POLÍTICA EMPRESARIAL DE SEGURANÇA DA INFORMAÇÃO

Aprovada pelo Conselho de Administração do El Corte Inglés a 25 de novembro de 2020

Grupo El Corte Inglés

Índice

1. Introdução

O Conselho de Administração da El Corte Inglés, S.A. é responsável pela formulação da Estratégia e Políticas Empresariais do Grupo de Empresas El Corte Inglés (GRUPO ECI), bem como pela aprovação dos programas e sistemas de conformidade e controlo interno.

Para o Grupo ECI, a informação, em qualquer dos formatos disponíveis (informação física, ficheiros electrónicos, etc.), é um activo estratégico que requer uma adequada protecção, contribuindo para a competitividade, para o cumprimento da legalidade vigente e para a boa imagem comercial. É por isso que, com o objectivo de estabelecer os princípios gerais que devem reger o tratamento da informação em todas as Empresas do Grupo ECI, o Conselho de Administração, através e como consequência da proposta da Comissão de Auditoria e Controlo, aprovou a seguinte Política Empresarial de Segurança da Informação Empresarial do Grupo ECI, doravante a PESI.

2. Objectivo

A PESI visa garantir uma protecção adequada da informação, independentemente do formato em que é apresentada, para que as empresas do Grupo ECI estejam preparadas para prevenir, detectar, reagir e recuperar de incidentes de segurança da informação.

O Grupo ECI compromete-se a implementar as medidas técnicas e organizacionais necessárias para que a informação, independentemente do formato em que é apresentada, seja suficientemente protegida contra qualquer ameaça com potencial para afectar a sua confidencialidade, integridade e disponibilidade.

3. Âmbito de aplicação e órgãos intervenientes

Para a implementação da PESI, a Comissão de Segurança da Informação desenvolverá regulamentos internos para a gestão global da segurança da informação, em função da importância relativa da mesma para o Grupo ECI.

A PESI, bem como o regulamento interno que a desenvolve, serão supervisionados pelo Comité de Segurança da Informação e serão aplicáveis a todas as empresas do Grupo ECI, aos seus administradores, executivos e funcionários, bem como a todas as pessoas que estejam relacionadas com as empresas pertencentes ao Grupo ECI.

Por outro lado, os profissionais, órgãos internos e/ou comités que assumam estas funções em cada um dos âmbitos em que o Grupo ECI opera, com a intervenção obrigatória do Comité de Segurança da Informação, estabelecerão os procedimentos internos de carácter específico que apliquem os princípios estabelecidos na PESI, adaptando o seu conteúdo em função do regulamento aplicável.

O Comité de Segurança da Informação é responsável por zelar para que as práticas e procedimentos internos do Grupo ECI e das suas empresas estejam em conformidade com os regulamentos de segurança da informação aplicáveis num determinado momento, e deve divulgar e informar sobre qualquer nova regulamentação que seja publicada e entre em vigor.

Em virtude desta Política Empresarial, nos seus regulamentos e procedimentos de desenvolvimento serão definidas medidas de segurança que serão aplicadas, conforme determinado nos referidos regulamentos, a todos os serviços, sistemas e outros recursos do Grupo de Empresas ECI, para garantir o cumprimento dos regulamentos internos sobre a gestão global da segurança da informação, mantendo os referidos desenvolvimentos pontualmente actualizados.

Como suporte às actividades do Comité de Segurança da Informação, as diferentes áreas e departamentos deverão, além de colaborar com o Comité:

- Designar os coordenadores da segurança da informação no seu âmbito. Estas pessoas agirão de acordo com as directrizes do Comité de Segurança da Informação.
- Informar sobre a existência e/ou a criação de qualquer ficheiro e/ou base de dados com informação que devam ser protegidos, independentemente de quem tenha gerado a informação.

4. Princípios de segurança do tratamento da informação

Os princípios que regem a PESI são os seguintes:

4.1 Princípios gerais:

1. As Empresas do Grupo ECI cumprirão a legislação em matéria de segurança e protecção da informação, aplicável nos países em que opera.

2. O Comité de Segurança da Informação zelará pelo cumprimento dos princípios de confidencialidade, integridade e disponibilidade da informação do Grupo ECI, independentemente do formato que tenha a informação.

3. O Grupo ECI deve assegurar que os princípios reunidos na PESI sejam tidos em conta: (i) durante a concepção e implementação dos procedimentos estabelecidos para o Grupo ECI e suas empresas; (ii) nos produtos e serviços oferecidos pelo Grupo ECI e suas empresas; (iii) em todos os contractos e obrigações celebrados ou assumidos pelo Grupo ECI e suas empresas; e (iv) na implementação de sistemas e plataformas que permitam o acesso dos trabalhadores ou de terceiros à informação do Grupo ECI e das suas empresas.

4. A segurança da informação deve ser entendida como um processo integral que envolve todos os intervenientes, assim como os diferentes elementos técnicos, materiais e organizacionais envolvidos em actividades em que se gere informação do Grupo ECI. Consequentemente, devem ser tomadas medidas adequadas para garantir que todas as pessoas envolvidas na gestão e utilização da informação tenham conhecimento da PESI e desempenhem as suas funções em conformidade com a mesma.

5. O desenvolvimento da PESI deverá:

   - ser adequado ao propósito da Organização;
   - incluir objectivos de segurança da informação e/ou proporcionar um quadro de referência para o estabelecimento dos objectivos de segurança da informação aplicáveis às empresas do Grupo ECI;
   - determinar as medidas técnicas e/ou organizacionais de segurança que devem ser implementadas em conformidade com a apetência pelo risco definida. As referidas medidas não poderão ser recusadas pelos “donos e/ou geradores” da informação sem uma causa justificada, que deverá estar convenientemente aprovada.

