



POLÍTICA DE **SEGURANÇA DA INFORMAÇÃO**

DIRETRIZES INSTITUCIONAIS
ALINHADAS À ISO/IEC 27001:2022,
À EMENDA 1:2024, À PROTEÇÃO
DE DADOS E À CONTINUIDADE.

ÍNDICE

Política de Segurança da Informação	8
1. Mensagem institucional	8
2. Objetivo	9
3. Alcance e público	9
4. Contexto da Vert Analytics	10
5. Princípios de segurança	10



6. Governança e responsabilidades	11
7. Como usar e aplicar esta Política	12
8. Ciclo de gestão e melhoria contínua	13
9. Regras essenciais para qualquer usuário	13
10. Diretrizes executivas para os controles da ISO/IEC 27001:2022	14

ÍNDICE

11. Controles organizacionais	14
12. Controles de pessoas	28
13. Controles físicos	30
14. Controles tecnológicos	35
15. Integração com proteção de dados, IA e decisões automatizadas	46
16. Indicadores, monitoramento e análise crítica	47



17. Comunicação de eventos, incidentes e solicitações	48
18. Exceções, não conformidades e consequências	48
19. Documentação relacionada	49
20. Referências externas	50
21. Glossário essencial	51

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Código	POL-001	Classificação	Pública
Versão	1.1	Data de emissão	13/07/2026
Elaboração	Comitê Multidisciplinar do SGSI/SGPI	Aprovação	Alta Direção
Abrangência	Vert Analytics, pessoas, processos, tecnologias e terceiros	Revisão	Anual ou por mudança relevante
Referencial	ISO/IEC 27001:2022 e Emenda 1:2024	Integração	ISO/IEC 27701, LGPD e continuidade
Repositório oficial	ECM institucional / Outline Wiki	Impressão	Cópia não controlada

Natureza desta edição

Este documento apresenta compromissos, princípios e regras de aplicação compreensíveis para colaboradores, clientes, fornecedores, parceiros, candidatos, titulares de dados e demais usuários. Detalhes de arquitetura, configurações, riscos específicos, vulnerabilidades, planos de resposta e evidências operacionais permanecem em documentos internos de acesso controlado.

1. MENSAGEM INSTITUCIONAL

Na Vert Analytics, segurança da informação é parte do valor entregue. Nossas soluções de inteligência artificial, análise de dados, automação, prevenção a fraudes, onboarding digital, reconhecimento facial, verificação documental e autenticação biométrica dependem de confiança, qualidade, disponibilidade e uso responsável da informação.

Esta Política expressa o compromisso da Alta Direção com uma gestão de segurança baseada em riscos, melhoria contínua, proteção de dados pessoais, continuidade dos serviços e respeito às obrigações

legais, regulatórias, contratuais e éticas. A segurança não é responsabilidade exclusiva da área de tecnologia: ela resulta das decisões diárias de todas as pessoas que participam de nossos processos.

Compromisso central

Proteger informações e serviços de forma proporcional aos riscos, promovendo confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, privacidade e resiliência, sem impedir a inovação responsável.

2. OBJETIVO

- ▶ Estabelecer as diretrizes gerais para proteger as informações e os ativos associados da Vert Analytics, de clientes, parceiros, colaboradores, fornecedores e titulares de dados.
- ▶ Traduzir os princípios e os controles da ISO/IEC 27001:2022 em regras executivas, aplicáveis e compreensíveis, preservando o caráter baseado em riscos da norma.
- ▶ Orientar comportamento, decisões, projetos, operações, desenvolvimento, contratação, uso de nuvem, inteligência artificial, tratamento de dados e resposta a incidentes.
- ▶ Disponibilizar ao público uma declaração transparente de compromisso, sem divulgar detalhes que possam reduzir a segurança dos ambientes ou das partes interessadas.

3. ALCANCE E PÚBLICO

A Política aplica-se à Vert Analytics Ltda., às suas unidades, atividades presenciais e remotas, processos corporativos, projetos, produtos, serviços, informações, dados, modelos, códigos, plataformas, infraestrutura, ambientes em nuvem, instalações, equipamentos e integrações.

É obrigatória para administradores, empregados, estagiários, aprendizes, temporários, consultores, prestadores, fornecedores, parceiros e qualquer pessoa que utilize ativos ou trate informações sob responsabilidade da Vert Analytics. Requisitos específicos de cliente, contrato, setor ou legislação prevalecem quando forem mais restritivos.

4. CONTEXTO DA VERT ANALYTICS

A Vert Analytics atua na transformação digital por meio de soluções personalizadas de inteligência artificial e análise de dados. Seu portfólio envolve processamento de documentos, dados transacionais, imagens, vídeos, áudios e outras fontes, com aplicações em automação, decisão, prevenção a fraudes e serviços digitais.

Essa natureza exige proteção consistente de dados, algoritmos, modelos, integrações, códigos, resultados e informações confiadas por organizações públicas e privadas.



Missão

Desenvolver soluções para alcançar a melhor versão do negócio de nossos clientes e resolver problemas em diferentes níveis de maturidade digital.



Visão

Ser referência em soluções analíticas de alto valor agregado nos mercados de atuação.



Valores

Comprometimento, responsabilidade, ética, respeito às pessoas e busca incessante pela excelência.

5. PRINCÍPIOS DE SEGURANÇA

- ▶ **Confidencialidade:** Informações são acessadas somente por pessoas, sistemas e serviços autorizados.
- ▶ **Integridade:** Dados, códigos, modelos, documentos e registros permanecem completos, corretos e protegidos contra alteração indevida.
- ▶ **Disponibilidade:** Informações e serviços estão acessíveis quando necessários, de acordo com requisitos de negócio e continuidade.
- ▶ **Autenticidade e rastreabilidade:** É possível verificar origem, identidade, ações e sequência de eventos relevantes.
- ▶ **Privacidade:** Dados pessoais são tratados com finalidade, necessidade, transparência, segurança e respeito aos direitos dos titulares.
- ▶ **Segurança e privacidade desde a concepção:** Controles são incorporados ao planejamento e ao desenvolvimento, e não adicionados apenas ao final.

- ▶ **Menor privilégio e necessidade de saber:** Acesso é limitado ao mínimo necessário para a atividade autorizada.
- ▶ **Responsabilização:** Decisões, aprovações, mudanças e exceções devem possuir responsável e evidência.
- ▶ **Resiliência:** Pessoas, processos e tecnologia são preparados para prevenir, responder, recuperar e aprender.
- ▶ **Melhoria contínua:** Riscos, controles, indicadores, incidentes, auditorias e mudanças alimentam o ciclo de evolução do SGSI.

