



PUIG

Política de seguridad de la información



Contexto	4
Propósito y ámbito	4
Principios y acciones derivados de esta política	5
Principios	5
Acciones	5
Alcance y responsabilidades	7
Aprobación, publicación y revisión	7





Contexto

El Código Ético de **Puig** considera los datos o activos de la información un bien cuya obtención y tratamiento debe limitarse a las necesidades propias del desarrollo de las actividades legítimas de la empresa, promoviendo un marco proactivo para su debida protección.

Propósito y ámbito

Esta Política, desarrolla los compromisos plasmados en el Código Ético de **Puig** y define los principios y acciones que configuran el marco para el tratamiento, gestión y la seguridad de los datos o activos de la información. Los datos o activos de la información son cualquier tipo de recurso que contenga información necesaria para el desarrollo del negocio, con independencia del soporte, canal o forma en que se comunique, transmita, comparta, proyecte o almacene, sea interno o externo y la titularidad de **Puig** o de terceros.

El propósito de esta política es dotar a **Puig** de un marco de protección de los datos o activos de la información para preservar su confidencialidad, integridad, disponibilidad y garantizar el cumplimiento de la normativa aplicable relacionada con la seguridad de la información.

Esta Política ha sido aprobada por el Consejo de Administración de **Puig** Brands, S.A. y se aplica a todas las compañías y actividades de **Puig**¹.

Esta Política es el marco genérico que define los principios y las acciones a desarrollar por los responsables de los datos y activos de la información de las distintas áreas funcionales.

Las distintas divisiones y unidades de negocio de **Puig** pueden desarrollar esta Política a través de otras regulaciones de ámbito divisional o local que cumplan con las disposiciones de esta Política.

¹ “Puig” hace referencia a la sociedad **Puig** Brands, S.A. y sus filiales y cualquier otra entidad jurídica que pueda constituirse en el futuro, respecto de la cual **Puig** Brands, S.A. ostente o pueda ostentar (directa o indirectamente) el control, de conformidad con el artículo 42 del Código de Comercio español.



Principios y acciones derivados de esta política

Principios

Esta Política se fundamenta en los siguientes principios:

- **Protección del negocio**, priorizando la protección de la información que afecta directamente a la operativa de negocio, la innovación y la mejora continua de nuestra actividad.
- **Gestión de riesgos**, adoptando medidas que permitan identificar los riesgos existentes y evitar aquellos que resulten innecesarios o excesivos en la gestión de la información.

Acciones

Para cumplir con los objetivos y principios establecidos, se prevén las siguientes acciones:

- **Clasificación de la información**: todos los activos de información deben ser identificados y clasificados en términos de valor, requisitos legales, confidencialidad, sensibilidad y criticidad para la organización. Los propietarios de los activos son responsables de asegurar que estén adecuadamente clasificados y protegidos de acuerdo a la siguiente clasificación en función de la ley y las buenas prácticas, su impacto en el negocio, en la imagen, en los socios o en las personas vinculadas a Puig:
 - **Highly Confidential (altamente confidencial)**: información de importancia estratégica que puede causar un impacto severo o irreparable y cuyo acceso está limitado a un grupo muy reducido de personas.
 - **Confidential (confidencial)**: información que puede causar un serio impacto y cuyo acceso está limitado a un grupo concreto de personas, áreas específicas o parte de ellas.
 - **Internal (interna)**: es aquella información que puede causar un impacto limitado y está disponible de forma general para todo o gran parte de las personas aunque no puede ser divulgada públicamente.



- **Public (pública):** información que es de dominio público o que se pone a disposición para su distribución pública a través de un canal de Puig y que puede ser consultada libremente.
- **Gestión de la seguridad de la información:** se garantiza un nivel de protección, control y manejo adecuado de los activos de información de Puig.
- **Gestión de incidentes:** se establecen procedimientos para la gestión de incidentes de seguridad de la información que incluyen su notificación, respuesta y recuperación.
- **Control de identidades:** el ciclo de vida de las identidades, así como las cuentas asociadas a cada una de ellas, deben ser controlado y gestionado de forma adecuada.
- **Control de accesos:** el acceso a la información debe ser controlado y restringido a personas autorizadas, debiendo revisarse los derechos de acceso de forma regular para asegurar que son adecuados.
- **Continuidad del negocio:** ante eventuales interrupciones o disfunciones de la operativa del negocio, se desarrollan con carácter previo planes que garanticen su continuidad, protegiendo, manteniendo y recuperando la información.
- **Formación y concienciación:** se implementan aquellas acciones de formación y concienciación que garanticen la seguridad de la información por parte los usuarios.
- **Cumplimiento:** se garantiza el cumplimiento de la normativa aplicable en materia de seguridad de la información.
- **Revisión y mejora continua:** se llevarán a cabo las auditorías y actividades regulares de revisión para evaluar la eficacia de la política y las prácticas de seguridad de la información.

Puig garantiza los principios, acciones y metodología recogidos en esta Política a través de los recursos materiales, tecnológicos, financieros y humanos necesarios.



Alcance y responsabilidades

Esta Política resulta de obligado cumplimiento a cualquier persona física o jurídica que tenga acceso a datos o activos de la información de **Puig**, debiéndose promover su cumplimiento por todas las partes interesadas.

El incumplimiento de esta Política puede determinar la adopción de medidas disciplinarias, así como cualquier otra consecuencia legalmente prevista.

Aprobación, publicación y revisión

Esta Política ha sido aprobada por el Consejo de Administración de **Puig** el 5 de abril de 2024, entrando en vigor a partir de ese momento.

La responsabilidad de la publicación, comunicación y revisión de esta Política está asignada al Área de Seguridad de la Información y Ciberseguridad en coordinación con el Área Legal.