Grupo SICOR

El Corte Inglés

# POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN

**Aprobada por el Consejo de Administración de El Corte Inglés el 25 de noviembre de 2020**

# Índice

## 1. Introducción

El Consejo de Administración de El Corte Inglés, S.A. tiene atribuida la responsabilidad de formular la Estrategia y las Políticas Corporativas del Grupo de Empresas El Corte Inglés (GRUPO ECI), así como de aprobar los programas y sistemas de cumplimiento y control interno.

Para el Grupo ECI la información, en cualquiera de los formatos disponibles (información física, ficheros electrónicos, etc.), es un activo estratégico que requiere una adecuada protección, contribuyendo a la competitividad, al cumplimiento de la legalidad vigente y a la buena imagen comercial. Es por ello que, con el objeto de establecer los principios generales que deben regir el tratamiento de la información en todas las Empresas del Grupo ECI, el Consejo de Administración, por y como consecuencia de la propuesta de la Comisión de Auditoría y Control, ha aprobado la siguiente Política Corporativa de Seguridad de la Información del Grupo ECI, en adelante PCSI.

## 2. Objeto

La PCSI tiene por objeto garantizar una protección adecuada de la información, con independencia del formato en el que se presente, de modo tal que las Empresas del Grupo ECI estén preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad en esta materia.

El Grupo ECI se compromete a implantar las medidas técnicas y organizativas necesarias para que la información, independientemente del formato en el que se presente, esté suficientemente protegida contra cualquier amenaza con potencial para incidir en su confidencialidad, integridad y disponibilidad.



C/ Marqués de Mondéjar 16, posterior.
28028 Madrid - T. 91 354 12 92

## 3. Ámbito de aplicación y órganos intervinientes

Para la implantación de la PCSI, el Comité de Seguridad de la Información desarrollará la normativa interna de gestión global de seguridad de la información en función de la importancia relativa de la misma para el Grupo ECI.

La PCSI, así como la normativa interna que la desarrolle, será supervisada por el Comité de Seguridad de la Información y será de aplicación a todas las empresas del Grupo ECI, a sus administradores, directivos y empleados, así como a todas las personas que se relacionen con las empresas pertenecientes al Grupo ECI.

Por otra parte, los profesionales, órganos internos y/o comités que asuman estas funciones en cada uno de los ámbitos en los que el Grupo ECI opera, con la preceptiva intervención del Comité de Seguridad de la Información, establecerán los procedimientos internos de carácter específico que apliquen los principios establecidos en la PCSI, adaptando su contenido en función de la normativa aplicable.

El Comité de Seguridad de la Información será el responsable de velar por que las prácticas y los procedimientos internos del Grupo ECI y sus empresas sean conformes con la regulación en materia de seguridad de la información que resulte aplicable en cada momento, debiendo difundir e informar de las novedades normativas que se publiquen y entren en vigor.

En virtud de esta Política Corporativa, en sus normativas y procedimientos de desarrollo se definirán unas medidas de seguridad que se aplicarán, según se determine en dichas normas, a todos los servicios, sistemas y demás recursos del Grupo de Empresas ECI, con el fin de garantizar el cumplimiento de la normativa interna de gestión global de seguridad de la información, manteniendo dichos



C/ Marqués de Mondéjar 16, posterior.
28028 Madrid - T. 91 354 12 92

desarrollos puntualmente actualizados.

Como soporte a las actividades del Comité de Seguridad de la Información, las distintas áreas y departamentos deberán, además de colaborar con el Comité:

- Designar a los coordinadores de la seguridad de la información en su ámbito. Dichas personas actuarán de acuerdo con las directrices del Comité de Seguridad de la Información.
- Informar sobre la existencia y/o la creación de cualquier fichero y/o base de datos con información que deban ser protegidos, con independencia de quién haya generado la información.

