

Política Corporativa de Segurança da Informação

Aprovado pelo Conselho de Administração
do El Corte Inglés, S.A.
30 de novembro de 2020

Versão 2.0 de 30 de outubro de 2024

El Corte Inglés

ÍNDICE

1. INTRODUÇÃO 1
2. OBJETIVO 1
3. ÂMBITO DE APLICAÇÃO 1
4. PRINCÍPIOS DE AÇÃO 2
5. ESTRUTURA ORGANIZATIVA 3
5.1 Governação da segurança da informação 3
5.2 Gestão e operação da segurança da informação 4
6. COMPONENTES SGSI 4
7. DELIGÊNCIA DEVIDA 5
8. CONHECIMENTO E DECLARAÇÃO DE CUMPRIMENTO 5
9. COMUNICAÇÃO DE INCUMPRIMENTOS 6
9.1 Não conformidade com os regulamentos de segurança da informação 6
9.2 Notificação de incidentes de segurança da informação 7
10. APROVAÇÃO, ENTRADA EM VIGOR E ATUALIZAÇÃO 7
11. DIVULGAÇÃO E APLICAÇÃO 7
12. CONTROLO, ACOMPANHAMENTO E SUPERVISÃO 7
12.1 Controlo e monitorização 7
12.2 Controlo 8
Anexo I - Definições 10

NOTA: **O Anexo I** contém as definições dos termos frequentemente utilizados no presente documento e nos regulamentos conexos que integram o Sistema de Gestão da Segurança da Informação, bem como os que integram o Sistema de Gestão do Cumprimento Penal do EL CORTE INGLÉS.

1. INTRODUÇÃO

O Conselho de Administração do El Corte Inglés, S.A. é responsável pela formulação da Estratégia e das Políticas Corporativas das sociedades do Grupo El Corte Inglés (doravante, o "Grupo"), bem como pela aprovação dos programas e sistemas de cumprimento e controlo interno.

Desde o início, a informação registada, gerada e gerida no Grupo foi considerada um dos seus ativos estratégicos e fundamental para a sustentabilidade e competitividade da Organização. Assim, com o objetivo de estabelecer os princípios gerais que devem reger o tratamento da informação em todas as empresas do Grupo, o Conselho de Administração, por e como resultado da proposta da Comissão de Auditoria e Controlo, aprovou a seguinte Política Corporativa de Segurança da Informação do Grupo (doravante, a "Política").

Esta Política está alinhada com os valores do Grupo, ratificando a vontade firme de contribuir para os 17 Objetivos de Desenvolvimento Sustentável das Nações Unidas e de manter uma conduta que respeite tanto as regras aplicáveis às suas atividades como os padrões éticos e outras regras e iniciativas que o Grupo se compromete a respeitar através da sua certificação ou adesão, tais como a UNE-ISO/IEC 27001:2023, o Esquema Nacional de Segurança (ENS) e a Payment Card Industry - Data Security Standard (PCI-DSS).

A Política constitui a base do Sistema de Gestão da Segurança da Informação (a seguir designado "SGSI"), a partir do qual são estabelecidas a estratégia e as operações de proteção da informação da Organização.

2. OBJETIVO

O objetivo da Política é estabelecer os princípios para o controlo e gestão dos riscos de Segurança da Informação no interesse das empresas integradas no Grupo, de forma a estabelecer as bases para a preservação da sua confidencialidade, integridade e disponibilidade.

A aplicação destes princípios permitirá:

- assegurar a continuidade das operações,
- cumprir a legislação atual,
- manter uma boa reputação comercial,

3. ÂMBITO DE APLICAÇÃO

Esta Política é de cumprimento obrigatório e aplica-se globalmente às empresas que compõem o Grupo El Corte Inglés, aos empregados, colaboradores e terceiros que gerem a informação do Grupo em qualquer formato ou suporte, em todas as atividades relacionadas com a sua cadeia de valor, tanto a montante como a jusante, independentemente do país em que se desenvolvam, bem como aos grupos de interesse afetados.