4.2 Gestão de riscos:

A análise e a gestão de riscos são uma parte essencial do processo de segurança da informação. Os níveis de risco devem ser mantidos dentro de parâmetros adequados, através da aplicação de medidas técnicas e organizacionais de segurança adequadas e continuamente actualizadas, de modo a estabelecer um equilíbrio e proporcionalidade

entre a natureza da informação pertencente ao Grupo ECI, os riscos a que está exposta e as medidas de segurança a implementar.

4.3 Gestão de incidentes de segurança:

O Grupo de empresas El Corte Inglés deve dispor de um serviço de resposta a incidentes de segurança da informação que esteja dotado dos meios necessários para responder a tais incidentes.

Este serviço poderá aplicar as medidas de correcção necessárias incluindo, entre outras, a desconexão ou isolamento de dispositivos nos casos que suponham um risco potencial ou real para o resto dos sistemas de informação.

Qualquer utilizador deve comunicar, por meios a ser determinados, quaisquer incidentes e/ou fraquezas que consiga identificar e que estejam relacionados com a segurança da informação.

No sistema de gestão de incidentes deve centralizar-se a recolha, análise e gestão dos incidentes identificados.

4.4 Princípios relativos à recolha de informação:

De acordo com a legislação aplicável em todos os momentos, em relação aos processos de recolha de informações e processamento de dados sobre accionistas, funcionários, clientes, visitantes, fornecedores, etc., informá-lo-emos de forma transparente, expressa, precisa e inequívoca sobre a finalidade para a qual as informações e/ou dados são recolhidos.

4.5 Princípios de medidas de segurança e confidencialidade:

As Empresas do Grupo ECI deverão conceber, implementar, executar e manter todas as medidas de segurança organizacionais e técnicas que sejam necessárias para garantir que a recolha, tratamento e protecção da informação é realizada cumprindo os requisitos legalmente estabelecidos.

Da mesma forma, terceiros que lidam com empresas do Grupo devem cumprir as directrizes de segurança da informação estabelecidas nesta Política Empresarial e regulamentos associados.

Em conformidade com a legislação aplicável, as informações recolhidas e tratadas pelas Empresas do Grupo ECI e terceiros relacionados com as mesmas serão mantidas com a devida confidencialidade e sigilo, e não serão utilizadas para fins diferentes daqueles para os quais foram recolhidas e não poderão ser comunicadas ou transferidas para terceiros fora dos casos permitidos por lei e em conformidade com os procedimentos legalmente estabelecidos. Os períodos de conservação indicados para cada caso específico deverão também ser respeitados.

4.6 Princípios sobre as aquisições e as transferências de informação:

É proibida a aquisição e/ou recolha e/ou transferência de informação de fontes ilegítimas que não possam garantir a origem legítima da informação disponibilizada e/ou não possam garantir a protecção adequada da informação.

4.7 Princípios sobre a contratação de encarregados do tratamento:

A contratação de prestadores de serviços externos que, em virtude da actividade ou serviço a prestar, possam ter acesso a informação da responsabilidade das Empresas do Grupo ECI, deverá ser verificada e deverá confirmar-se que o prestador de serviços reúne as garantias necessárias e cumpre as medidas de segurança exigidas em cada jurisdição em que o Grupo ECI opera durante o período da relação contratual.

4.8 Transferências internacionais de informação:

Todo o tratamento de informação sujeito ao regulamento da União Europeia que implique uma transferência da mesma fora do Espaço Económico Europeu deverá ser levado a cabo dentro do estrito cumprimento dos requisitos estabelecidos na lei aplicável.

Da mesma forma, as Empresas do Grupo localizadas fora da União Europeia devem cumprir os requisitos estabelecidos na sua jurisdição para realizar uma transferência internacional de informação.

4.9 Formação e sensibilização do pessoal:

A formação dos funcionários em matéria de Segurança da Informação é crucial para as empresas do Grupo ECI, por isso deve ser estabelecido um conjunto de acções de formação para garantir os conhecimentos, competências e atitudes dos funcionários,

com o objectivo de melhorar as actividades relacionadas com a segurança da informação.

É fundamental que os conhecimentos adquiridos não se tornem obsoletos e para isso devem estabelecer-se os meios necessários para actualizar periodicamente os conhecimentos e obter, por parte de cada funcionário, um desempenho eficaz e diligente no tratamento da segurança da informação.

5. Avaliação, controlo e supervisão

O Comité de Segurança da Informação avaliará periodicamente a conformidade e eficácia da PESI e comunicará o resultado ao Comité de Direcção de Segurança da Informação.

O Comité de Segurança da Informação é responsável pelo acompanhamento contínuo da implementação do disposto na PESI pelo Grupo ECI e suas empresas.

6. Aprovação, entrada em vigor e actualização

A alteração desta Política é competência do Conselho de Administração.

Esta Política deverá manter-se actualizada ao longo do tempo. Para o efeito, deve ser revista anualmente e de forma extraordinária sempre que haja alterações significativas nos objectivos estratégicos ou no regulamento aplicável. As propostas de alteração serão apresentadas à Comissão de Auditoria e Controlo pelo Comité de Segurança da Informação, após validação pelo Departamento Jurídico e de Conformidade e com a correspondente supervisão do órgão de controlo interno encarregado desta função. Caso a Comissão de Auditoria e Controlo a considerar apropriada, deverá submetê-la ao Conselho de Administração para aprovação final.

CONTROLO DE MUDANÇAS

POLÍTICA EMPRESARIAL DE SEGURANÇA DA INFORMAÇÃO

Primeira Versão

Data de aprovação: Ref. Doc. Cumprimento: