Política Corporativa de Seguridad de la Información

Aprobado por el Consejo de Administración de El Corte Inglés, S.A. el 30 de noviembre de 2020

Versión 2.0 de 30 de octubre de 2024

El Corte Inglés

ÍNDICE

1. INTRODUCCIÓN 1
2. OBJETIVO 1
3. ÁMBITO DE APLICACIÓN 1
4. PRINCIPIOS DE ACTUACIÓN 2
5. ESTRUCTURA ORGANIZATIVA 3
5.1 Gobierno de la Seguridad de la Información 4
5.2 Gestión y Operación de la Seguridad de la Información 4
6. COMPONENTES DEL SGSI 4
7. DILIGENCIA DEBIDA 5
8. CONOCIMIENTO Y DECLARACIÓN DE CONFORMIDAD 6
9. COMUNICACIÓN DE INCUMPLIMIENTOS 6
9.1 Incumplimientos de la normativa de seguridad de la información 6
9.2 Notificación de incidencias de seguridad de la información 7
10. APROBACIÓN, ENTRADA EN VIGOR Y ACTUALIZACIÓN 7
11. DIFUSIÓN Y APLICACIÓN 8
12. CONTROL, SEGUIMIENTO Y SUPERVISIÓN 8
12.1 Control y seguimiento 8
12.2 Supervisión 8
Anexo I - Definiciones 10

NOTA: En el **Anexo I** se relacionan las definiciones de aquellos términos que se utilizan de manera frecuente en el presente documento y en las normas relacionadas que conforman el Sistema de Gestión de Seguridad de la Información, así como las que conforman el Sistema de Gestión de Compliance Penal de EL CORTE INGLÉS.

1. INTRODUCCIÓN

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

Desde sus orígenes, se ha considerado que la información registrada, generada y gestionada en el Grupo constituye uno de sus activos estratégicos y es fundamental para la sostenibilidad y competitividad de la Organización. Es por ello, que con el objetivo de establecer los principios generales que deben regir en el tratamiento de información en todas las empresas del Grupo, 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 (en adelante, la "Política").

La presente Política está alineada con los valores del Grupo, ratificando la firme voluntad de contribuir a los 17 Objetivos de Desarrollo Sostenible de Naciones Unidas y mantener una conducta respetuosa tanto con las normas exigibles a sus actividades, como con los estándares éticos y demás normas e iniciativas que el Grupo se compromete a respetar mediante su certificación o adhesión, tales como UNE-ISO/IEC 27001:2023, Esquema Nacional de Seguridad (ENS) y Payment Card Industry – Data Security Standard (PCI-DSS).

La Política constituye la base del Sistema de Gestión de Seguridad de la Información (en adelante, "SGSI"), a partir del cual se establecen la estrategia y operativa de protección de la información de la Organización.

2. OBJETIVO

El objeto de la Política es establecer los principios para el control y la gestión de los riesgos de Seguridad de la Información en interés de las sociedades integradas en el Grupo con el fin de establecer los fundamentos para preservar su confidencialidad, integridad y disponibilidad.

La aplicación de dichos principios permitirá:

- garantizar la continuidad de las operaciones,
- cumplir con la legislación vigente,
- mantener una buena reputación comercial,

3. ÁMBITO DE APLICACIÓN

La presente Política es de obligado cumplimiento y de aplicación global a las sociedades que conforman el Grupo El Corte Inglés, empleados, colaboradores y terceros, que gestionen información del Grupo en cualquier formato o soporte, en todas las actividades relacionadas con su cadena de valor, tanto ascendente como descendente, independientemente del país en el que se desarrollen, así como los grupos de partes interesadas afectadas

Todos los Miembros de la Organización, especialmente los trabajadores de la cadena de valor deberán cumplir con su contenido, independientemente del cargo que ocupen y del territorio desde donde operen. También será de aplicación a los Socios de Negocio cuando desarrollen sus actividades en el Grupo, así como a todos los trabajadores de la cadena de valor y al resto de partes interesadas involucradas en la cadena de valor.

