:

##### 5.1 Responsabilidades del personal



Todo el personal de la entidad deberá asumir y cumplir la Política, así como la normativa interna de seguridad y de los sistemas vigentes, estando obligados a mantener el secreto profesional y la confidencialidad de la Información manejada en su entorno de trabajo.

Igualmente tienen la obligación de comunicar con carácter de urgencia y según los procedimientos establecidos, las posibles incidencias o problemas de seguridad que se detecten.

El personal que contrate servicios de terceros que impliquen el uso o acceso de estos últimos a la información, deberán entender los riesgos derivados del proceso de externalización y asegurar una gestión eficaz de los mismos.

El uso de los servicios digitales por parte del personal, incluyendo el correo electrónico y los servicios de mensajería instantánea, estará limitado a fines exclusivamente profesionales. En consecuencia, estos medios y sistemas no están destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.

## **5.2 Responsabilidades en relación con proveedores y otros terceros**

Los contratos con terceros (por ejemplo, Contratos de prestación de servicios o Contratos de externalización) que impliquen el uso o acceso de estos a la información, deberán incluir requerimientos específicos de seguridad relativos a la tecnología y las actividades de aquellos que llevan a cabo dichos servicios.

En este sentido, dichos contratos deberán incluir provisiones mediante las que garantice que los proveedores, el personal subcontratado o cualquier empresa externa que utilice o acceda a la Información de la entidad, conocen y cumplen con la Política en lo que les sea de aplicación, estando obligados a mantener el secreto profesional y la confidencialidad de la Información.

## **5.3 Seguridad de la Información**

El Departamento de Informática, o servicio externo ejercerá su función de control de manera independiente y en su responsabilidad implementar esta Política. Por ello, es responsable de:

- Implementar una estrategia de seguridad de la Información que vele por el cumplimiento de los principios básicos de esta política.
- Establecer y revisar los controles correspondientes para asegurar el cumplimiento de esta Política y su normativa de desarrollo.
- Prevenir, detectar y responder ante cualquier incidente en materia de Seguridad de la Información.
- Revisar, actualizar y comunicar cualquier cambio que derive en modificaciones sustanciales de esta Política.
- Realizar actividades de formación en materia de los procesos de Seguridad de la Información.



- Velar por el cumplimiento con la legislación vigente en el ámbito de las competencias que le atribuye la presente Política.

## **6. IMPLEMENTACIÓN**

FUNDACIÓN DE LA COMUNITAT VALENCIANA CENTRO DE ESTUDIOS AMBIENTALES DEL MEDITERRÁNEO (CEAM) se compromete a asignar recursos específicos para asegurar la implementación efectiva de la Política.

## **7. COMUNICACIÓN DE LA POLÍTICA**

La presente Política estará disponible en la intraweb de CEAM para todo el personal. Asimismo, la Política será objeto de las adecuadas acciones de comunicación, formación y sensibilización para su oportuna comprensión y puesta en práctica.

## **8. ACTUALIZACIÓN Y REVISIÓN DE LA POLÍTICA**

La Política sería revisada y actualizada cuando proceda, con el fin de adaptarla a los cambios que puedan surgir en el modelo de negocio en el contexto donde opere la compañía, garantizando en todo momento su efectiva implantación.