Todos os Membros da Organização, especialmente os trabalhadores da cadeia de valor, devem cumprir o seu conteúdo, independentemente do cargo que ocupam e do território a partir do qual operam. Aplica-se igualmente aos Parceiros Comerciais quando estes desenvolvem as suas

atividades no Grupo, bem como a todos os trabalhadores da cadeia de valor e a todas as outras partes interessadas envolvidas na cadeia de valor.

Este compromisso deve ser formalizado tal como previsto na secção "8. Conhecimento e declaração de cumprimento" da presente política.

A política também se aplica aos riscos decorrentes de ameaças e vulnerabilidades dos sistemas de informação e comunicação do Grupo, incluindo quaisquer ativos de gestão subcontratados utilizados para conduzir operações e/ou prestar serviços.

4. PRINCÍPIOS DE AÇÃO

O Grupo El Corte Inglés espera que qualquer Membro da Organização, bem como os seus Parceiros de Negócio e outros identificados no ponto "3. Âmbito de Aplicação", cumpram os seguintes princípios de atuação do Grupo em matéria de Segurança da Informação, com base nos quais se consegue uma proteção eficaz dos ativos e da informação:



Princípio 1 - Cumprimento com as leis e regulamentos.

O Grupo garante o cumprimento das leis e regulamentos nacionais e internacionais em matéria de Segurança da Informação em vigor nos territórios em que opera, especialmente os relacionados com a proteção dos dados pessoais, a segurança dos sistemas, a acessibilidade, as comunicações e os serviços eletrónicos.



Princípio 2: Aplicação de medidas de segurança da informação com base no risco e na eficácia.

O Grupo aplica critérios de risco e de eficácia na definição e implementação de medidas de segurança para proteger os ativos e os sistemas de informação e para prevenir atividades fraudulentas e ataques contra a integridade e a reputação da empresa.

Os procedimentos de controlo aplicados na empresa envolvem, entre outras opções, o armazenamento e a verificação de mensagens, transações ou comunicações através do acesso ao seu conteúdo, com os seus ficheiros anexos ou links, o que os exclui da esfera pessoal de confidencialidade e privacidade dos interlocutores, que devem ser informados pelos membros da organização.

Da mesma forma, os membros da Organização não poderão instalar nos equipamentos/sistemas disponibilizados pela empresa qualquer programa ou versão não aprovada através do processo de contratação corporativa e de serviços do El Corte Inglés, S.A., especialmente assistentes inteligentes conversacionais e produtivos e/ou codificação (IA) com dados empresariais, salvo autorização prévia.



Princípio 3. Cultura de segurança da informação.

A cultura de Segurança da Informação visa estabelecer o conjunto de crenças, comportamentos e costumes dos utilizadores relativamente ao tratamento da informação de forma a preservar a sua confidencialidade, integridade e disponibilidade.

Para o efeito, o Grupo desenvolve ações de divulgação, educação e formação nesta área, assegurando que todo o pessoal interno e externo possui as qualificações adequadas.



Princípio 4: Responder eficazmente a incidentes de segurança da informação.

O Grupo El Corte Inglés estabelece mecanismos para detetar e reagir a incidentes de segurança que possam comprometer os sistemas ou ativos de informação do Grupo, com o objetivo de dar uma resposta eficaz e, assim, minimizar o impacto na empresa e noutras partes interessadas, e reduzir os tempos de recuperação.

Para o efeito, o Grupo estabeleceu relações sólidas e de colaboração com as autoridades e agências de segurança da informação relevantes para garantir o cumprimento regulamentar e responder eficazmente a incidentes de segurança.

Estas relações são estabelecidas em conformidade com os regulamentos internos em vigor.



Princípio 5: Segurança da informação na cadeia de valor.

O Grupo comunica estes princípios aos fornecedores e às partes interessadas no âmbito da gestão dos riscos de segurança da informação.

Por conseguinte, aquando da contratação de fornecedores, deve garantir-se que os requisitos decorrentes da regulamentação interna relativa aos fornecedores são aplicados tanto a nível contratual como a nível da formação.



