

Política Corporativa De Ciberresiliência

**Aprovada pelo Conselho de Administração
do El Corte Inglés, S.A.
em 29 de outubro de 2025**

Versão 1.0 de 29 de outubro de 2025

ÍNDICE

1. INTRODUÇÃO	1
2. OBJETIVO.....	1
3. ÂMBITO DE APLICAÇÃO	1
4. PRINCÍPIOS DE AÇÃO	2
5. ESTRUTURA ORGANIZACIONAL	3
6. COMPONENTES DO SGCr	4
7. ANÁLISE LEGAL E REGULAMENTAR.....	4
8. NECESSIDADES E EXPECTATIVAS DAS PARTES INTERESSADAS	5
9. DILIGÊNCIA DEVIDA	7
10. CONHECIMENTO E DECLARAÇÃO DE CONFORMIDADE	8
11. COMUNICAÇÃO DE INCUMPRIMENTOS.....	8
11.1 Incumprimentos da regulamentação em matéria de segurança da informação	8
12. APROVAÇÃO, ENTRADA EM VIGOR E ATUALIZAÇÃO	9
13. DIVULGAÇÃO E APLICAÇÃO.....	9
14. CONTROLO, MONITORIZAÇÃO E SUPERVISÃO	9
14.1 Controlo e monitorização	9
14.2 Supervisão	10
Anexo I - Definições	12

NOTA: O Anexo I contém as definições dos termos frequentemente utilizados no presente documento e nos regulamentos conexos que integram o Sistema de Gestão de Ciberresiliência, bem como os que integram o Sistema de Gestão de Conformidade 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 capacidade operacional do Grupo tem sido considerada um dos seus ativos estratégicos, sendo fundamental para a sustentabilidade e a competitividade da Organização. Nesse contexto, com o objetivo de estabelecer os princípios gerais que devem reger a ciberresiliência em todas as empresas do Grupo, o Conselho de Administração aprovou a presente Política Corporativa de Ciberresiliência (doravante, a «Política»).

A presente Política encontra-se alinhada com os valores do Grupo, reiterando a sua firme vontade de contribuir para os 17 Objetivos de Desenvolvimento Sustentável das Nações Unidas e de manter uma conduta respeitadora tanto das normas aplicáveis às suas atividades como dos padrões éticos e das demais normas e iniciativas que o Grupo se compromete a observar através de certificação ou adesão, designadamente DORA, CRA, ENS, NIS2, entre outras, bem como das boas práticas reconhecidas, como ISO/IEC 27001:2020, UNE-ISO/IEC 22301:2020 e UNE-ISO/IEC 22316:2020, entre outras.

A presente Política constitui a base do Sistema de Gestão de Ciberresiliência (doravante, "SGCr"), a partir do qual se definem a estratégia e a operacionalização da Organização.

2. OBJETIVO

O objetivo da presente Política é estabelecer os princípios, compromissos e diretrizes que permitem ao Grupo antecipar, resistir, responder e recuperar face a ameaças e oportunidades no âmbito cibernético, suscetíveis de afetar a continuidade operacional, a segurança e a integridade da informação e a resiliência organizacional.

A aplicação destes princípios permite:

- reduzir o impacto dos incidentes no âmbito cibernético;
- aumentar a capacidade de antecipação e de resposta;
- promover a melhoria contínua do sistema de gestão e da resiliência organizacional;
- assegurar a continuidade operacional e manter a confiança dos clientes;
- cumprir a legislação aplicável.

A presente Política pretende constituir um instrumento que promova uma tomada de decisões informada, alinhada com o apetite ao risco do Grupo, com os requisitos regulamentares e com as expectativas das partes interessadas.

3. ÂMBITO DE APLICAÇÃO

A presente Política é de cumprimento obrigatório e aplica-se globalmente às empresas que compõem o Grupo, bem como aos seus colaboradores, parceiros e terceiros, em todas as atividades relacionadas com a sua cadeia de valor, tanto a montante como a jusante, independentemente do país em que se desenvolvam.

