

Política de Segurança da Informação

1. OBJETIVO

A presente Política de Segurança da Informação (“Política”) visa estabelecer o Sistema de Gestão da Segurança da Informação e consolidar as diretrizes a serem adotadas pelas empresas do Grupo Ultra, seus colaboradores e Terceiros (incluindo fornecedores de produtos e/ou serviços), para tratar de Segurança da Informação, definindo papéis e responsabilidades dentro da estrutura de governança do Grupo Ultra.

Este documento deve ser considerado em conjunto com o Código de Ética e as demais políticas e normas do Grupo Ultra e de seus Negócios. Em caso de conflito desta Política com outros procedimentos da Companhia, o Comitê Diretor de Segurança da Informação deverá ser consultado.

2. ABRANGÊNCIA

Esta Política é aplicável a todas as empresas do Grupo Ultra e a todos os Colaboradores e Terceiros com acessos físicos ou digitais a informações e aos ambientes de tecnologia do Grupo Ultra e seus Negócios.

3. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Confidencialidade: As informações devem estar disponíveis apenas para indivíduos, entidades e/ou processos autorizados pelo Grupo Ultra.

Integridade: O processamento de informações no Grupo Ultra deve garantir a sua exatidão e a sua completude.

Disponibilidade: as informações e os ambientes de tecnologia do Grupo Ultra devem estar acessíveis e disponíveis aos Negócios e seus usuários de maneira permanente.

4. DOCUMENTOS RELACIONADOS

Além desta Política, aplicam-se à Segurança da Informação no Grupo Ultra as seguintes legislações e normas:

- Código de Ética do Grupo Ultra;
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD;
- Lei nº 12.965/14 – Marco Civil da Internet;
- Lei Sarbanes-Oxley – SOX;
- Política Corporativa de Gestão de Riscos;
- Política Corporativa de Privacidade e Proteção de Dados Pessoais;
- Norma de Classificação da Informação;

- Norma de Gestão de Incidente de Segurança;
- Demais Políticas, diretrizes e normas de gestão de Segurança da Informação, disponíveis na intranet e extranet do Grupo Ultra.

5. PAPÉIS E RESPONSABILIDADES

Elencamos a seguir as responsabilidades de cada um dos elementos/áreas do Grupo Ultra na melhoria e manutenção da segurança nos ambientes de informação do Grupo Ultra. As responsabilidades elencadas devem ser vistas como o mínimo a ser garantido pelos responsáveis, sem limitar ou impedir cada área de atuar de maneira abrangente em benefício da segurança.

5.1. DIRETORIA ESTATUTÁRIA DA ULTRAPAR

Compete à Diretoria Estatutária da Ultrapar:

Aprovar a Política e suas revisões;

Aprovar a composição do Comitê Diretor de Segurança da Informação; e

Deliberar acerca de eventos relacionados ao descumprimento da Política e encaminhar os casos ao Comitê de Conduta, quando aplicável.

5.2. DIRETOR RESPONSÁVEL NO NEGÓCIO

Compete ao Diretor do Negócio ao qual a área de Tecnologia ("TI") da Informação está subordinada:

Destinar investimentos para manter ativos de tecnologia atualizados, seguros e suportados pelos seus respectivos fabricantes, e para execução e manutenção dos Mecanismos de Gestão de Segurança da Informação no negócio, independentemente se tais ativos de tecnologia sejam operados ou hospedados pela TI do Negócio, ou pelo CSC, ou por fornecedores contratados pelo Negócio;

Garantir a implementação dos programas de conscientização e treinamento em Segurança da Informação elaborados e/ou propostos pela Gerência de Segurança da Informação da Holding para todos os Colaboradores e Terceiros que atuam no respectivo Negócio zelando pelo cumprimento de tais regras;

Garantir a priorização e execução de planos e investimentos para mitigação de riscos de Segurança da Informação e para garantir a conformidade com os princípios desta Política;

Monitorar e supervisionar a implementação dos planos de ação e controles mitigatórios relacionados a riscos de Segurança da Informação no seu respectivo Negócio, assegurado o apoio da Gerência de Segurança da Informação da Holding se o Negócio entender necessário; e

Assegurar a efetividade desta Política, sugerindo revisões e atualizações para o Comitê Diretor de Segurança da Informação.

5.3. DIRETORIA DE RISCO, COMPLIANCE E AUDITORIA ("DRCA")

Compete à DRCA:

Apoiar a avaliação periódica dos riscos de Segurança da Informação dos Negócios e da Holding;

Auditar a aderência dos Mecanismos de Gestão de Segurança da Informação com as Políticas, diretrizes e normas de gestão de Segurança da Informação vigentes;

Apoiar na resposta e/ou investigação de incidentes de Segurança da Informação, quando aplicável.

5.4. COMITÊ DIRETOR DE SEGURANÇA DA INFORMAÇÃO

Compõem o Comitê:

- Diretoria de Controladoria e CSC da Ultrapar;
- DRCA; e
- Diretoria Jurídica da Ultrapar.