6. GOVERNANÇA E RESPONSABILIDADES

Responsável	Responsabilidade executiva
Alta Direção	Aprovar a Política, fornecer recursos, estabelecer prioridades, aceitar riscos quando competente e demonstrar liderança.
Comitê Multidisciplinar do SGSI/SGPI	Coordenar o sistema de gestão, acompanhar riscos, controles, indicadores, incidentes, auditorias e planos de ação.
Proprietários de processos, informações e sistemas	Definir requisitos, classificação, acesso, retenção, continuidade e tratamento de riscos sob sua responsabilidade.
Tecnologia e Segurança	Implementar, operar e monitorar controles técnicos; apoiar arquitetura, vulnerabilidades, incidentes, continuidade e evidências.
Privacidade e Jurídico	Orientar proteção de dados, requisitos legais, contratos, titulares, autoridades e comunicações regulatórias.
Gestão de Pessoas	Integrar requisitos ao ciclo de vida das pessoas, capacitação, termos, movimentações e desligamentos.
Facilities e Administração	Proteger instalações, acessos físicos, equipamentos, serviços de apoio e ameaças ambientais.
Gestores de contratos e fornecedores	Avaliar riscos, inserir requisitos, acompanhar serviços e assegurar encerramento seguro.
Todos os usuários	Cumprir regras, proteger credenciais e ativos, limitar o uso à finalidade autorizada e reportar eventos rapidamente.

7. COMO USAR E APLICAR ESTA POLÍTICA

Leitura orientada à ação

Cada diretriz deve ser interpretada em conjunto com a classificação da informação, o risco, a função da pessoa, o contrato, o processo e os procedimentos internos vigentes. A Política indica o comportamento esperado; os documentos internos detalham responsáveis, passos, ferramentas, prazos e evidências.

- ▶ **Antes de agir:** verifique se a finalidade é legítima, se você possui autorização e se o canal ou ferramenta foi aprovado.
- ▶ **Ao tratar informação:** use somente o necessário, mantenha a classificação e evite cópias, exposições ou retenções desnecessárias.
- ▶ **Ao usar IA:** não insira informações restritas em ferramentas não aprovadas; avalie fonte, qualidade, vieses, segurança e necessidade de revisão humana.
- ▶ **Ao compartilhar:** confirme destinatário, conteúdo, canal, contrato e eventual necessidade de criptografia ou autorização.
- ▶ **Ao perceber um problema:** interrompa a ação de risco quando seguro, preserve evidências e reporte imediatamente.
- ▶ **Ao encerrar uma atividade:** devolva ativos, revogue acessos, organize registros e elimine cópias conforme temporalidade.

8. CICLO DE GESTÃO E MELHORIA CONTÍNUA

Planejar

Compreender contexto, partes interessadas, riscos, obrigações, objetivos, controles e recursos.

Executar

Implementar políticas, procedimentos, arquitetura, treinamentos, contratos e controles operacionais.

Verificar

Monitorar indicadores, logs, conformidade, incidentes, fornecedores, auditorias e eficácia.

Agir

Corrigir causas, atualizar riscos e documentos, melhorar controles e comunicar mudanças.

9. REGRAS ESSENCIAIS PARA QUALQUER USUÁRIO

01. Use somente contas, dispositivos, aplicações, repositórios, redes e serviços aprovados.
02. Proteja senhas, tokens, certificados e códigos de autenticação; nunca os compartilhe.
03. Não envie informação corporativa para e-mail pessoal, mensageiro particular ou nuvem não autorizada.
04. Não utilize dados restritos, pessoais, biométricos, códigos ou documentos de clientes em ferramentas públicas de IA sem aprovação.
05. Confirme destinatários, anexos, permissões e links antes de compartilhar.
06. Mantenha sistemas atualizados e não desative controles de segurança.
07. Bloqueie a tela, preserve mesa limpa e proteja conversas em ambientes compartilhados.
08. Não instale software, extensões, bibliotecas ou dispositivos sem autorização.
09. Reporte phishing, perda, envio incorreto, acesso suspeito, falha ou vazamento imediatamente.
10. Não investigue incidentes por conta própria, não apague evidências e não divulgue ocorrências externamente.

10. DIRETRIZES EXECUTIVAS PARA OS CONTROLES DA ISO/IEC 27001:2022

A aplicação definitiva de cada controle é determinada pela avaliação de riscos e registrada na Declaração de Aplicabilidade. Os textos abaixo são interpretações executivas próprias e não reproduzem o conteúdo normativo da ISO.

37 Organizacionais	8 Pessoas	14 Físicos	34 Tecnológicos
Governança, ativos, acesso, terceiros, incidentes, continuidade e conformidade	Ciclo de vida, termos, conscientização, trabalho remoto e reporte.	Instalações, acesso, equipamentos, ambiente e descarte.	Endpoints, identidades, redes, nuvem, logs, desenvolvimento e criptografia.

11. CONTROLES ORGANIZACIONAIS

Governança, organização, ativos, acessos, fornecedores, incidentes, continuidade e conformidade.

11.1. POLÍTICAS PARA SEGURANÇA DA INFORMAÇÃO

Diretriz executiva: A segurança da informação deve ser orientada por políticas aprovadas pela Alta Direção, coerentes com os riscos, objetivos de negócio, obrigações legais e expectativas das partes interessadas.

Aplicação na Vert Analytics: A POL-001 funciona como documento público de compromisso. Regras complementares, padrões técnicos, procedimentos e formulários são controlados no ECM institucional e revisados quando houver mudanças relevantes em ameaças, tecnologias, contratos, legislação, estrutura organizacional ou serviços.

Nota de uso: Conheça as políticas aplicáveis ao seu trabalho antes de utilizar dados, sistemas ou recursos da empresa. Em caso de dúvida, consulte o gestor responsável ou os canais institucionais.

Registros e evidências relacionadas: POL-001; Declaração de Aplicabilidade (SoA); Matriz GAP; base de documentos do SGSI/SGPI no ECM; registros de aprovação e revisão.

11.2. PAPÉIS E RESPONSABILIDADES DE SEGURANÇA DA INFORMAÇÃO

Diretriz executiva: As responsabilidades de segurança devem ser atribuídas, comunicadas e mantidas de forma inequívoca, evitando lacunas de decisão, execução, supervisão e prestação de contas.

Aplicação na Vert Analytics: A governança envolve Alta Direção, Comitê Multidisciplinar do SGSI/SGPI, responsáveis por processos, Tecnologia, Segurança, Privacidade, Jurídico, Pessoas, Facilities, Comunicação, fornecedores e usuários. A matriz RACI e os documentos de nomeação registram autoridade e substituição.

Nota de uso: Cada pessoa é responsável pela proteção das informações que acessa. Responsabilidade não é transferida pelo uso de terceiros, automações ou ferramentas de inteligência artificial.

Registros e evidências relacionadas: Ata de nomeação do Comitê; matriz RACI; organogramas; descrições de função; termos de responsabilidade; SoA.

11.3. SEGREGAÇÃO DE FUNÇÕES

Diretriz executiva: Atividades incompatíveis devem ser separadas para reduzir riscos de erro, fraude, abuso de privilégio, alteração indevida ou ausência de revisão independente.

Aplicação na Vert Analytics: A Vert Analytics adota separação proporcional entre solicitação, autorização, execução, teste, homologação, implantação, pagamento, administração e auditoria. Quando a estrutura não permitir separação completa, são aplicados controles compensatórios, rastreabilidade e revisão por segunda pessoa.

Nota de uso: Não aprove sua própria solicitação quando houver conflito de interesse. Não compartilhe credenciais para contornar etapas de autorização.

Registros e evidências relacionadas: Matriz RACI; fluxos de aprovação; perfis de acesso; registros de mudança; trilhas de auditoria; matriz de riscos MR-001.

11.4. RESPONSABILIDADES DA GESTÃO

Diretriz executiva: Gestores devem assegurar que suas equipes conheçam, compreendam e cumpram as regras de segurança aplicáveis às atividades sob sua responsabilidade.

Aplicação na Vert Analytics: As lideranças incorporam requisitos de segurança no planejamento, na distribuição de tarefas, na gestão de desempenho, na contratação, no acompanhamento de projetos e na resposta a desvios. Demandas urgentes não afastam a necessidade de controles mínimos.

Nota de uso: Gestores devem orientar a equipe, corrigir práticas inseguras e escalar riscos que excedam sua autoridade ou capacidade de tratamento.

Registros e evidências relacionadas: Registros de comunicação; planos de ação; atas de reunião; avaliações; treinamentos; registros de não conformidade.

11.5. CONTATO COM AUTORIDADES

Diretriz executiva: A organização deve manter canais e critérios para interação tempestiva, autorizada e consistente com autoridades competentes.

Aplicação na Vert Analytics: Contatos com ANPD, órgãos reguladores, autoridades policiais, Poder Judiciário, organismos de certificação e órgãos contratantes são coordenados por funções autorizadas, preservando evidências, sigilo, prazos e coerência das informações.

Nota de uso: Nenhum colaborador deve responder oficialmente a uma autoridade em nome da Vert Analytics sem autorização, salvo dever legal imediato.

Registros e evidências relacionadas: Cadastro de autoridades; fluxo jurídico e regulatório; plano de resposta a incidentes; registros de comunicações oficiais.

11.6. CONTATO COM GRUPOS DE INTERESSE ESPECIAL

Diretriz executiva: A Vert Analytics deve manter intercâmbio responsável com comunidades técnicas, entidades setoriais, fóruns profissionais e fontes confiáveis de conhecimento.

Aplicação na Vert Analytics: A participação em grupos de segurança, privacidade, tecnologia, IA, análise de dados, prevenção a fraudes e continuidade apoia a atualização de práticas, a identificação de ameaças e a melhoria dos controles, sem divulgação de informações restritas.

Nota de uso: Ao participar de eventos ou comunidades, compartilhe somente informações autorizadas e evite detalhar arquiteturas, clientes, incidentes ou vulnerabilidades.

Registros e evidências relacionadas: Plano de capacitação; registros de participação; inteligência de ameaças; política de comunicação e classificação.

11.7. INTELIGÊNCIA DE AMEAÇAS

Diretriz executiva: Informações sobre ameaças devem ser coletadas, qualificadas, analisadas e convertidas em decisões preventivas e corretivas.



Aplicação na Vert Analytics: A empresa acompanha alertas de fabricantes, provedores, comunidades especializadas, fontes governamentais e sinais internos. A análise considera tecnologias de nuvem, APIs, biometria, IA generativa, documentos digitais, bases de dados, integrações e cadeias de fornecedores.

Nota de uso: Encaminhe alertas suspeitos ou notícias relevantes à equipe responsável; não execute testes ou contramedidas sem autorização.

Registros e evidências relacionadas: Registros de inteligência de ameaças; boletins; MR-001; gestão de vulnerabilidades; planos de ação.

11.8. SEGURANÇA DA INFORMAÇÃO NA GESTÃO DE PROJETOS

Diretriz executiva: Requisitos de segurança e privacidade devem integrar todo projeto, desde a concepção até o encerramento e a transição para operação.

Aplicação na Vert Analytics: Projetos de analytics, automação, antifraude, onboarding digital, reconhecimento facial, verificação documental, IA generativa e integração de dados devem considerar risco, classificação, acesso, logs, continuidade, fornecedores, testes, descarte e proteção de dados desde o desenho.

Nota de uso: Antes de iniciar ou alterar um projeto, registre requisitos de segurança e envolva as áreas responsáveis na fase adequada, não apenas antes da entrega.

Registros e evidências relacionadas: Metodologia de projetos; checklist de segurança e privacidade; AIPD/DPIA; ROPA; plano de testes; termo de aceite.

11.9. INVENTÁRIO DE INFORMAÇÕES E ATIVOS ASSOCIADOS

Diretriz executiva: Informações, sistemas, dados, modelos, equipamentos, serviços, credenciais e demais ativos relevantes devem possuir inventário, proprietário e tratamento compatível com seu valor e risco.

Aplicação na Vert Analytics: O inventário abrange bases de dados, documentos, códigos-fonte, modelos de IA, prompts estruturados, APIs, pipelines, ambientes, endpoints, mídias, contratos, serviços em nuvem e ativos de terceiros sob responsabilidade da Vert Analytics.

Nota de uso: Não crie repositórios paralelos ou mantenha dados corporativos fora dos ambientes aprovados. Informe ativos novos, transferidos ou desativados.

Registros e evidências relacionadas: Inventário de ativos; Mapa de Dados LGPD; CMDB ou registros equivalentes; ROPA; termos de custódia; SoA.

11.10. USO ACEITÁVEL DE INFORMAÇÕES E ATIVOS

Diretriz executiva: Os recursos da Vert Analytics devem ser usados de forma profissional, legal, ética, segura e compatível com a finalidade autorizada.

Aplicação na Vert Analytics: São vedados uso abusivo, instalação não autorizada, compartilhamento indevido, armazenamento pessoal de dados corporativos, tentativa de burlar controles, processamento de informações em serviços não aprovados e uso de IA pública com conteúdo restrito sem autorização.

Nota de uso: Use somente contas, equipamentos, redes, aplicações e serviços aprovados. Trate acessos corporativos como pessoais e intransferíveis.

Registros e evidências relacionadas: Termo de uso aceitável; código de conduta; registros de treinamento; inventário de ativos; registros disciplinares quando aplicável.

11.11. DEVOLUÇÃO DE ATIVOS

Diretriz executiva: Ativos físicos, digitais, credenciais, documentos e informações devem ser devolvidos ou ter seu acesso revogado quando cessar a necessidade legítima.

Aplicação na Vert Analytics: Mudanças de função, término de contrato, férias prolongadas, afastamentos e encerramento de projetos acionam fluxos de devolução, transferência de custódia, revogação de acesso e confirmação de retenção ou eliminação.

Nota de uso: Não retenha cópias de arquivos, códigos, modelos, documentos, contatos ou dados da Vert Analytics após o encerramento da relação ou da necessidade de uso.

Registros e evidências relacionadas: Checklist de desligamento e movimentação; termos de devolução; inventário; registros de revogação; cadeia de custódia.

11.12. CLASSIFICAÇÃO DA INFORMAÇÃO

Diretriz executiva: A informação deve ser classificada conforme sensibilidade, impacto, obrigação legal, valor de negócio e necessidade de compartilhamento.

Aplicação na Vert Analytics: A classificação orienta acesso, identificação, transmissão, armazenamento, retenção, cópia, publicação e descarte. Dados pessoais, biométricos, credenciais, códigos,





modelos, bases de clientes e informações contratuais recebem proteção proporcional.

Nota de uso: Antes de compartilhar, identifique a classificação e confirme se o destinatário, o canal e a finalidade são adequados.

Registros e evidências relacionadas: Matriz Integrada de Comunicação, Classificação e Temporalidade; inventário; ROPA; contratos; registros de revisão.

11.13. ROTULAGEM DA INFORMAÇÃO

Diretriz executiva: Informações devem receber identificação visual ou lógica suficiente para que usuários e sistemas reconheçam o tratamento esperado.

Aplicação na Vert Analytics: Rótulos podem constar em documentos, metadados, cabeçalhos, rodapés, repositórios, pastas, e-mails, sistemas e mecanismos de prevenção contra perda de dados. A ausência de rótulo não transforma informação corporativa em pública.

Nota de uso: Mantenha os rótulos existentes e aplique a classificação indicada nos modelos institucionais.

Registros e evidências relacionadas: Padrão de classificação e rotulagem; modelos documentais; configurações de ECM e e-mail; evidências de DLP.

11.14. TRANSFERÊNCIA DE INFORMAÇÃO

Diretriz executiva: Toda transferência deve utilizar canais autorizados, destinatários verificados, proteção proporcional e registro quando necessário.

Aplicação na Vert Analytics: A política se aplica a e-mail, portais, APIs, integrações, nuvem, mídia removível, mensageria, reuniões, compartilhamentos, exportações e transferências internacionais. Dados sensíveis podem exigir criptografia, contrato, autenticação reforçada e aprovação.

Nota de uso: Confirme destinatários e anexos antes do envio. Nunca utilize mensageiros, e-mails pessoais ou links públicos para contornar controles.

Registros e evidências relacionadas: Procedimento de transferência; contratos e cláusulas; registros de integração; ROPA; avaliação de transferência internacional.

11.15. CONTROLE DE ACESSO

Diretriz executiva: O acesso deve ser concedido segundo necessidade de negócio, menor privilégio, segregação, classificação e risco.

Aplicação na Vert Analytics: Regras de acesso abrangem pessoas, sistemas, APIs, bancos de dados, modelos, ambientes, redes, repositórios e instalações. Decisões são autorizadas pelo proprietário do recurso e revisadas periodicamente.

Nota de uso: Solicite somente o acesso necessário e informe quando ele deixar de ser utilizado. Não tente acessar conteúdos fora de sua atribuição.

Registros e evidências relacionadas: Política de controle de acesso; matriz de perfis; solicitações e aprovações; recertificações; trilhas de auditoria.

11.16. GESTÃO DE IDENTIDADES

Diretriz executiva: Identidades digitais devem ser únicas, verificáveis, administradas durante todo o ciclo de vida e vinculadas a uma pessoa, função ou serviço responsável.

Aplicação na Vert Analytics: A empresa controla criação, alteração, suspensão, revogação e revisão de identidades humanas, técnicas, privilegiadas e de integração. Contas genéricas são evitadas ou justificadas, monitoradas e protegidas.

Nota de uso: Não empreste conta, token, certificado ou sessão. Comunique imediatamente suspeita de uso indevido.

Registros e evidências relacionadas: Diretório corporativo; registros de identidade; inventário de contas técnicas; fluxo de admissão, movimentação e desligamento.

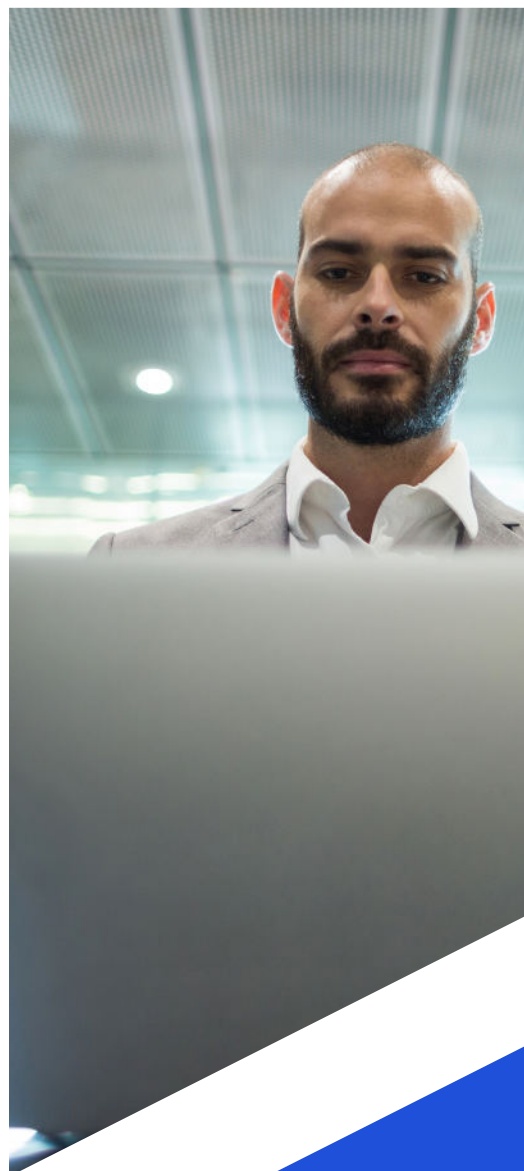
11.17. INFORMAÇÕES DE AUTENTICAÇÃO

Diretriz executiva: Senhas, chaves, tokens, certificados e demais fatores de autenticação devem ser protegidos contra criação fraca, exposição, reutilização e compartilhamento.

Aplicação na Vert Analytics: A Vert Analytics aplica requisitos de complexidade, armazenamento seguro, troca quando necessária, autenticação multifator em cenários definidos e cofres ou mecanismos aprovados para segredos técnicos.

Nota de uso: Nunca registre segredos em texto aberto, código-fonte, planilhas, mensagens ou chamados. Em caso de exposição, solicite revogação imediata.

Registros e evidências relacionadas: Padrão de autenticação; cofre de segredos; registros de MFA; gestão de certificados; tratamento de incidentes.



11.18. DIREITOS DE ACESSO

Diretriz executiva: Direitos de acesso devem ser solicitados, aprovados, implementados, revisados e removidos de forma rastreável.

Aplicação na Vert Analytics: Revisões periódicas e eventos de mudança verificam privilégios excessivos, contas inativas, acessos incompatíveis e permissões herdadas. A revogação tem prioridade quando houver risco ou término de vínculo.

Nota de uso: Aprovações devem considerar função e necessidade real; conveniência não é justificativa para privilégio amplo.

Registros e evidências relacionadas: Solicitações de acesso; relatórios de recertificação; logs; registros de revogação; matriz RACI.

11.19. SEGURANÇA EM RELACIONAMENTOS COM FORNECEDORES

Diretriz executiva: Riscos de segurança e privacidade relacionados a fornecedores devem ser avaliados antes, durante e ao final da relação.

Aplicação na Vert Analytics: A avaliação considera criticidade, acesso a dados, dependência tecnológica, subcontratação, nuvem, localização, continuidade, incidentes, evidências de conformidade e capacidade de retorno ou eliminação de informações.

Nota de uso: Não contrate ou utilize fornecedor para processar dados corporativos sem o fluxo de avaliação e aprovação aplicável.

Registros e evidências relacionadas: Cadastro e avaliação de fornecedores; due diligence; MR-001; contratos; ROPA; plano de continuidade.

11.20. SEGURANÇA NOS ACORDOS COM FORNECEDORES

Diretriz executiva: Contratos devem definir responsabilidades, requisitos mínimos, confidencialidade, acesso, notificação de incidentes, auditoria, continuidade, proteção de dados e encerramento.

Aplicação na Vert Analytics: As cláusulas são proporcionais ao serviço e podem contemplar suboperadores, níveis de serviço, localização de dados, criptografia, evidências, testes, devolução, eliminação e cooperação regulatória.

Nota de uso: Gestores de contrato devem verificar não apenas preço e entrega, mas também obrigações de segurança e privacidade.

Registros e evidências relacionadas: Modelos contratuais; anexos de segurança; acordo de tratamento de dados; SLA; registros de aceite.

11.21. SEGURANÇA NA CADEIA DE SUPRIMENTOS DE TIC

Diretriz executiva: A cadeia de tecnologia deve ser gerida considerando dependências, componentes, atualizações, origem, integridade e riscos de terceiros sucessivos.

Aplicação na Vert Analytics: Soluções, bibliotecas, APIs, equipamentos, provedores e serviços são avaliados quanto a vulnerabilidades, manutenção, autenticidade, componentes de software e capacidade de resposta. Dependências críticas devem possuir alternativas ou planos de contingência.

Nota de uso: Não incorpore componentes, bibliotecas ou serviços externos sem verificar licença, origem, manutenção e segurança.

Registros e evidências relacionadas: Inventário de componentes; SBOM quando aplicável; avaliação de fornecedores; gestão de vulnerabilidades; contratos.

11.22. MONITORAMENTO, REVISÃO E MUDANÇA DE SERVIÇOS DE FORNECEDORES

Diretriz executiva: Serviços terceirizados devem ser acompanhados para verificar desempenho, conformidade, mudanças e riscos emergentes.

Aplicação na Vert Analytics: A Vert Analytics monitora níveis de serviço, incidentes, acessos, evidências, alterações relevantes, subcontratações e continuidade. Mudanças de escopo ou tecnologia exigem reavaliação proporcional.

Nota de uso: Registre problemas e mudanças do fornecedor; não aceite alterações críticas apenas por comunicação informal.

Registros e evidências relacionadas: SLA; atas de acompanhamento; relatórios de serviço; avaliações periódicas; registros de mudança; planos de ação.

11.23. SEGURANÇA PARA USO DE SERVIÇOS EM NUVEM

Diretriz executiva: Serviços em nuvem devem ser selecionados, configurados, utilizados, monitorados e encerrados com governança compartilhada claramente definida.

Aplicação na Vert Analytics: A avaliação considera classificação de dados, regiões, identidades, criptografia, logs, backup, continuidade, portabilidade, exclusão, subcontratados, responsabilidades e requisitos contratuais. Contas e ambientes de nuvem devem seguir padrões aprovados.

Nota de uso: Não crie ambientes, contas ou compartilhamentos em nuvem fora da governança institucional.

Registros e evidências relacionadas: Política de nuvem; arquitetura aprovada; matriz de responsabilidade compartilhada; inventário; contratos; ROPA.

11.24. PLANEJAMENTO E PREPARAÇÃO PARA INCIDENTES

Diretriz executiva: A organização deve manter capacidade planejada para detectar, registrar, classificar, comunicar e responder a incidentes.

Aplicação na Vert Analytics: Planos definem papéis, níveis de severidade, canais, preservação de evidências, comunicação, acionamento de continuidade, privacidade e relacionamento com terceiros. Exercícios e simulações validam a prontidão.

Nota de uso: Saiba como reportar um evento e preserve o cenário. Não investigue isoladamente nem divulgue o incidente.

Registros e evidências relacionadas: Plano de Resposta a Incidentes; matriz de severidade; listas de contato; exercícios; registros de capacitação.

11.25. AVALIAÇÃO E DECISÃO SOBRE EVENTOS DE SEGURANÇA

Diretriz executiva: Eventos devem ser triados para distinguir alertas, falhas, suspeitas e incidentes confirmados, com prioridade baseada em impacto e urgência.

Aplicação na Vert Analytics: A avaliação considera ativos afetados, dados pessoais, alcance, persistência, evidências, impacto em clientes, serviços e obrigações de comunicação. Decisões são registradas e reavaliadas quando surgirem fatos novos.

Nota de uso: Reporte fatos observados, sem minimizar ou exagerar. A classificação formal cabe à função autorizada.

Registros e evidências relacionadas: Registros de eventos; tickets; critérios de severidade; análises técnicas; atas de decisão.

11.26. RESPOSTA A INCIDENTES DE SEGURANÇA

Diretriz executiva: Incidentes devem ser contidos, erradicados, recuperados e comunicados de maneira coordenada, segura e rastreável.

Aplicação na Vert Analytics: A resposta prioriza pessoas, serviços essenciais, integridade das evidências, redução de danos,

restauração segura e comunicação apropriada. Incidentes com dados pessoais são avaliados conforme LGPD e regulamentação da ANPD.

Nota de uso: Siga as instruções da equipe de resposta e evite apagar arquivos, reiniciar equipamentos ou contatar partes externas sem orientação.

Registros e evidências relacionadas: Plano de Resposta; registros de incidente; comunicações; cadeia de custódia; planos de recuperação.

11.27. APRENDIZADO COM INCIDENTES

Diretriz executiva: Lições de incidentes, quase incidentes e falhas devem resultar em melhoria de controles, processos e comportamento.

Aplicação na Vert Analytics: Após a estabilização, são analisadas causas, fatores contribuintes, eficácia da resposta, impactos, controles ausentes e ações preventivas. O aprendizado pode atualizar riscos, políticas, treinamentos, arquitetura e contratos.

Nota de uso: Participe de revisões com transparência e foco em melhoria, evitando ocultação ou culpabilização indevida.

Registros e evidências relacionadas: Relatório pós-incidente; análise de causa; MR-001; plano de ação; registros de eficácia.

11.28. COLETA DE EVIDÊNCIAS

Diretriz executiva: Evidências devem ser identificadas, coletadas, preservadas e apresentadas de forma íntegra, legal e rastreável.

Aplicação na Vert Analytics: A coleta observa cadeia de custódia, sincronização de tempo, competência técnica, minimização de acesso e requisitos jurídicos. Logs, imagens, equipamentos, arquivos e registros não devem ser alterados sem método autorizado.

Nota de uso: Ao perceber um incidente, preserve o contexto e aguarde orientação. Não encaminhe evidências por canais pessoais.

Registros e evidências relacionadas: Procedimento de evidências; cadeia de custódia; logs; registros forenses; pareceres jurídicos.

11.29. SEGURANÇA DA INFORMAÇÃO DURANTE INTERRUPÇÕES

Diretriz executiva: A proteção da informação deve permanecer ativa durante crises, contingências, degradações e operações alternativas.

Aplicação na Vert Analytics: Planos de continuidade definem controles mínimos, acessos emergenciais, comunicação, trabalho



remoto, proteção de cópias, priorização de serviços e retorno controlado à normalidade.

Nota de uso: Em contingência, utilize somente procedimentos e canais autorizados; urgência não justifica exposição desnecessária.

Registros e evidências relacionadas: PCN; planos de contingência; BIA; exercícios; registros de crise; MR-001.

11.30. PRONTIDÃO DE TIC PARA CONTINUIDADE DE NEGÓCIOS

Diretriz executiva: Recursos de TIC devem suportar os objetivos de recuperação definidos para processos críticos.

Aplicação na Vert Analytics: Arquiteturas, backups, redundâncias, capacidade, dependências e procedimentos de recuperação são alinhados à análise de impacto, com testes periódicos e tratamento de resultados.

Nota de uso: Conheça as alternativas aprovadas para seu processo e não mantenha dependências críticas não registradas.

Registros e evidências relacionadas: BIA; PCN; PRD; planos de backup; testes de recuperação; relatórios de disponibilidade.

11.31. REQUISITOS LEGAIS, REGULATÓRIOS E CONTRATUAIS

Diretriz executiva: Obrigações aplicáveis devem ser identificadas, atualizadas, traduzidas em controles e acompanhadas.

Aplicação na Vert Analytics: A base de requisitos contempla legislação de proteção de dados, internet, propriedade intelectual, contratos, obrigações setoriais, regras de clientes e requisitos de certificação. Mudanças são avaliadas pelo Comitê e responsáveis.

Nota de uso: Cumpra requisitos do contrato e do contexto do cliente; em caso de conflito ou dúvida, escale antes de agir.

Registros e evidências relacionadas: Base de legislações, normas e padrões; contratos; matriz de requisitos; pareceres; avaliações de conformidade.

11.32. DIREITOS DE PROPRIEDADE INTELECTUAL

Diretriz executiva: Direitos autorais, licenças, marcas, segredos de negócio, software, bases, modelos e demais ativos intelectuais devem ser respeitados e protegidos.

Aplicação na Vert Analytics: A empresa controla uso de código, bibliotecas, modelos de IA, conteúdos, dados, imagens e materiais de terceiros, bem como a proteção de criações próprias. Licenças e restrições são avaliadas antes da incorporação.

Nota de uso: Não copie, publique ou reutilize material sem autorização e licença compatível.

Registros e evidências relacionadas: Inventário de licenças; contratos; registros de desenvolvimento; política de software; termos de confidencialidade.

11.33. PROTEÇÃO DE REGISTROS

Diretriz executiva: Registros devem permanecer legíveis, íntegros, disponíveis e protegidos pelo período necessário, com descarte controlado.

Aplicação na Vert Analytics: Regras de temporalidade abrangem contratos, evidências de auditoria, logs, documentos de projeto, registros de pessoas, segurança, privacidade, atendimento e operações. Retenções excessivas também são evitadas.

Nota de uso: Não elimine ou altere registros corporativos fora do procedimento aprovado, especialmente quando houver investigação, auditoria ou obrigação legal.

Registros e evidências relacionadas: Matriz de temporalidade; ECM; política de backup; registros de descarte; base legal e contratual.

11.34. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Diretriz executiva: Dados pessoais devem ser tratados de forma legítima, transparente, segura, limitada à finalidade e compatível com os direitos dos titulares.

Aplicação na Vert Analytics: A Vert Analytics integra LGPD, ROPA, Mapa de Dados, AIPD/DPIA, gestão de consentimento quando aplicável, contratos, segurança desde a concepção, atendimento a titulares e avaliação de incidentes. Dados biométricos e outros dados sensíveis recebem proteção reforçada.

Nota de uso: Utilize somente os dados necessários, para a finalidade autorizada, no ambiente aprovado. Encaminhe solicitações de titulares ao canal de privacidade.

Registros e evidências relacionadas: Política de Privacidade; ROPA; AIPD/DPIA; Mapa de Dados; contratos; registros de atendimento; plano de incidentes.

11.35. ANÁLISE INDEPENDENTE DA SEGURANÇA DA INFORMAÇÃO

Diretriz executiva: O SGSI deve ser avaliado por pessoas com independência suficiente para verificar adequação, implementação e eficácia.





Aplicação na Vert Analytics: Auditorias internas, avaliações especializadas e auditorias externas são planejadas considerando risco, imparcialidade e competência. Resultados são tratados pela gestão e acompanhados até a verificação de eficácia.

Nota de uso: Coopere com auditorias, forneça evidências autênticas e registre limitações; não crie evidências retroativas.

Registros e evidências relacionadas: Programa de auditoria; relatórios; planos de ação; atas de análise crítica; registros de competência.

11.36. CONFORMIDADE COM POLÍTICAS, REGRAS E PADRÕES DE SEGURANÇA

Diretriz executiva: A aderência aos controles deve ser monitorada, e desvios devem gerar orientação, correção, tratamento de risco ou ação disciplinar proporcional.

Aplicação na Vert Analytics: Verificações podem envolver revisão de acessos, configurações, registros, documentos, contratos, práticas de usuários e requisitos de projetos. Exceções devem ser formais e temporárias.

Nota de uso: Não trate práticas informais como autorização. Registre exceções antes da execução sempre que possível.

Registros e evidências relacionadas: Checklists de conformidade; relatórios; registros de exceção; não conformidades; planos de ação.

11.37. PROCEDIMENTOS OPERACIONAIS DOCUMENTADOS

Diretriz executiva: Atividades relevantes devem possuir procedimentos claros, atualizados, acessíveis e controlados.

Aplicação na Vert Analytics: Procedimentos descrevem entradas, responsabilidades, etapas, controles, registros, indicadores, contingências e aprovações. A consulta oficial ocorre no ECM; cópias impressas são consideradas não controladas.

Nota de uso: Use a versão vigente no ECM e comunique inconsistências ou oportunidades de melhoria.

Registros e evidências relacionadas: Procedimentos do SGSI/SGPI; SIPOCs; formulários FO-001 a FO-160; histórico de versões; registros de treinamento.

12. CONTROLES DE PESSOAS

Responsabilidades e proteção ao longo do ciclo de vida das pessoas.

12.1. VERIFICAÇÃO PRÉVIA

Diretriz executiva: Verificações relacionadas a pessoas devem ser proporcionais à função, ao risco, à legislação e à privacidade.

Aplicação na Vert Analytics: Antes da contratação ou alocação em atividades sensíveis, podem ser verificadas qualificações, referências, identidade, conflitos e requisitos contratuais, dentro dos limites legais e com acesso restrito.

Nota de uso: Forneça informações verdadeiras e utilize os canais oficiais para documentação pessoal.

Registros e evidências relacionadas: Procedimento de recrutamento; consentimentos ou bases legais; registros de verificação; análise de risco da função.

12.2. TERMOS E CONDIÇÕES DE CONTRATAÇÃO

Diretriz executiva: Obrigações de segurança, privacidade, confidencialidade e uso de recursos devem constar nos instrumentos aplicáveis à relação de trabalho ou prestação.

Aplicação na Vert Analytics: Contratos, termos e políticas comunicam deveres durante e após o vínculo, incluindo propriedade intelectual, tratamento de dados, ativos, monitoramento, incidentes e sanções.

Nota de uso: Leia e cumpra os termos assinados; solicite esclarecimento antes de aceitar atividade incompatível.

Registros e evidências relacionadas: Contratos; termos de responsabilidade; código de conduta; políticas; registros de aceite.

12.3. CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO

Diretriz executiva: Pessoas devem receber orientação contínua e adequada ao papel, aos riscos e às mudanças do ambiente.

Aplicação na Vert Analytics: O programa combina integração, campanhas, treinamentos em EAD, reciclagens, avaliações, simulações e conteúdos específicos para gestores, desenvolvedores, administradores, atendimento, privacidade e fornecedores.



Nota de uso: Aplique o aprendizado no trabalho diário e conclua treinamentos dentro dos prazos definidos.

Registros e evidências relacionadas: Plano anual de conscientização; EAD; listas de presença; avaliações; campanhas; indicadores.

12.4. PROCESSO DISCIPLINAR

Diretriz executiva: Violações deliberadas ou negligentes devem ser tratadas por processo justo, documentado, proporcional e compatível com a legislação.

Aplicação na Vert Analytics: A apuração considera gravidade, intenção, reincidência, impacto, cooperação e responsabilidades. Medidas disciplinares não substituem correções técnicas, melhoria de processo ou comunicação legal.

Nota de uso: Reporte falhas de boa-fé; ocultar incidente ou retaliar quem reporta pode agravar o tratamento.

Registros e evidências relacionadas: Código de conduta; procedimento disciplinar; registros de apuração; ações corretivas.

12.5. RESPONSABILIDADES APÓS TÉRMINO OU MUDANÇA

Diretriz executiva: Obrigações que permanecem válidas devem ser comunicadas e aplicadas após desligamento, transferência ou mudança de função.

Aplicação na Vert Analytics: Confidencialidade, propriedade intelectual, proteção de dados e devolução de ativos permanecem conforme contrato e lei. Acessos são ajustados rapidamente ao novo contexto.

Nota de uso: Mudança de equipe não autoriza manter acessos ou cópias anteriores.

Registros e evidências relacionadas: Checklist de movimentação; termos de confidencialidade; registros de acesso; devolução de ativos.