Todos os Membros da Organização e os parceiros comerciais, 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.

Este compromisso deve ser formalizado tal como previsto na secção 10. "Conhecimento e declaração de conformidade" da presente Política.

A Política aplica-se igualmente a todos os recursos* utilizados nos diferentes ambientes operacionais do Grupo.

4. PRINCÍPIOS DE AÇÃO

O Grupo espera de todos os Membros da Organização, bem como dos seus Parceiros Comerciais e demais intervenientes, a observância dos seguintes princípios de atuação, que estabelecem as bases da Ciberresiliência Corporativa:



Princípio 1: Governança e liderança comprometida.

A Alta Direção assume um papel ativo no desenvolvimento, supervisão e melhoria da ciberresiliência, garantindo a integração dos objetivos de continuidade e de resiliência na estratégia empresarial. Devem ser alocados os recursos necessários e definida uma governança clara, com papéis e responsabilidades para a tomada de decisões, em especial em situações de crise no âmbito cibernético.



Princípio 2: Cultura organizacional resiliente.

É promovida uma cultura organizacional orientada para a prevenção, a colaboração e a resposta proativa face a ameaças no âmbito cibernético. Todo o pessoal deve receber formação, ações de sensibilização e os mecanismos necessários para atuar de forma coerente com os objetivos de resiliência e de segurança.



Princípio 3: Abordagem baseada na gestão de riscos

A estratégia do Grupo baseia-se na identificação e avaliação dos riscos suscetíveis de afetar os seus processos críticos, visando uma ciberresiliência eficaz. Esta avaliação é realizada de forma sistemática e contínua, considerando ameaças internas e externas, com vista à prevenção, à priorização de ações e à garantia da continuidade do negócio em cenários disruptivos.



Princípio 4: Preparação e capacidade de resposta.

A Organização desenvolve e implementa planos que asseguram uma resposta ágil e coordenada, limitando o impacto de qualquer evento no âmbito cibernético sobre as operações e os processos críticos. Estes planos devem ser previamente testados, de modo a garantir que os intervenientes sabem como atuar de forma eficaz.



Princípio 5: Proteção de recursos críticos.

São implementados controlos e medidas de segurança diferenciados para proteger os recursos mais relevantes da Organização, incluindo sistemas, dados, pessoas e processos críticos. A proteção baseia-se no respetivo nível de criticidade e no impacto que uma ameaça poderá ter sobre a operação.



Princípio 6: Comunicação eficaz.

O Grupo garante a existência de canais de comunicação interna e externa claros, acessíveis e redundantes para a gestão de crises no âmbito cibernético. A informação relevante flui em tempo real entre as partes interessadas, facilitando uma resposta eficiente, coerente e alinhada com os princípios da transparência e da responsabilidade.



Princípio 7: Colaboração com terceiros.

O Grupo comunica estes princípios aos fornecedores e às partes interessadas no âmbito da gestão dos riscos que possam afetar os processos críticos. 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 8: Conformidade normativa e contratual.

A ciberresiliência é gerida em conformidade com as leis, regulamentos, normas e compromissos contratuais aplicáveis em matéria de segurança da informação, resiliência e continuidade do negócio. A conformidade é objeto de auditorias periódicas, sendo as alterações regulamentares geridas de forma proativa.



Princípio 9: Transparência e melhoria contínua.

É estabelecido um ciclo de revisão e melhoria contínua que incorpora as lições aprendidas, os resultados de exercícios e simulacros, as auditorias internas e as mudanças no ambiente tecnológico. A Política, os controlos e os procedimentos de ciberresiliência são atualizados de forma sistemática, assegurando a sua eficácia ao longo do tempo.

Estes princípios constituem a base operacional e estratégica sobre a qual se desenvolve a capacidade da Organização para resistir, adaptar-se e recuperar de ameaças cibernéticas, garantindo a sua sustentabilidade e competitividade a longo prazo.

5. ESTRUTURA ORGANIZACIONAL

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

5.1. Governação da Ciberresiliência.

A Governação assenta na **Direção de Prevenção e Segurança Corporativa**, órgão de referência responsável por liderar, coordenar e supervisionar a estratégia global de segurança e de ciberresiliência, garantindo o seu alinhamento com os objetivos corporativos e com o quadro normativo aplicável.

Sob a sua supervisão estruturam-se os seguintes órgãos colegiais:

- **Gabinete Consultivo em matéria de Crises, Emergências e Catástrofes:** órgão principal e de maior relevância, de natureza consultiva e de apoio estratégico à Alta Direção, responsável por assessorar na tomada de decisões críticas, recomendar a ativação de planos de gestão de crises e coordenar a interlocução com autoridades e entidades externas.

- **CSI (Comité de Segurança da Informação):** comité multidisciplinar e de carácter periódico que promove e supervisiona a segurança da informação em toda a Organização, assegurando que as boas práticas são aplicadas de forma transversal e consistente.

5.2. Gestão da Ciberresiliência

A **Gestão** é articulada através da **Área de Ciberresiliência**, integrada no âmbito de GRC. Esta unidade coordena, define e regula as capacidades de ciberresiliência do Grupo, garantindo a coerência das atuações em todos os âmbitos organizacionais e promovendo a adoção de políticas, procedimentos e controlos comuns.

5.3. Operação da Ciberresiliência

A **Operação** cabe às **áreas operacionais** responsáveis pela execução das medidas e capacidades de ciberresiliência. Estas áreas asseguram a correta aplicação dos recursos necessários para manter a resiliência organizacional, incluindo, designadamente, pessoas, localizações, tecnologia, terceiros, segurança, entre outros.

6. COMPONENTES DO SGCr

O Sistema de Gestão de Ciberresiliência (SGCr) constitui o enquadramento organizacional adotado pelo Grupo e assenta em quatro componentes fundamentais que suportam o seu funcionamento eficaz:

- **Estratégia de Ciberresiliência:** abordagem de alto nível definida pelo Grupo com o objetivo de assegurar a capacidade de antecipar, resistir e recuperar face a ameaças. Inclui documentos que apresentam a declaração dos princípios e valores da Organização em matéria de ciberresiliência, bem como o respetivo alinhamento com a estratégia corporativa e os objetivos de negócio.
- **Quadro Normativo de Ciberresiliência:** desenvolvimento de um conjunto de políticas, normas, e procedimentos gerais e específicos que abranjam os requisitos identificados no quadro de controlo e na regulamentação aplicável.
- **Quadro de Controlo de Ciberresiliência:** estabelece a estrutura técnica e organizacional de controlos destinada a adaptar e proteger os ativos, gerir os riscos e assegurar a recuperação dos processos de negócio do Grupo.
- **Scorecard de Ciberresiliência:** ferramenta que permite medir e avaliar o desempenho das ações e dos processos associados à ciberresiliência.

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. ANÁLISE LEGAL E REGULAMENTAR

O Grupo reconhece a necessidade de cumprir integralmente todas as obrigações legais, regulamentares e contratuais relacionadas com a segurança da informação, a proteção da privacidade dos dados e a continuidade do negócio. Nesse sentido, o componente legal da ciberresiliência é considerado uma prioridade estratégica.

Quadro normativo aplicável

A Organização compromete-se a identificar, acompanhar e cumprir a legislação em vigor em todas as jurisdições em que opera, incluindo, nomeadamente, mas não se limitando a:

- **Legislação em matéria de proteção de dados pessoais**, como o Regulamento Geral sobre a Proteção de Dados (RGPD) na União Europeia;

- **Normas e regulamentos específicos de cibersegurança** aplicáveis ao setor do retalho ou a setores regulados (por exemplo, PCI-DSS para o tratamento de dados de cartões de pagamento, ISO, ENS, entre outros);
- **Leis de notificação obrigatória de incidentes**, como as que exigem a comunicação de violações de dados às autoridades competentes ou aos titulares dos dados.
- **Requisitos impostos por entidades de supervisão financeira ou de defesa do consumidor**, sempre que aplicáveis a plataformas de pagamento, comércio eletrónico ou serviços de crédito.

Obrigações contratuais

Inclui-se igualmente a análise das cláusulas de segurança e ciberresiliência nos contratos celebrados com terceiros, parceiros tecnológicos, operadores logísticos e prestadores de serviços em nuvem, assegurando que:

- sejam claramente definidas as responsabilidades em caso de incidentes de segurança;
- sejam estabelecidos prazos máximos de resposta e de notificação (SLA); e
- seja incluído o direito de auditoria relativamente aos controlos de segurança implementados.

8. NECESSIDADES E EXPECTATIVAS DAS PARTES INTERESSADAS

A identificação e a gestão das necessidades e expectativas das partes interessadas são fundamentais para assegurar o seu alinhamento com o contexto interno e externo do Grupo.

As seguintes partes interessadas foram identificadas como críticas para o desempenho, a sustentabilidade e a resiliência da Organização:

PARTE INTERESSADA	PAPEL
Clientes	Utilizadores finais de produtos e serviços.
Colaboradores	Executores de processos, operadores de sistemas e atendimento ao cliente.
Responsáveis pelos processos de negócio	Definem os requisitos mínimos necessários para assegurar a execução dos processos críticos.
Alta Direção e acionistas	Responsáveis pelo governo corporativo e pela estratégia do negócio.
Fornecedores e terceiros	Fornecimento de produtos, tecnologia e serviços críticos.
Entidades reguladoras	Supervisão do cumprimento legal e regulamentar.
Parceiros comerciais	Alianças estratégicas, franchisados e operadores logísticos.
Comunidade e sociedade	Enquadramento social, ambiental e económico.
Organismos de resposta	Forças de segurança, autoridades de proteção civil e CERTs.

De acordo com os princípios das normas ISO 22301 e ISO 22316, a compreensão das necessidades e expectativas das partes interessadas é essencial para reforçar a continuidade operacional e a resiliência organizacional. Esta identificação permite alinhar as capacidades de resposta com os requisitos do contexto envolvente e gerar confiança entre os principais intervenientes. De seguida, apresentam-se as principais necessidades e expectativas, em função do papel desempenhado por cada parte interessada:

Clientes

- Acesso ininterrupto aos canais de venda (físicos e digitais).
- Proteção dos seus dados pessoais e financeiros.
- Transparência em caso de incidentes que os possam afetar.
- Confiança na disponibilidade e segurança dos serviços.

Colaboradores

- Formação adequada sobre papéis e responsabilidades em matéria de ciberresiliência e continuidade.
- Canais de trabalho seguros, especialmente em modelos híbridos ou remotos.
- Procedimentos claros de atuação em caso de incidentes ou situações de crise.
- Confiança na Organização enquanto local de trabalho seguro e estável.

Responsáveis pelos processos de negócio

- Definição e validação dos requisitos de continuidade do negócio e dos tempos de recuperação (RTO/RPO) aplicáveis aos respetivos processos.
- Garantia da disponibilidade dos recursos críticos (tecnologia, pessoas e instalações) em cenários de interrupção.
- Acesso a informação atempada sobre riscos e vulnerabilidades suscetíveis de afetar as operações.
- Participação em exercícios de simulação, testes e revisões do sistema de gestão da continuidade e da ciberresiliência.
- Coordenação fluida com as áreas de TI, segurança da informação e gestão de crises, assegurando o alinhamento das capacidades de resposta com os objetivos do negócio.
- Tomada de decisões informada, com base em análises de impacto no negócio (BIA) e avaliações de risco.
- Confiança de que a Organização protege e prioriza a resiliência dos processos críticos para assegurar a continuidade operacional.

Alta Direção e acionistas

- Alinhamento da ciberresiliência com a estratégia empresarial.
- Minimização dos impactos financeiros, operacionais e reputacionais em situações de crise.
- Conformidade normativa e mitigação dos riscos legais.
- Reportes claros e periódicos sobre o nível de preparação e maturidade organizacional.

Fornecedores e terceiros

- Definição clara de requisitos de segurança e continuidade nos contratos.
- Estabelecimento de SLA e tempos de recuperação (RTO/RPO).
- Procedimentos definidos de comunicação em caso de incidentes.
- Interoperabilidade e confiança mútua em situações de contingência.

Entidades reguladoras e de cumprimento

- Cumprimento da legislação em matéria de proteção de dados (por exemplo, o RGPD).
- Notificação adequada e atempada de incidentes e violações de segurança.
- Disponibilidade de evidência documental relativa a planos, testes e controlos implementados.
- Participação em auditorias, inspeções ou ações de supervisão, quando aplicável.

Parceiros comerciais e franchisados

- Garantia da continuidade das operações partilhadas.
- Integridade e fiabilidade dos dados transacionais.
- Acesso a plataformas corporativas com elevados padrões de segurança.
- Apoio e alinhamento em situações de incidentes graves ou crises reputacionais.

Comunidade e sociedade

- Comportamento ético e responsável por parte da Organização.
- Gestão de crises que minimize o impacto sobre os consumidores e o emprego.
- Transparência na comunicação pública de eventos relevantes.
- Contributo para a estabilidade social e económica do contexto envolvente.

Organismos de resposta a emergências

- Coordenação eficaz em caso de desastres ou ataques cibernéticos.
- Acesso a informação crítica e relevante sobre incidentes.
- Colaboração em exercícios conjuntos e simulacros.

Estas necessidades e expectativas são revistas periodicamente, através da análise do contexto organizacional, da realização de inquéritos e de reuniões com partes interessadas relevantes.

Para o efeito, são utilizadas ferramentas como o mapeamento de influência e impacto, bem como a monitorização de reclamações e não conformidades, assegurando uma adaptação contínua às alterações do contexto e reforçando a resiliência do Grupo.

9. DILIGÊNCIA 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 prestem, ou potencialmente possam prestar, suporte aos processos de negócio 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 Ciberresiliência 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 Ciberresiliência e a aplicar as medidas técnicas e organizacionais que garantam a proteção correta dos recursos 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 recursos, a eliminação da informação e a revogação dos acessos à informação por parte do terceiro.

10. CONHECIMENTO E DECLARAÇÃO DE CONFORMIDADE

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 Comerciais, espera-se que estes desenvolvam comportamentos em consonância com a mesma.

Este compromisso deve ser formalizado por meio de:

- i. Declarações dos Membros da Organização atestando a sua conformidade com os princípios estabelecidos, mediante adesão aos **Elevados Padrões Éticos**.
- ii. **Cláusulas de cumprimento incluídas nos contratos** com os Parceiros Comerciais
- iii. **Adesões expressas ou tomadas de conhecimento** pelos órgãos de administração das sociedades que integram o Grupo El Corte Inglés, nos termos da regulamentação interna elaborada para o efeito.

A Direção de Conformidade 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. De igual modo, e no que respeita aos Parceiros Comerciais, 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.

11. COMUNICAÇÃO DE INCUMPRIMENTOS

11.1 Incumprimentos da regulamentação em matéria 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 Organização.

- **Endereço postal:**

El Corte Inglés, S.A.
Direção de Conformidade e Controlo de Riscos
Hermosilla 112
28009 Madrid

- **Telefone do Departamento de Conformidade Normativa:** 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 retaliações.

Além disso, a Direção de Conformidade e Controlo de Riscos pode agir por sua própria iniciativa para investigar quaisquer indícios de incumprimento da presente Política.

12. 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 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 Conformidade e Controlo de Riscos e com a correspondente supervisão do organismo de controlo interno responsável pela Função.

