1. OBJETIVO

Este documento estabelece as diretrizes de Tecnologia e de Segurança da Informação aplicáveis a Ultrapar Participações S.A. ("Ultrapar") e suas controladas, as quais são tratadas individualmente como "Negócios" (em conjunto com Ultrapar, "Grupo Ultra").

Esta Diretriz deve ser interpretada em conjunto com o Código de Ética e demais políticas e normas do Grupo Ultra.

2. DIRETRIZES GERAIS

Todo Negócio deverá:

- Estabelecer e manter planos de continuidade de negócios e de resposta a incidentes;
- Conduzir, com periodicidade mínima de duas vezes ao ano, testes de intrusão, de engenharia social, de efetividade do plano de resposta a incidentes e de recuperação de ambientes;
- Promover regularmente campanhas de conscientização e treinamento de Segurança da Informação para todos os colaboradores e terceiros com acessos ao ambiente de tecnologia do Negócio;
- Relatar imediatamente para a Ultrapar incidentes críticos e/ou materiais de segurança cibernética;
- Implementar, manter e monitorar sistemas e processos de gestão de acessos e identidades em *softwares*, sistemas, ambientes, ferramentas, serviços em nuvem, serviços de armazenamento de dados, incluindo, mas não se limitando ao *onedrive* e *sharepoint*, que atendam aos seguintes requisitos mínimos:
  - ✓ Matriz de segregação de funções ("SOD");
  - ✓ Funcionalidades de concessão, revogação e transferência de acessos, contemplando os diferentes tipos de acessos e identidades, perfis específicos para cada função ou responsabilidade e fluxos e alçadas de aprovação adequados.
- Implementar e manter sistema automatizado para aprovação, concessão, revisão, transferência, monitoração e revogação de acessos e identidades, gerenciando todo o seu ciclo de vida e contemplando integração SSO;
- Implementar e manter sistema para gerenciamento e monitoramento de acessos privilegiados, contemplando registro, gravação e armazenamento de todo e qualquer acesso privilegiado, permitindo revisão ou auditoria a qualquer momento, e atendendo definições e critérios estabelecidos pela Ultrapar e requisitos estabelecidos nos controles gerais de Tecnologia ("ITGC") da *Sarbanes* Oxley ("*SOx*");
- Implementar configuração e regras de senhas contendo no mínimo 11 caracteres, combinando letras, números e caracteres especiais, alteração obrigatória a cada 90 dias e segundo fator de autenticação ou conforme regras de senhas estabelecidas pela aplicação. Exceções deverão ter justificativa formalizada com a Ultrapar;
- Implementar e manter processo contínuo de gestão de vulnerabilidades, monitoramento, atualizações e correções, contemplando:
  - ✓ atualizações de patches, correções e configurações técnicas em todos os ativos de tecnologia, seja *software* ou *hardware*;
  - ✓ 100% dos ativos no *CMDB* monitorados no *Tenable*;
  - ✓ atualizações ou substituições de versões de *software* ou *hardware* em *backlevel*, ou seja, que deixaram de ser suportadas pelos seus fabricantes;

    demais regras e prazos estabelecidos pela Gerência de Segurança da Informação Ultrapar, pela área de Riscos da Ultrapar e em conformidade com controles ITGC;

- Identificar riscos, implementar, monitorar e executar controles gerais de Tecnologia ("ITGC") que atendam plenamente os requisitos e normas da *Sarbanes Oxley ("SOx")* e das áreas de Auditoria Interna e de Controles Internos da Ultrapar.
- Somente adquirir ou contratar *software* ou novas soluções digitais que contemplem os seguintes requisitos mínimos:
  - ✓ Conformidade com SOx e/ou possuir certificações SOC1- e/ou SOC2 (*System and Organization Controls* 1 e 2) conforme a característica de uso.
  - ✓ Permitir integração com *software* de gerenciamento de identidades e acessos.
- Implementar, manter, documentar e publicar processos e regras de backup e recuperação de dados, contemplando minimamente tempo de retenção, meios de armazenamento, testes periódicos de recuperação, métodos de criptografia, e quando aplicável, observando a Lei Geral de Proteção de Dados ("LGPD"), controles ITGC e/ou regulamentações específicas.
- Implementar e manter um processo de gestão de ativos tecnológicos que contemple:
  - ✓ Inventário (*CMDB*) atualizado periodicamente de todos os ativos, incluindo os dispositivos móveis, tais como notebooks, *tablets*, *smartphones* e coletores.
  - ✓ *Software* de gerenciamento de dispositivos moveis MDM – *Mobile Device Management* para smartphones, tablets e coletores com capacidade para manutenção de configuração, atualizações automáticas, criptografia, localização e bloqueio.
  - ✓ *Software* e regras para criptografia de dispositivos móveis que permita gerenciamento seguro através de chaves de acesso.
- Implementar e manter processo de gestão de mudanças automatizado em ferramenta específica para ITSM – IT Service Management – Gestão de Serviços de TI, em conformidade com os controles ITGC;
- Garantir que toda contratação de fornecedores e terceiros esteja em conformidade com leis e regulamentações vigentes, tais como LGPD, SOx, em conformidade com nossas diretrizes e políticas de Tecnologia, Segurança da Informação e de Compras, incluindo assinatura previa de acordos de confidencialidade, quando aplicável;
- Implementar processos de gestão de fornecedores, parceiros, soluções e serviços de tecnologia, incluindo identificação e classificação de riscos associados ou relacionados;
- Implementar e manter as seguintes tecnologias e soluções de rede e segurança:
  - ✓ Solução de Proxy
  - ✓ ZTNA (*Zero Trust Network Access*)
  - ✓ *Firewall* camada 7
  - ✓ IPS norte/sul e leste/oeste
  - ✓ AntiDDoS para os links de dados
  - ✓ WAF – *Firewall* de Aplicações Web para aplicações publicadas
  - ✓ Segurança de DNS
  - ✓ *Baseline* de segurança com as melhores práticas e garantia de que as configurações estejam implementadas.
  - ✓ Soluções EDR- Detecção e Resposta de *Endpoint*, XDR - Detecção e Resposta Estendidas para monitoramento, análise de atividades suspeitas e correlação de dados, monitoramento contínuo, proteção *anti-malware*, garantindo cobertura total em computadores e servidores.

3. SOLUÇÃO PADRÃO

A Ultrapar estabelece soluções de *software* ou de serviços que são únicas e padronizadas para todas as empresas do Grupo, conforme abaixo relacionadas:

- Microsoft Office 365 (e-mail, colaboração, produtividade)
- Ferramenta de *Data Loss Prevention*
- CyberArk (gerenciamento de acessos privilegiados)
- CAR e Imperva (controle de acessos em bancos de dados)
- IDM *Symantec Identity Suite* (Gestão de identidades)
- CrowdStrike (*anti-malware* XDR)
- Zscaler (ZTNA e filtro de conteúdo)

- Tenable e ScoreCard (gerenciamento de vulnerabilidades)
- Microsoft Sentinel (solução de SIEM)
- Operação de SOC 24x7 (Security Operation Center)

As soluções e os serviços acima poderão ser revisados periodicamente, sempre em conjunto com os Negócios, visando evolução, eficiência e/ou maior segurança. Uma vez aprovada a substituição de uma solução ou um serviço, de forma colegiada entre os Negócios e a Ultrapar, sua implementação deve ser realizada em todas as empresas, conforme prazo estabelecido na decisão.

A substituição de uma solução ou de um serviço padrão conforme estabelecido nesta diretriz também poderá ocorrer individualmente em apenas uma empresa do Grupo desde que previamente aprovada pela Diretoria responsável por Tecnologia e pela Segurança da Informação da Ultrapar.

4. CANAL ABERTO

Todos os Negócios do Grupo Ultra devem aderir a estas diretrizes, inclusive relatando eventuais desvios por meio do Canal Aberto https://canalabertoultra.com.br.

5. GLOSSÁRIO

SOD (*Segregation of Duties ou Segregação de Funções*): Princípio de controle interno que impede que um único indivíduo tenha controlo sobre todas as fases críticas de um processo.

SSO (*Single Sign-On ou início de sessão único*): método de autenticação que permite que um usuário acesse múltiplos aplicativos e serviços com um único conjunto de credenciais.

CMDB (*Configuration Management Database ou Banco de Dados do Gerenciamento de Configuração*): Um repositório centralizado que armazena e gerencia informações sobre os componentes de uma infraestrutura de TI, como hardware, software, redes e outros ativos

Backlevel: Termo utilizado para se referir a um software ou um hardware atingiu a fase final do seu ciclo de vida e não tem mais suporte do fabricante.

EDR (*Endpoint Detection and Response ou Detecção e Resposta de Endpoints*): Solução de segurança cibernética que monitora continuamente dispositivos físicos (*endpoints*) como computadores e celulares, detecta comportamentos maliciosos e automáticos para investigar e responder a ameaças em tempo real.

SIEM (*Security Information and Event Management ou Gestão de Informações e Eventos de Segurança*): Solução de cibersegurança que recolhe, analisa e correlaciona dados de diversas fontes (aplicações, dispositivos, servidores etc.) para detectar e responder a ameaças de segurança em tempo real.