Princípio 6 - Utilização responsável dos sistemas de informação

Todos os Membros da Organização e outros utilizadores dos sistemas e equipamentos informáticos do Grupo devem utilizá-los apenas de forma profissional.

Para o efeito, o Grupo El Corte Inglés poderá monitorizar o acesso à Internet e as mensagens, transações ou comunicações, com os respetivos ficheiros anexos ou ligações, que sejam enviadas ou recebidas através dos equipamentos/sistemas acedidos sob a sua identificação, verificando assim o disposto na presente Política e demais normas internas.

Do mesmo modo, a utilização dos instrumentos de trabalho colocados à disposição pela Organização não pertence à esfera privada dos utilizadores.

Estes princípios estão relacionados com a gestão dos impactos, riscos e oportunidades específicos identificados na secção do Objetivo Político do presente documento. A sua aplicação é efetuada através de um SGSI que se articula sob uma estrutura organizacional responsável pela sua Governação, Gestão e Operação. Para o seu bom funcionamento, o SGSI baseia-se em quatro componentes-chave: Estratégia, Quadro de Controlo, Quadro Regulamentar e Quadro de Avaliação da Segurança da Informação.

5. ESTRUTURA ORGANIZATIVA

O SGSI do Grupo estabelece uma estrutura organizacional baseada em três pilares fundamentais: Governação, Gestão e Operação da Segurança da Informação.

5.1 Governação da segurança da informação

Como base de governação, o Grupo criou três comités para supervisionar e monitorizar todos os aspetos da segurança da informação a diferentes níveis de responsabilidade, diálogo e funcionamento:

- **ISC (Information Security Committee):** comité multidisciplinar que funciona regularmente e é responsável por promover e supervisionar a segurança da informação em toda a

organização, garantindo que as boas práticas de gestão da segurança são aplicadas de forma holística, eficaz e coerente.

- **SCSI (Subcomité de Segurança da Informação):** comité multidisciplinar e regular responsável por assegurar a implementação e a aplicação das atividades de segurança da informação conduzidas e supervisionadas pelo ISC.
- **CODES (Comité Delegado para a Segurança da Informação):** comité responsável pela gestão operacional e pela aplicação do quadro de controlo da segurança da informação do Grupo.

Garante que estes três comités para a governação da segurança da informação comunicam entre si de forma fluida, escalando e fundamentando as questões a tratar de forma estruturada e organizada. Isto garante que as decisões e ações são tomadas com a coordenação necessária para que os objetivos de segurança da informação sejam abordados de forma abrangente e eficiente em toda a organização.

O funcionamento destes comités está regulamentado nos respetivos regulamentos internos.

5.2 Gestão e operação da segurança da informação

Sob a supervisão dos comités previamente estabelecidos, a Gestão e Operação da Segurança da Informação está estruturada em cinco áreas funcionais de gestão da segurança da informação, suportadas pela área transversal de Operações. Neste contexto, o Departamento de Segurança da Informação e Cibersegurança, dirigido pelo Diretor de Segurança da Informação e Cibersegurança (RSIC), lidera, coordena e supervisiona estas funções.

- **RSIC (Responsável pela Segurança da Informação e Cibersegurança)**: responsável pela gestão da segurança da informação.
- **Áreas de gestão da segurança da informação**: estas áreas são responsáveis pela articulação das diferentes capacidades de segurança da informação: governação e riscos de segurança, proteção, deteção, resposta e segurança desde a conceção.
- **Centro de Operações de Segurança (COS):** é a área transversal responsável pelo apoio operacional ao Departamento de Segurança da Informação e Cibersegurança.

6. COMPONENTES SGSI

Para a implementação do SGSI, o Grupo definiu quatro componentes fundamentais nos quais se baseia o seu funcionamento efetivo:

- **Estratégia de Segurança da Informação:** abordagem de alto nível definida pelo Grupo com o objetivo de realizar a gestão adequada dos riscos de segurança da informação através de uma série de linhas de trabalho definidas para a sua mitigação.
- **Quadro de Controlo da Segurança da Informação:** quadro de controlo que serve de base para o estabelecimento da estratégia, bem como para a própria operação de segurança da informação, com base nos requisitos de referência para as quinze capacidades operacionais de segurança da informação definidas na UNE-ISO/IEC 27001:2023.
- **Quadro da política de segurança da informação:** desenvolvimento de um conjunto de políticas, normas, procedimentos e procedimentos gerais e específicos que abranjam os requisitos identificados no quadro de controlo e na regulamentação aplicável.
- **Scorecard da Segurança da Informação: uma** ferramenta para medir e avaliar o desempenho das ações e processos relacionados com a segurança da informação no Grupo.

Estes quatro componentes são mantidos e atualizados de acordo com o contexto e as necessidades da organização pelo Departamento de Segurança da Informação e Cibersegurança.

7. DELIGÊNCIA DEVIDA

Os processos de diligência devida referem-se à gestão e monitorização da relação com terceiros, sejam eles fornecedores, clientes, parceiros comerciais ou quaisquer outros terceiros com os quais exista uma relação contratual e que tenham, ou possam potencialmente ter, acesso a informações sensíveis da organização.

O processo de diligência devida de terceiros baseia-se nos seguintes pilares:

- Antes de estabelecer uma relação com um terceiro, deve ser avaliado o impacto do acordo na segurança da informação e, caso exista, deve ser efetuada uma análise de risco correspondente.
- A organização deve estabelecer um quadro de controlos e medidas para gerir os riscos de segurança associados à colaboração ou contratação de terceiros de forma normalizada e sistemática.
- O terceiro deve comprometer-se contratualmente a cumprir a Política de Segurança da Informação e a aplicar as medidas técnicas e organizativas que garantam a proteção correta dos ativos de informação da Organização.
- Periodicamente, e com base no nível de risco associado ao acordo, devem ser efetuados processos de monitorização e auditoria para garantir que o terceiro mantém um ecossistema de segurança equivalente ao contratualmente comprometido.
- Após a cessação da relação contratual, a Organização deve assegurar a devolução dos bens, a destruição das informações e a revogação do acesso às informações por parte do terceiro.

8. CONHECIMENTO E DECLARAÇÃO DE CUMPRIMENTO

O cumprimento das normas e padrões éticos é um compromisso de toda a Organização e constitui um objetivo estratégico da mesma, pelo que se espera que todos os Membros da Organização conheçam e respeitem o conteúdo desta Política. De igual modo, e no que respeita aos Parceiros de Negócio, espera-se que estes desenvolvam comportamentos em consonância com a mesma.

Este compromisso deve ser formalizado por meio de:

i. Declarações de cumprimento com os princípios aí desenvolvidos pelos membros da Organização, através da sua adesão às **Normas Éticas Elevadas**,
ii. Cláusulas de cumprimento incluídas nos contratos com os parceiros comerciais
iii. Adesões ou reconhecimentos expressos por parte dos órgãos de administração das empresas que fazem parte do Grupo Corte Inglés, de acordo com as normas internas elaboradas para o efeito.

A Direção de Cumprimento e Controlo de Riscos do Grupo El Corte Inglés deve ser informada destas adesões e das suas renovações quando estas forem formalizadas.

Quando se produzirem alterações significativas na presente Política, entendidas como aquelas que requerem a aprovação formal do Conselho de Administração do El Corte Inglés, S.A., os compromissos anteriores deverão ser formalmente renovados.

Uma vez que o cumprimento das normas e padrões éticos é um compromisso de toda a Organização e constitui um objetivo estratégico para a mesma, espera-se que todos os Membros da Organização conheçam e respeitem o conteúdo da presente Política. Do mesmo modo, e no que respeita aos Parceiros de Negócio, espera-se que estes desenvolvam comportamentos em consonância com a mesma.

A Organização reagirá imediatamente a eventuais violações das disposições da presente Política, em cumprimento com as disposições dos seus regulamentos internos e de acordo com a legislação aplicável em vigor.