Este compromiso debe formalizarse según se establece en el apartado "8. Conocimiento y declaración de conformidad" de la presente Política.

Asimismo, la Política se aplica en lo relativo a los riesgos derivados de amenazas y vulnerabilidades de los sistemas de información y comunicaciones del Grupo, incluyendo cualquier activo de gestión externalizada que se utilice para realizar operaciones y/o prestar servicios.

4. PRINCIPIOS DE ACTUACIÓN

El Grupo El Corte Inglés espera de cualquier Miembro de la Organización, así como de sus Socios de Negocio y demás implicados identificados en el apartado "3. Ámbito de Aplicación", el seguimiento de los siguientes principios de actuación del Grupo con relación a la Seguridad de la Información, a partir de los cuales se realiza la efectiva protección de los activos y de la información:

Principio 1. Cumplimiento de las leyes y regulaciones.

El Grupo vela por el cumplimiento de las leyes y regulaciones tanto nacionales como internacionales en materia de Seguridad de la Información vigentes en cada momento en los territorios en los que opera el Grupo en especial aquellas relacionadas con la protección de datos de carácter personal, seguridad de los sistemas, accesibilidad, comunicaciones y servicios electrónicos.

Principio 2. Implementación de medidas de Seguridad de la Información basadas en riesgo y eficiencia.

El Grupo aplica criterios de riesgo y eficiencia a la hora de definir y aplicar medidas de seguridad para proteger los activos y sistemas de información y evitar actividades fraudulentas y ataques contra la integridad y reputación de la empresa.

Los procedimientos de control aplicados en la empresa implican, entre otras opciones, el almacenamiento y comprobación de los mensajes, transacciones o comunicaciones mediante el acceso al contenido de los mismos, con sus ficheros adjuntos o enlaces, lo que los excluye del ámbito personal de confidencialidad e intimidad del de los interlocutores, a los que los miembros de la Organización deben informar de ello.

Asimismo, los miembros de la Organización no deben instalar en los equipos/sistemas puestos a disposición por la empresa ningún programa ni versión no homologada mediante el proceso corporativo y de contratación de servicios de El Corte Inglés, S.A., en especial, asistentes inteligentes conversacionales y productivos y/o de codificación (IA) con datos empresariales, salvo que haya sido previamente autorizado.

Principio 3. Cultura de la Seguridad de la Información.

La cultura de Seguridad de la Información pretende establecer el conjunto de creencias, conductas y costumbres de los usuarios sobre el manejo de la información de tal forma que se preserve su confidencialidad, integridad y disponibilidad.

Para ello, el Grupo realiza acciones de divulgación, formación y capacitación en la materia, asegurando la adecuada cualificación de todo el personal tanto interno como externo.

Principio 4. Respuesta de manera efectiva ante incidentes de Seguridad de la Información.

El Grupo El Corte Inglés establece mecanismos de detección y reacción frente a incidentes de seguridad que puedan comprometer los sistemas o activos de información del Grupo con la finalidad de dar una respuesta de manera efectiva y así minimizar los impactos en la empresa y demás partes interesadas, y reducir los tiempos de recuperación.

Para ello, el Grupo ha establecido relaciones sólidas y colaborativas con las autoridades y organismos competentes encargados de la seguridad de la información con el fin de garantizar el cumplimiento normativo y responder de manera efectiva a los incidentes de seguridad.

Estas relaciones se establecerán según la normativa interna vigente.

Principio 5. Seguridad de la Información en la Cadena de Valor.

El Grupo traslada estos principios a los proveedores y las partes interesadas como parte de la gestión de los riesgos de seguridad de la información.

En consecuencia, en la contratación de proveedores, se deberá asegurar que se trasladan tanto a nivel contractual como de formación los requisitos que emanen de la normativa interna en relación con proveedores.