## 4. Principios de seguridad del tratamiento de la información

Los principios por los que se rige la PCSI son los siguientes:

### 4.1 Principios generales:

1. Las Empresas del Grupo ECI cumplirán con la legislación en materia de seguridad y protección de la información, aplicable en aquellos países en los que opera.
2. El Comité de Seguridad de la Información velará por el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información del Grupo ECI, independientemente del formato que tenga la información.
3. El Grupo ECI propiciará que los principios recogidos en la PCSI sean tenidos en cuenta: i) durante el diseño e implantación de los procedimientos establecidos para el Grupo ECI y sus empresas, ii) en los



C/ Marqués de Mondéjar 16, posterior.
28028 Madrid - T. 91 354 12 92

productos y servicios ofrecidos por el Grupo ECI y sus empresas, iii) en todos los contratos y obligaciones que se formalicen o se asuman por el Grupo ECI y sus empresas; y iv) en la implantación de los sistemas y plataformas que permitan el acceso de empleados o terceros a la información del Grupo ECI y sus empresas.

4. La seguridad de la información ha de ser entendida como un proceso integral que involucra a todos y cada uno de los intervinientes, así como a los diferentes elementos técnicos, materiales y organizativos involucrados en actividades en las que se gestiona información del Grupo ECI. En consecuencia, habrán de adoptarse las medidas oportunas para que todas las personas que intervienen en la gestión y uso de la información, conozcan la PCSI y desarrollen sus funciones de conformidad con la misma.

5. El desarrollo de la PCSI deberá:

   - Ser adecuado al propósito de la Organización;
   - Incluir objetivos de seguridad de la información y/o proporcionar un marco de referencia para el establecimiento de los objetivos de seguridad de la información aplicables a las empresas del Grupo ECI;
   - Determinar las medidas técnicas y/u organizativas de seguridad que han de ser implantadas de conformidad con el apetito al riesgo definido. Dichas medidas no podrán ser rechazadas por los "dueños y/o generadores" de la información sin una causa justificada, que deberá estar convenientemente aprobada.



C/ Marqués de Mondéjar 16, posterior.
28028 Madrid - T. 91 354 12 92

## 4.2 Gestión de riesgos:

El análisis y la gestión de riesgos es una parte esencial del proceso de seguridad de la información. Los niveles de riesgo han de mantenerse dentro de unos parámetros adecuados, mediante el despliegue de las medidas técnicas y organizativas de seguridad apropiadas y permanentemente actualizadas, de modo tal que se establezca un equilibrio y proporcionalidad entre la naturaleza de la información perteneciente al Grupo ECI, los riesgos a los que está expuesta y las medidas de seguridad a implantar.

## 4.3 Gestión de incidentes de seguridad:

El Grupo de empresas El Corte Inglés debe disponer de un servicio de respuesta ante incidentes de seguridad de la información que esté dotado de los medios necesarios para dar respuesta a los mismos.

Este servicio podrá aplicar las medidas de subsanación necesarias incluyendo, entre otras, la desconexión o aislamiento de dispositivos en aquellos casos que supongan un riesgo potencial o real para el resto de los sistemas de información.

Cualquier usuario debe informar, por los cauces que se determinen, sobre los incidentes y/o debilidades que puedan identificar y que tengan relación con la seguridad de la información.

En el sistema de gestión de incidentes se debe centralizar la recogida, análisis y gestión de los incidentes identificados.



C/ Marqués de Mondéjar 16, posterior.
28028 Madrid - T. 91 354 12 92

### 4.4 Principios relativos a la recogida de información:

De conformidad con la legislación aplicable en cada momento, en relación con los procesos de recopilación de información y tratamiento de datos sobre accionistas, empleados, clientes, visitas, proveedores, etc., se informará de modo transparente, expreso, preciso e inequívoco, sobre la finalidad para la que la información y/o datos son recabados.

### 4.5 Principios en materia de medidas de seguridad y confidencialidad:

Las Empresas del Grupo ECI deberán diseñar, implantar, ejecutar y mantener todas las medidas de seguridad organizativas y técnicas que sean necesarias para garantizar que la recopilación, tratamiento y protección de la información se realiza cumpliendo los requisitos legalmente establecidos.

Asimismo, los terceros que se relacionen con las empresas del Grupo deberán cumplir las directrices de seguridad de la información que estén establecidas en esta Política Corporativa y la normativa asociada.