9. COMUNICAÇÃO DE INCUMPRIMENTOS

9.1 Não conformidade com os regulamentos de segurança da informação

Todos os Membros da Organização, Parceiros Comerciais ou Terceiros com relação direta e legítimo interesse comercial ou profissional, e outras partes interessadas, no caso de detetarem um incumprimento da presente Política ou de terem dúvidas sobre se alguma prática observada pode constituir um ato ilícito, tanto no setor público como no privado, têm a obrigação de contactar imediatamente a Direção de Compliance e Controlo de Riscos do Grupo El Corte Inglés através do Canal Ético, em qualquer um dos seus canais de comunicação:

- **Canal digital:**

  O Grupo El Corte Inglés dispõe de um canal digital ao qual se pode aceder através do seguinte endereço web:

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

  Este acesso está disponível no sítio Web da empresa e, adicionalmente, na intranet da NEXO para os membros da NEXO.

- **Endereço postal:**

  El Corte Inglés, S.A.
  Cumprimento e gestão de riscos
  c/ Hermosilla, 112
  28009 Madrid

- **Departamento de Cumprimento Regulamentar Telefone:** 91 401 85 00

- **Solicitar uma reunião pessoalmente ou por meios telemáticos**

As informações transmitidas por esta via são confidenciais, tal como a identidade dos informadores, a quem a Organização agradece a sua colaboração e em relação aos quais garante que não haverá represálias.

Além disso, o Departamento de Cumprimento e Controlo de Riscos pode agir por sua própria iniciativa para investigar quaisquer indícios de incumprimento da presente política.

9.2 Notificação de incidentes de segurança da informação

Qualquer Membro da Organização, Parceiro de Negócio ou Terceiro com relação direta e legítimo interesse comercial ou profissional, no caso de detetar um evento de segurança que possa provocar um incidente nos sistemas de informação do Grupo, tem a obrigação de contactar imediatamente o Centro de Operações de Segurança (COS) do Grupo El Corte Inglés, através dos seguintes canais de comunicação:

- **Caixa de correio:**

  O COS do Grupo El Corte Inglés tem a seguinte caixa de correio:

  cos_notificaciones@elcorteingles.es

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

10. APROVAÇÃO, ENTRADA EM VIGOR E ATUALIZAÇÃO

A presente Política entrará em vigor na data da sua aprovação pelo Conselho de Administração do El Corte Inglés, S.A.

Esta Política deve ser mantida atualizada ao longo do tempo. Para o efeito, deve ser revista numa base anual ordinária e, numa base extraordinária, e em qualquer caso o mais rapidamente possível, quando se verificarem variações significativas nos objetivos estratégicos ou na regulamentação externa ou interna aplicável que impliquem a sua atualização ou modificação.

As propostas de alteração são apresentadas ao Comité de Auditoria e Controlo pelo Comité de Segurança da Informação, após validação pela Direção de Assessoria Jurídica e pela Direção de Cumprimento e Controlo de Riscos e com a correspondente supervisão do organismo de controlo interno responsável pela função.

Se as alterações forem materiais, devem ser apresentadas ao Conselho de Administração para aprovação, mediante proposta do Comité de Auditoria e Cumprimento Normativo.

11. DIVULGAÇÃO E APLICAÇÃO

Esta Política estará disponível no NEXO para todos os Membros da Organização e na página web corporativa para todos os grupos de interesse do Grupo, uma vez aprovada pelo Conselho de Administração do El Corte Inglés, S.A.

Da mesma forma, o Comité de Segurança da Informação será responsável por promover as ações necessárias para a sua adequada divulgação e conhecimento.

12. CONTROLO, ACOMPANHAMENTO E SUPERVISÃO

12.1 Controlo e monitorização

O Subcomité de Segurança da Informação avalia periodicamente o cumprimento e a eficácia da presente política através de análises, controlos e auditorias internos e externos coordenados pelo Departamento de Segurança da Informação e Cibersegurança e comunica os resultados ao Comité de Segurança da Informação.

O Comité de Segurança da Informação é responsável pela supervisão contínua da aplicação das disposições da presente Política pelas empresas do Grupo.

12.2 Controlo

O Departamento de Auditoria Interna analisará a adequação e eficácia das medidas aplicadas no SGSI para supervisionar o cumprimento das normas aplicáveis às diferentes atividades da Organização, na medida em que o Plano Anual de Auditoria aprovado pela Comissão de Auditoria e Controlo inclua trabalhos relacionados com o referido Sistema e, extraordinariamente, como consequência da ocorrência de incidentes ou da identificação de irregularidades. Como resultado destas auditorias, a Auditoria Interna emitirá o relatório correspondente, emitindo recomendações no caso de serem identificadas oportunidades de melhoria.

As oportunidades de melhoria que possam ser potencialmente identificadas em resultado destas análises devem ser consideradas no processo de melhoria contínua do sistema.

A avaliação de uma eventual violação da Política Corporativa de Segurança da Informação será determinada no procedimento correspondente, de acordo com as disposições em vigor, sem prejuízo das responsabilidades legais, incluindo as de caráter sancionatório no âmbito laboral, que, se for caso disso, possam ser exigidas ao incumpridor.

CONTROLO CAMBIAL

Versão 2.0 aprovada pelo Conselho de Administração em 30/11/2020

Versão	Data de alteração	Objeto da alteração	Artigos em causa
1.1	28/06/2023	- Incorporação de canais de comunicação	- Comunicação de incumprimentos
2.0	30/10/2024	- Adaptação ao novo quadro estratégico e regulamentar - Adaptação da política aos requisitos da Diretiva relativa aos relatórios de sustentabilidade das empresas. - Incorporação do processo de diligência devida. - Inclusão de referência ao novo regulamento interno para a adesão das empresas do Grupo às Políticas Corporativas. - Atualização dos canais digitais para a comunicação de incumprimentos. - Incorporação da secção de divulgação	- Todos

Última revisão, outubro de 2024

Anexos

Anexo I - Definições

As definições dos termos frequentemente utilizados no presente documento são apresentadas a seguir.

Ativo de informação: qualquer informação ou sistema relacionado com o processamento de informação que tenha valor para a organização, como processos empresariais, dados, aplicações, equipamento informático, pessoal, suportes de informação, redes, equipamento auxiliar ou instalações.

Ameaça: uma circunstância desfavorável que pode ocorrer e que, quando ocorre, tem um impacto negativo nos ativos, causando a sua indisponibilidade, mau funcionamento ou perda de valor.

Confidencialidade: refere-se à proteção de dados e sistemas para evitar ameaças como o acesso não autorizado ou a fuga de dados que possam resultar na divulgação, alteração ou destruição de informações sensíveis.

Disponibilidade: a capacidade de um serviço, sistema ou informação ser acessível e utilizável por utilizadores ou processos autorizados quando necessário.

Incidente de segurança: qualquer evento que afete a confidencialidade, a integridade ou a disponibilidade dos ativos de informação da empresa, por exemplo, acesso ou tentativa de acesso a sistemas, utilização não autorizada, divulgação, modificação ou destruição de informações.

Integridade: propriedade da informação, que garante a exatidão dos dados transportados ou armazenados, assegurando que não foram alterados ou perdidos.

Política de segurança da informação: documento de nível executivo através do qual uma empresa estabelece as suas orientações, decisões e medidas de segurança relativas à segurança dos seus sistemas de informação, após ter avaliado o valor dos seus ativos e os riscos a que estão expostos.

Resiliência: a capacidade de uma organização para construir, assegurar e rever a sua integridade operacional e fiabilidade, de modo a sustentar a prestação contínua de serviços.

Risco: é a possibilidade de ocorrência de incidentes ou eventos que comprometam a confidencialidade, a integridade ou a disponibilidade dos dados e sistemas da organização.

Segurança da informação: um conjunto de tecnologias, práticas e medidas destinadas a proteger a confidencialidade, a integridade e a disponibilidade da informação.