Compete ao Comitê:

Revisar, aprovar e monitorar os Mecanismos de Gestão de Segurança da Informação para o cumprimento desta Política, e das diretrizes e normas de gestão de Segurança de Informação aplicáveis, bem como do plano de treinamento de Segurança da Informação;

Monitorar e supervisionar a implementação dos planos de ação e controles mitigatórios relacionados a riscos de Segurança da Informação;

Reportar para Diretoria Estatutária Ultrapar eventos relacionados a violações desta Política; e

Assegurar a efetividade desta Política, propondo revisões e atualizações para a Diretoria da Ultrapar.

5.5. COMITÊ GESTOR DA SEGURANÇA DA INFORMAÇÃO

Compõem o Comitê:

- Gerência de Segurança da Informação da Holding; e
- Executivos responsáveis por Tecnologia da Informação dos Negócios e do CSC.

Compete ao Comitê:

Compartilhar conhecimento, iniciativas e planos relacionados a práticas, processos, tecnologias e soluções.

Discutir, avaliar, revisar e propor:

- Mecanismos de Gestão de Segurança da Informação para o cumprimento desta Política, e das diretrizes e normas de gestão de Segurança de Informação aplicáveis;
- padrões e requisitos mínimos de Segurança da Informação nos ambientes de tecnologia.

Supervisionar e validar planos de ação e controles relacionados a riscos de Segurança da Informação; e

Atualizar o Comitê Diretor quanto às atividades e propostas discutidas no Comitê Gestor.

5.6. GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO DA HOLDING

Compete à Gerência de Segurança da Informação da Holding:

Estruturar e propor:

- as Políticas, diretrizes e normas de gestão de Segurança da Informação;
- os Mecanismos de Gestão de Segurança da Informação para o cumprimento desta Política e das diretrizes e normas de gestão de Segurança da Informação;
- o programa de conscientização e treinamento em Segurança da Informação;
- os padrões e requisitos mínimos de Segurança da Informação nos ambientes de tecnologia.

Identificar, classificar e reportar para o Comitê Diretor de Segurança da Informação ou para as Diretorias dos Negócios:

- riscos e vulnerabilidades de Segurança da Informação;
- violações a esta Política, e/ou às diretrizes e normas de gestão de Segurança da Informação.

Definir ou recomendar planos de ação e controles mitigatórios relacionados a riscos e vulnerabilidades de Segurança da Informação;

Gerir os processos de Segurança da Informação dos sistemas e infraestrutura corporativas; e

Coordenar os comitês e demais fóruns relacionados à Segurança da Informação.

5.7. EXECUTIVOS RESPONSÁVEIS POR TECNOLOGIA DA INFORMAÇÃO DO NEGÓCIO E DO CSC

Compete aos executivos responsáveis por tecnologia da informação do Negócio ou CSC:

Implementar e manter os Mecanismos de Gestão de Segurança da Informação para o cumprimento desta Política e demais diretrizes e normas de gestão de Segurança da Informação;

Garantir a implementação e manutenção dos padrões e requisitos mínimos de Segurança da Informação nos ambientes de tecnologia sob sua responsabilidade;

Elaborar, propor e implementar planos de ação e controles mitigatórios relacionados a riscos de Segurança da Informação;

Garantir a alocação e execução de recursos e investimentos necessários para:

- execução e manutenção dos Mecanismos de Gestão de Segurança da Informação;
- identificação, análise, reporte e tratamento de riscos e vulnerabilidades de Segurança da Informação;
- manter ativos de tecnologia sob sua gestão atualizados, seguros e suportados pelos seus respectivos fabricantes.

Gerir os processos de Segurança da Informação dos sistemas específicos do negócio.

5.8. COLABORADORES E TERCEIROS

Compete a todos os Colaboradores e Terceiros do Grupo Ultra:

Seguir o disposto neste documento e demais políticas, diretrizes e normas de gestão de Segurança da Informação;

Classificar o nível de confidencialidade de todo documento criado ou informação transmitida com base nos critérios da Norma de Classificação da Informação;

Relatar tempestivamente ocorrências de incidentes de Segurança da Informação através do seu gestor, do Service Desk ou diretamente para as equipes de Segurança da Informação ou de Tecnologia; e

Participar de todas as ações de treinamento e conscientização em Segurança da Informação estabelecidas pelo Grupo Ultra.

6. TREINAMENTO E CONSCIENTIZAÇÃO

Será elaborado plano anual de treinamento em Segurança da Informação contendo iniciativas, periodicidade e o conteúdo de treinamentos de prevenção e conscientização em Segurança da Informação a ser implementado no Grupo Ultra.

Todos os Colaboradores e Terceiros do Grupo Ultra deverão participar de tais treinamentos periódicos. As Diretorias dos Negócios deverão garantir que seus Colaboradores e Terceiros participem de tais treinamentos sobre os assuntos tratados nesta Política.

7. DIRETRIZES GERAIS

Esta Política deve ser observada em todos os processos e procedimentos adotados pelo Grupo Ultra, devendo a Holding e os Negócios adotar controles que demonstrem a adoção das normas aqui descritas quando apropriado.