De conformidad con la legislación aplicable, la información recabada y tratada por las Empresas del Grupo ECI y terceras partes relacionadas con las mismas, se conservará con la confidencialidad y secreto debidos, no siendo utilizada para otros fines distintos que para los que se recopiló y sin que pueda ser comunicada o cedida a terceros fuera de los casos permitidos por la ley y de conformidad con los procedimientos legalmente establecidos. Asimismo, se respetarán los plazos de conservación señalados para cada caso en concreto.



C/ Marqués de Mondéjar 16, posterior.
28028 Madrid - T. 91 354 12 92

## 4.6 Principios sobre las adquisiciones y las cesiones de información:

Queda prohibida la adquisición y/o recopilación y/o la cesión de información de fuentes ilegítimas o de fuentes que no puedan garantizar la legítima procedencia de la información ofrecida y/o no puedan garantizar la protección adecuada de la información.

## 4.7 Principios sobre la contratación de encargados del tratamiento:

La contratación de terceros prestadores de servicios que, en virtud de la actividad o servicio a prestar, pudieran tener acceso a información responsabilidad de las Empresas del Grupo ECI, deberá ser verificada y deberá confirmarse que el prestador de servicios reúne las garantías necesarias y cumple con las medidas de seguridad exigibles en cada jurisdicción en la que el Grupo ECI opera durante la vigencia de la relación contractual.

## 4.8 Transferencias internacionales de información:

Todo tratamiento de información sujeto a la normativa de la Unión Europea que implique una transferencia de la misma fuera del Espacio Económico Europeo, deberá llevarse a cabo dentro del estricto cumplimiento de los requisitos establecidos en la ley aplicable.

Asimismo, las Empresas del Grupo ubicadas fuera de la Unión Europea deberán cumplir con los requisitos establecidos en el ámbito de su jurisdicción para efectuar una transferencia internacional de información.



C/ Marqués de Mondéjar 16, posterior.
28028 Madrid - T. 91 354 12 92

### 4.9 Formación y concienciación del personal:

La formación en materia de Seguridad de la Información para los empleados es crucial para las empresas del Grupo ECI, por ello debe establecerse un conjunto de acciones formativas para garantizar los conocimientos, las habilidades y las actitudes de los empleados, con el objetivo de mejorar las actividades relacionadas con la seguridad de la información.

Es fundamental que los conocimientos que se adquieran no se queden obsoletos y para ello han de establecerse los medios necesarios para actualizar periódicamente los conocimientos y obtener, por parte de cada empleado, un desempeño eficaz y diligente en el manejo de la seguridad de la información.

## 5. Evaluación, control y supervisión

El Comité de Seguridad de la Información evaluará periódicamente el cumplimiento y la eficacia de la PCSI e informará del resultado al Comité de Dirección de Seguridad de la Información.

Corresponde al Comité de Seguridad de la Información la supervisión de forma continua de la aplicación de lo dispuesto en la PCSI por parte del Grupo ECI y sus Empresas.



C/ Marqués de Mondéjar 16, posterior.
28028 Madrid - T. 91 354 12 92

## 6. Aprobación, entrada en vigor y actualización

La modificación de esta Política es competencia del Consejo de Administración.

Esta Política habrá de mantenerse actualizada en el tiempo. Para ello, debe revisarse de forma ordinaria con periodicidad anual y, de forma extraordinaria, cada vez que se produzcan variaciones significativas en los objetivos estratégicos o en la normativa aplicable. Las propuestas de modificación se presentarán a la Comisión de Auditoría y Control por parte del Comité de Seguridad de la Información, previa validación de Asesoría Jurídica y Cumplimiento y con la correspondiente supervisión del órgano de control interno que tenga atribuida tal función. En caso de que la Comisión de Auditoría y Control la considere apropiada, la elevará, al Consejo de Administración para, en su caso, su aprobación definitiva.



C/ Marqués de Mondéjar 16, posterior.
28028 Madrid - T. 91 354 12 92

# CONTROL DE CAMBIOS

## POLÍTICA CORPORATIVA SEGURIDAD DE LA INFORMACIÓN

Primera Versión

Fecha aprobación: 25/11/20

| Fecha revisión | Conformidad | Prop. Modificación |
|---|---|---|



C/ Marqués de Mondéjar 16, posterior.
28028 Madrid - T. 91 354 12 92