Caso as alterações sejam relevantes, deverão ser submetidas à aprovação do Conselho de Administração, mediante proposta prévia da Comissão de Auditoria e Controlo.

13. DIVULGAÇÃO E APLICAÇÃO

Esta Política estará disponível na 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.

14. CONTROLO, MONITORIZAÇÃO E SUPERVISÃO

14.1 Controlo e monitorização

O Subcomité de Ciberresiliência avaliará periodicamente o cumprimento e a eficácia da presente Política através de análises, controlos e auditorias internas e externas, coordenados pelo Departamento de Segurança da Informação e Cibersegurança, e comunicará os respetivos 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.

14.2 Supervisão

O Departamento de Auditoria Interna analisará a adequação e eficácia das medidas aplicadas no SGCr 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 deverá emitir o relatório correspondente, formulando 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 um eventual incumprimento da Política Corporativa de Ciberresiliência deverá ser efetuada no procedimento correspondente, de acordo com as disposições em vigor, sem prejuízo das responsabilidades legais, incluindo as de carácter sancionatório no âmbito laboral, que, se for caso disso, possam ser exigidas ao incumpridor.

HISTÓRICO DE ALTERAÇÕES

Versão 1.0 aprovada pelo Conselho de Administração em 29 de outubro de 2025

Versão	Data de alteração	Objeto da alteração	Artigos em causa
		-	-

Última revisão, 29 de outubro de 2025

Anexos

Anexo I - Definições

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

Ativo de informação: qualquer recurso, componente ou elemento de valor para uma Organização que deve ser protegido, gerido e, se necessário, recuperado, para garantir a continuidade e a segurança das operações.

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

Ciberresiliência ou resiliência cibernética: capacidade de uma Organização para antecipar, resistir, responder e recuperar de eventos adversos, garantindo a continuidade das suas operações e a proteção dos seus ativos e recursos críticos face a ameaças com impacto no domínio cibernético.

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.

Crise: qualquer evento, incidente ou conjunto de circunstâncias que provoque uma interrupção grave da disponibilidade ou da integridade dos processos de negócio, com impacto no domínio cibernético, afetando significativamente a capacidade da Organização para operar de forma normal e exigindo uma resposta imediata e coordenada para mitigar danos, restaurar funções críticas e proteger os recursos.

Disponibilidade: a capacidade de um serviço, sistema ou processo se manter acessível e utilizável por utilizadores ou processos autorizados quando requerido.

Efetivo: que produz o efeito esperado. Refere-se ao resultado alcançado, independentemente dos meios, do tempo ou dos recursos utilizados.

Eficaz: que alcança o objetivo pretendido. Centra-se na obtenção do resultado, sem considerar se foram utilizados muitos ou poucos recursos.

Eficiente: que alcança um objetivo utilizando a menor quantidade possível de recursos (tempo, dinheiro, esforço, entre outros).

Evento: qualquer ocorrência identificável num sistema, rede ou ambiente tecnológico que possa ter relevância para a segurança da informação ou para o funcionamento normal dos processos. Um evento não implica necessariamente uma ameaça ou um dano, mas pode constituir um indício de um possível incidente ou de uma atividade anómala.

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 a Organização estabelece as suas orientações, decisões e medidas de segurança relativas à proteção dos seus sistemas de informação, após avaliar o valor dos seus ativos e os riscos a que estes estão expostos.

Recurso: todos os ativos (incluindo infraestruturas e equipamentos), pessoas, competências, tecnologia, instalações, fornecimentos e informação de que a Organização deve dispor para utilizar quando necessário, com o objetivo de operar e cumprir a sua missão.

Resiliência: a capacidade de uma organização para construir, garantir 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: conjunto de tecnologias, práticas e medidas destinadas a proteger a confidencialidade, a integridade e a disponibilidade da informação.

Sistema de Gestão: conjunto de elementos inter-relacionados de uma Organização que interagem para estabelecer políticas, objetivos e processos.