Neste contexto, as empresas do Grupo Ultra, bem como seus Colaboradores e Terceiros, devem observar, no mínimo, as seguintes diretrizes:

Propriedade e Segurança da Informação: Toda informação criada ou adquirida no Grupo Ultra é de propriedade da empresa, devendo ser protegidas.

Classificação da informação: Toda informação de propriedade do Grupo Ultra deve ser classificada de acordo com o seu grau de confidencialidade e proteção, nos termos da Norma de Classificação da Informação.

Acesso controlado: Todo acesso à rede de computadores e aos ambientes digitais do Grupo Ultra deve ser precedido de uma ou dupla validação de identidade.

Desenvolvimento seguro: O desenvolvimento, a aquisição e a contratação de sistemas ou ativos de tecnologia devem respeitar os preceitos desta Política desde a sua concepção.

Compartilhamento de informações: Todas as transmissões de informação devem utilizar métodos de segurança e níveis de criptografia aderentes aos padrões mínimos estabelecidos.

Gestão de incidentes de Segurança da Informação: Todo incidente de Segurança da Informação deverá ser registrado, avaliado e receber uma tratativa, conforme diretrizes da Norma de Gestão de Incidente de Segurança. Todo Colaborador ou Terceiro deve reportar violações relacionadas a esta Política ou comportamentos suspeitos que possam comprometer a Segurança da Informação do Grupo Ultra.

Testes de vulnerabilidades: Os ambientes digitais do Grupo Ultra devem periodicamente ser submetidos a análises de segurança, *pentests* e testes de vulnerabilidade.

Gestão dos riscos de Segurança da Informação: A Holding e todos os Negócios deverão realizar gestão dos seus respectivos riscos de Segurança da Informação, reportando periodicamente à DRCA e a área de Segurança da Informação da Holding.

Precedência: As demandas de Segurança da Informação são prioritárias em relação às demais demandas recebidas pelas áreas de Tecnologia da Informação.

Backup: Negócios e Holding são responsáveis por manter e testar periodicamente sistemas de *backup* que garantam duplicidade e recuperação das informações e dos ambientes digitais.

Backlevel (ativos de tecnologia desatualizados): Negócios e Holding são responsáveis por manter seus respectivos ambientes tecnológicos atualizados de maneira a não comprometer a segurança.

Plano de continuidade: Negócios e Holding são responsáveis por elaborar e manter atualizado seus respectivos planos de continuidade que lhes permitam continuar operando na ocorrência de um incidente de Segurança da Informação ou indisponibilidade de seus ambientes tecnológicos.

8. INFRAÇÕES E SANÇÕES

Qualquer desrespeito ou violação às Políticas, diretrizes e normas de gestão de Segurança da Informação deverá ser reportado ao Canal Aberto Ultra.

Canal Aberto Ultra

0800 701 7172

www.canalabertoultra.com.br

Os casos serão analisados com observância às leis aplicáveis, a esta Política e aos interesses do Grupo Ultra, para que sejam tomadas as medidas cabíveis.

Para garantir sua efetividade, violações à referida Política e às demais políticas, diretrizes e normas de gestão de Segurança da Informação poderão resultar na aplicação aos Colaboradores por elas responsáveis de medidas disciplinares corporativas tais como: (a) advertências; (b) suspensões; e (c) demissões. A aplicação de tais medidas poderá ser cumulada com eventuais medidas administrativas ou judiciais cabíveis de natureza cível, criminal e trabalhista.

9. DEFINIÇÕES

Mecanismos de Gestão de Segurança da Informação: Estrutura organizacional, processos, ferramentas, controles e indicadores necessários para a implementação e gestão da Segurança da Informação no respectivo Negócio.

CSC (Centro de Serviços Compartilhados): Estrutura centralizada de operação de áreas administrativas e de suporte aos Negócios.

Colaborador(es): qualquer membro de diretoria, Conselho de Administração e Conselho Fiscal, acionista, empregado, estagiário (na forma da Lei de Estágio – Lei 11.788/2008) e jovem aprendiz (na forma da Lei de Aprendizagem, Lei 10.097/2000), que, por liame contratual tácito ou expresso, colabora de forma habitual com a consecução dos objetivos sociais das empresas que integram o Grupo Ultra.

Grupo Ultra e Negócio: Ultrapar Participações S.A. (“Ultrapar” ou “Holding”) e suas empresas controladas direta ou indiretamente controladas, no Brasil e no exterior (cada uma, individualmente, um “Negócio”).

Segurança da Informação: conjunto de padrões de comportamento ou sistemas que tem como objetivo a preservação da confidencialidade, integridade e disponibilidade, autenticidade, atribuição de responsabilidade e confiabilidade das informações utilizadas pelo Grupo Ultra.

Terceiro: pessoa física ou jurídica que representa os interesses ou manifesta-se em nome do Grupo Ultra, independentemente da existência da outorga de procuração ou formalização contratual, incluindo, mas não se limitando a assessores, consultores, contadores, intermediários, advogados e despachantes.