Principio 6. Uso responsable de los sistemas de información

Todos los Miembros de la Organización y demás usuarios de los sistemas y equipos informáticos del Grupo deben hacer un uso exclusivamente profesional de los mismos.

Para ello, el Grupo El Corte Inglés puede controlar los accesos a Internet y los mensajes, transacciones o comunicaciones, con sus ficheros adjuntos o enlaces, que se envíen o reciban a través de los equipos/sistemas a los que acceda bajo su identificación y así verificar lo establecido en esta Política y demás normativa interna.

Asimismo, la utilización de las herramientas de trabajo que la Organización pone a disposición de los usuarios no pertenece a la esfera privada de éstos.

Estos principios están relacionados con la gestión de los impactos, riesgos y oportunidades específicos identificados en el apartado Objetivo de la Política del presente documento. Su aplicación se lleva a cabo mediante un SGSI que se articula bajo una estructura organizativa encargada de su Gobierno, Gestión y Operación. Para su correcto funcionamiento, el SGSI se basa en cuatro componentes clave: Estrategia, Marco de Control, Marco Normativo y Cuadro de Mando de Seguridad de la Información.

5. ESTRUCTURA ORGANIZATIVA

El SGSI del Grupo establece una estructura organizativa basada en tres pilares fundamentales: el Gobierno, la Gestión y la Operación de la Seguridad de la Información.

5.1 Gobierno de la Seguridad de la Información

Como base de la Gobernanza, el Grupo ha establecido tres comités encargados de supervisar y dar seguimiento a todos los aspectos relacionados con la seguridad de la información en sus diferentes niveles de responsabilidad, interlocución y operación:

- **CSI (Comité de Seguridad de la Información):** comité de carácter multidisciplinar y funcionamiento periódico, encargado de impulsar y supervisar la seguridad de la información de manera transversal en la organización asegurando que las buenas prácticas sobre la gestión de la seguridad se apliquen holísticamente de manera efectiva y consistente.
- **SCSI (Subcomité de Seguridad de la Información):** comité de carácter multidisciplinar y funcionamiento periódico encargado de asegurar la ejecución y cumplimiento de las actividades de seguridad de la información impulsadas y supervisadas por el CSI.
- **CODES (Comisión Delegada de Seguridad de la Información):** comité encargado de la gestión operativa e implementación del Marco de Control de la Seguridad de la Información del Grupo.

Se garantiza que estos tres comités para el Gobierno de la Seguridad de la Información se comunican entre sí de manera fluida, escalando y aterrizando los temas a tratar de forma estructurada y organizada. Esto asegura que las decisiones y acciones se tomen con la coordinación necesaria para que los objetivos de seguridad de la información se aborden de manera integral y eficiente en toda la organización.

El funcionamiento de estos comités se regula en su correspondiente reglamento.

5.2 Gestión y Operación de la Seguridad de la Información

Bajo la supervisión de los comités previamente establecidos, la Gestión y Operación de la Seguridad de la Información se estructura en cinco áreas funcionales de gestión de la seguridad de la información, respaldadas por el área transversal de Operaciones. En este contexto, el Departamento de Seguridad de Información y Ciberseguridad, encabezado por el Responsable de Seguridad de la Información y Ciberseguridad (RSIC), lidera, coordina y supervisa estas funciones.

- **RSIC (Responsable de Seguridad de Información y Ciberseguridad):** responsable de liderar la gestión de la seguridad de la información.
- **Áreas de gestión de Seguridad de la Información:** estas áreas se encargan de articular las diferentes capacidades de la Seguridad de la Información: Gobernanza y Riesgos de Seguridad, Protección, Detección, Respuesta y Seguridad por Diseño.
- **Centro de Operaciones de Seguridad (COS):** es el área transversal que se encarga de dar soporte operativo al Departamento de Seguridad de Información y Ciberseguridad.

6. COMPONENTES DEL SGSI

Para la aplicación del SGSI, el Grupo ha definido cuatro componentes fundamentales sobre los que se articula su eficaz funcionamiento:

- **Estrategia de Seguridad de la Información:** aproximación de alto nivel definida por el Grupo con el objetivo de acometer la gestión adecuada de los riesgos de seguridad de la información a través de una serie de líneas de trabajo definidas para su mitigación.
- **Marco de Control de Seguridad de la Información:** marco de control que sirve como fundamento para el establecimiento de la estrategia, así como para la propia operación de seguridad de la información, basándose en los requisitos de referencia para las quince capacidades operativas de seguridad de la información definidas en la UNE-ISO/IEC 27001:2023.
- **Marco Normativo de Seguridad de la Información:** desarrollo de un conjunto de Políticas, Normas, Procedimientos generales y específicos que abarcan los requisitos identificados tanto en el Marco de Control, como en las regulaciones aplicables.
- **Cuadro de Mando de Seguridad de la Información:** herramienta que permite medir y evaluar el desempeño de las acciones y procesos relacionados con la seguridad de la información en el Grupo.

Estos cuatro componentes son mantenidos y actualizados según el contexto y las necesidades de la Organización por el Departamento de Seguridad de Información y Ciberseguridad.

7. DILIGENCIA DEBIDA

Los procesos de diligencia debida hacen referencia a la gestión y monitorización de la relación con terceros, bien sean estos proveedores, clientes, socios comerciales o cualquier otra tercera parte con la que medie relación contractual y tengan, o potencialmente puedan tener, acceso a la información sensible de la Organización.

El proceso de diligencia debida con terceros se asienta bajo los siguientes pilares:

- Antes de establecer una relación con una tercera parte, se debe evaluar el impacto del acuerdo en la Seguridad la Información y, si hay impacto, realizar el análisis de riesgos correspondiente.
- La Organización debe establecer un marco de controles y medidas que permita de forma normalizada y sistemática gestionar los riesgos de seguridad vinculados a la colaboración o contratación de terceras partes.
- La tercera parte se debe comprometer contractualmente al cumplimiento de la Política de Seguridad de la Información y a la implantación de las medidas técnicas y organizativas que aseguren la correcta protección de los activos de información de la Organización.
- De forma periódica y en base el nivel de riesgo asociado al acuerdo, se deben llevar a cabo procesos de monitorización y auditoría que aseguren que la tercera parte mantiene un ecosistema de seguridad equivalente al comprometido contractualmente.
- A la finalización de la relación contractual, la Organización debe asegurar la devolución de los activos, la destrucción de la información y la revocación de accesos a la información por parte del tercero.

8. CONOCIMIENTO Y DECLARACIÓN DE CONFORMIDAD

El cumplimiento de las normas y estándares éticos compromete a toda la Organización y constituye un objetivo estratégico para la misma, por ello, se espera que todos los Miembros de la Organización conozcan y respeten el contenido de esta Política. Igualmente, y respecto de Socios de Negocio, se espera que desarrollen comportamientos alineados con la misma.

Este compromiso debe formalizarse mediante:

i. Declaraciones de conformidad con los principios en ellas desarrollados por parte de los Miembros de la Organización, a través de su adhesión a los **Altos Estándares Éticos**,

ii. **Cláusulas en materia de Cumplimiento incluidas en los contratos** con Socios de Negocio

iii. **Adhesiones expresas o tomas de razón** por parte de los órganos de Administración de las empresas que forman parte de Grupo Corte Inglés, según normativa interna elaborada al respecto.

Estas adhesiones y sus renovaciones deberán comunicarse, cuando se formalicen, a la Dirección de Cumplimiento y Control de Riesgos del Grupo El Corte Inglés.

Cuando se produzcan cambios significativos en esta Política, entendiendo por éstos los que requieran una aprobación formal por parte del Consejo de Administración de El Corte Inglés, S.A. deberán renovarse formalmente los compromisos anteriores.

Puesto que el cumplimiento de las normas y estándares éticos compromete a toda la Organización y constituye un objetivo estratégico para la misma, se espera que todos los Miembros de la Organización conozcan y respeten el contenido de esta Política. Igualmente, y respecto de Socios de Negocio, se espera que desarrollen comportamientos alineados con la misma.

La Organización reaccionará de forma inmediata ante eventuales incumplimientos de lo establecido en esta Política, conforme a lo previsto en su normativa interna y de acuerdo con la legislación vigente que resulte de aplicación.

9. COMUNICACIÓN DE INCUMPLIMIENTOS

9.1 Incumplimientos de la normativa de seguridad de la información

Todos los Miembros de la Organización, Socio de Negocio o Tercero con relación directa e interés comercial o profesional legítimo, y demás partes interesadas, en caso de detectar un incumplimiento de la presente Política o de tener dudas sobre si alguna práctica observada puede suponer un acto ilícito, ya sea en el sector público como en el privado, está obligado a ponerse inmediatamente en contacto con la Dirección de Cumplimiento y Control de Riesgos del Grupo El Corte Inglés a través del Canal Ético, en cualquiera de sus vías de comunicación:

- **Canal Digital:**

  El Grupo El Corte Inglés dispone de un canal digital al que se puede acceder a través de la siguiente dirección web:

  https://www.elcorteingles.es/informacioncorporativa/es/gobierno-corporativo/etica-y-cumplimiento/

Este acceso está disponible en la web corporativa y adicionalmente en la intranet NEXO para los Miembros de la Organización

- **Dirección postal:**

  El Corte Inglés, S.A.
  Dirección de Cumplimiento y Control de Riesgos
  c/ Hermosilla, 112
  28009 Madrid

- **Teléfono Departamento Cumplimiento Normativo:** 91 401 85 00

- **Solicitud de reunión presencial o por medios telemáticos**

La información transmitida por este Canal es confidencial, así como la identidad de los informantes, a los que la Organización agradece su colaboración y respecto a los cuales garantiza la ausencia de represalias.

Además, la Dirección de Cumplimiento y Control de Riesgos podrá actuar por propia iniciativa investigando cualquier indicio de incumplimiento de esta Política.

9.2 Notificación de incidencias de seguridad de la información

Cualquier Miembro de la Organización, Socio de Negocio o Tercero con relación directa e interés comercial o profesional legítimo, en caso de detectar un evento de seguridad que pudiese causar una incidencia en los sistemas de la información del Grupo, está obligado a ponerse inmediatamente en contacto con el Centro de Operaciones de Seguridad (COS) del Grupo El Corte Inglés, a través de las siguientes vías de comunicación:

- **Buzón:**

  El COS del Grupo El Corte Inglés dispone del siguiente buzón:

  cos_notificaciones@elcorteingles.es

- **Teléfono COS:** 636 10 27 32 (78570)

10. APROBACIÓN, ENTRADA EN VIGOR Y ACTUALIZACIÓN

La presente Política entrará en vigor en la fecha de aprobación por el Consejo de Administración de El Corte Inglés, S.A.

Esta Política habrá de mantenerse actualizada en el tiempo. Para ello, debe revisarse de forma ordinaria con periodicidad anual y, de forma extraordinaria, y en todo caso, a la mayor brevedad, cuando se produzcan variaciones significativas en los objetivos estratégicos o en la normativa externa o interna aplicable que implique su actualización o modificación.

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 la Dirección de Asesoría Jurídica y de la Dirección de Cumplimiento y Control de Riesgos y con la correspondiente supervisión del órgano de control interno que tenga atribuida la función.

En caso de que los cambios sean relevantes, deberán someterse a la aprobación del Consejo de Administración previa propuesta de la Comisión de Auditoría y Control.

11. DIFUSIÓN Y APLICACIÓN

La presente Política estará disponible en NEXO para todos los Miembros de la Organización y en la web corporativa para todos los grupos de interés del Grupo, una vez sea aprobada por el Consejo de Administración de El Corte Inglés, S.A.

Asimismo, el Comité de Seguridad de la Información se ocupará de impulsar las acciones necesarias para su adecuada difusión y conocimiento.

12. CONTROL, SEGUIMIENTO Y SUPERVISIÓN

12.1 Control y seguimiento

El Subcomité de Seguridad de la Información evaluará periódicamente el cumplimiento y la eficacia de esta Política mediante revisiones, controles y auditorías internas y externas coordinados por el Departamento de Seguridad de Información y Ciberseguridad, e informará del resultado al Comité 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 esta Política por parte de las empresas del Grupo.

12.2 Supervisión

El departamento de Auditoría Interna revisará la adecuación y la eficacia de las medidas aplicadas en el SGSI para supervisar el cumplimiento de las normativas aplicables a las distintas actividades de la Organización en la medida en que el Plan Anual de Auditoría aprobado por la Comisión de Auditoría y Control incluya trabajos vinculados con dicho Sistema, y extraordinariamente, como consecuencia de la ocurrencia de incidencias o identificación de irregularidades. Como resultado de dichas auditorías, Auditoría Interna emitirá el correspondiente informe, emitiéndose recomendaciones en caso de identificarse oportunidades de mejora.

Las oportunidades de mejora que potencialmente puedan identificarse como resultado de estas revisiones, deberán considerarse en el proceso de mejora continua del Sistema.

La valoración de un posible incumplimiento de la Política Corporativa de Seguridad de la Información se determinará en el procedimiento correspondiente, según las disposiciones vigentes, sin perjuicio de las responsabilidades legales, incluso de carácter sancionador en el ámbito laboral, que, en su caso, puedan resultar exigibles al incumplidor.

CONTROL DE CAMBIOS

Versión 2.0 aprobada por el Consejo de Administración el 30/11/2020

Versión	Fecha Modificación	Objeto de la Modificación	Apartados afectados
1.1	28/06/2023	- Incorporación vías de Comunicación	- Comunicación de incumplimientos
2.0	30/10/2024	- Adecuación al nuevo marco estratégico y regulatorio - Adecuación de la Política a los requerimientos de la Directiva sobre Información Corporativa en Materia de Sostenibilidad. - Incorporación proceso de Diligencia debida. - Inclusión de referencia a la nueva normativa interna para la adhesión de las sociedades del Grupo a las Políticas Corporativas. - Actualización canales digitales para la comunicación de incumplimientos. - Incorporación apartado difusión	- Todos

Última revisión, octubre 2024

Anexos

Anexo I - Definiciones

Se relacionan a continuación las definiciones de aquellos términos que se utilizan de manera frecuente en el presente documento.

Activo de información: cualquier información o sistema relacionado con el tratamiento de la información que tenga valor para la organización, como pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.

Amenaza: circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

Confidencialidad: se refiere a la protección de datos y sistemas para evitar amenazas como el acceso no autorizado o la fuga de datos que podría resultar en la divulgación, alteración o destrucción de información sensible.

Disponibilidad: capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

Incidente de seguridad: cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

Integridad: propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración o pérdida.

Política de Seguridad de la Información: documento de nivel ejecutivo mediante el cual una empresa establece sus directrices, decisiones y medidas de seguridad respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riesgos a los que están expuestos.

Resiliencia: capacidad de una organización para construir, asegurar y revisar su integridad y fiabilidad operativas para sustentar la prestación continuada de los servicios.

Riesgo: es la posibilidad de que se produzcan incidentes o eventos que comprometan la confidencialidad, integridad o disponibilidad de los datos y sistemas de la Organización.

Seguridad de la Información: conjunto de tecnologías, prácticas y medidas diseñadas para proteger la confidencialidad, integridad y disponibilidad de la información.