12.6. ACORDOS DE CONFIDENCIALIDADE

Diretriz executiva: Acordos de confidencialidade devem proteger informações da Vert Analytics, clientes, parceiros, colaboradores e titulares.

Aplicação na Vert Analytics: O conteúdo define informações abrangidas, finalidade, prazo, exceções legais, retorno, descarte e consequências. A necessidade é revisada conforme riscos e relações.

Nota de uso: Compartilhe informações confidenciais apenas com destinatários autorizados e cobertos por obrigação adequada.

Registros e evidências relacionadas: NDA; cláusulas contratuais; registros de assinatura; classificação da informação.

12.7. TRABALHO REMOTO

Diretriz executiva: O trabalho remoto deve preservar segurança, privacidade, ergonomia operacional e continuidade em nível compatível com o ambiente corporativo.

Aplicação na Vert Analytics: São aplicados dispositivos e acessos aprovados, autenticação reforçada, proteção de tela, rede adequada, comunicação segura, cuidados com impressão, conversas e armazenamento local. Ambientes públicos exigem atenção adicional.

Nota de uso: Evite Wi-Fi inseguro, exposição de tela e conversas sensíveis em locais compartilhados. Bloqueie o equipamento ao se afastar.

Registros e evidências relacionadas: Política de trabalho remoto; inventário de endpoints; registros de acesso; termo de responsabilidade.

12.8. RELATO DE EVENTOS DE SEGURANÇA

Diretriz executiva: Toda pessoa deve comunicar rapidamente eventos, suspeitas, fragilidades e comportamentos anormais.

Aplicação na Vert Analytics: São reportáveis mensagens suspeitas, perda de dispositivo, envio incorreto, acesso indevido, vazamento, falha de sistema, alteração não autorizada, exposição de credencial e comportamento incomum de ferramentas ou modelos.

Nota de uso: Ao perceber algo anormal, pare a ação de risco quando seguro, preserve evidências e comunique imediatamente pelos canais oficiais.

Registros e evidências relacionadas: Registros de eventos; tickets; campanhas; plano de incidentes; indicadores de tempo de reporte.

13. CONTROLES FÍSICOS

Proteção de instalações, áreas, equipamentos e condições ambientais.

13.1. PERÍMETROS DE SEGURANÇA FÍSICA

Diretriz executiva: Áreas que processam ou armazenam informações devem possuir limites físicos compatíveis com o risco.

Aplicação na Vert Analytics: Escritórios, salas técnicas, arquivos, áreas de atendimento e ambientes de terceiros são classificados e protegidos por barreiras, regras de acesso e controles complementares.

Nota de uso: Respeite sinalizações, portas, barreiras e restrições de circulação.

Registros e evidências relacionadas: Plantas e classificação de áreas; avaliações físicas; registros de acesso; MR-001.

13.2. ENTRADA FÍSICA

Diretriz executiva: O acesso físico deve ser autorizado, identificado, registrado quando necessário e revogado ao término da necessidade.

Aplicação na Vert Analytics: Visitantes, colaboradores, prestadores e entregas seguem procedimentos de recepção, identificação, acompanhamento e restrição. Credenciais físicas são pessoais.

Nota de uso: Não permita entrada por carona, não empreste crachá e questione de forma segura acessos sem identificação.

Registros e evidências relacionadas: Cadastro de acesso; registros de visitantes; credenciais; procedimento de recepção.

13.3. PROTEÇÃO DE ESCRITÓRIOS, SALAS E INSTALAÇÕES

Diretriz executiva: Ambientes devem ser configurados para reduzir acesso indevido, observação, furto, dano e interrupção.

Aplicação na Vert Analytics: Portas, janelas, armários, salas, mobiliário, equipamentos e posicionamento de áreas são avaliados conforme informações e operações realizadas.

Nota de uso: Mantenha áreas protegidas fechadas e não exponha documentos ou equipamentos em locais de circulação.

Registros e evidências relacionadas: Inspeções físicas; inventário; registros de manutenção; avaliação de risco.

13.4. MONITORAMENTO DE SEGURANÇA FÍSICA

Diretriz executiva: Áreas críticas podem ser monitoradas para detectar acessos não autorizados e apoiar investigação, respeitando privacidade e legislação.

Aplicação na Vert Analytics: Monitoramento pode incluir alarmes, registros de acesso, vigilância e imagens, com retenção, acesso e finalidade controlados.

Nota de uso: Não bloqueie, desative ou altere dispositivos de monitoramento. Encaminhe solicitações de imagens aos responsáveis.

Registros e evidências relacionadas: Registros de monitoramento; política de privacidade; retenção; manutenção; incidentes.

13.5. PROTEÇÃO CONTRA AMEAÇAS FÍSICAS E AMBIENTAIS

Diretriz executiva: Instalações e ativos devem ser protegidos contra incêndio, água, calor, energia, eventos climáticos, acidentes e outras ameaças.

Aplicação na Vert Analytics: A avaliação considera localização, infraestrutura, recursos de combate, rotas de saída, climatização, manutenção, continuidade e mudanças climáticas relevantes ao contexto da organização.

Nota de uso: Siga instruções de emergência e reporte sinais de risco, como aquecimento, vazamento, odor, faísca ou obstrução.

Registros e evidências relacionadas: AIA-001; MR-001; planos de emergência e continuidade; inspeções; manutenção.

13.6. TRABALHO EM ÁREAS SEGURAS

Diretriz executiva: Atividades em áreas restritas devem seguir regras adicionais de acesso, acompanhamento, comunicação e registro.

Aplicação na Vert Analytics: Intervenções técnicas, visitas, manutenção, manipulação de mídias e acesso a equipamentos críticos são autorizados e supervisionados conforme risco.

Nota de uso: Não fotografe, grave ou conecte dispositivos em área segura sem autorização.

Registros e evidências relacionadas: Procedimento de área segura; ordens de serviço; registros de acesso; termos de terceiros.

13.7. MESA LIMPA E TELA LIMPA

Diretriz executiva: Informações não devem permanecer expostas quando não estiverem em uso.

Aplicação na Vert Analytics: Documentos, anotações, crachás, mídias e dispositivos são guardados; telas são bloqueadas e impressões são retiradas prontamente. Reuniões e home office seguem o mesmo princípio.

Nota de uso: Ao se afastar, bloqueie a tela e guarde conteúdos sensíveis.

Registros e evidências relacionadas: Campanhas; inspeções; política de classificação; configurações de bloqueio.

13.8. POSICIONAMENTO E PROTEÇÃO DE EQUIPAMENTOS

Diretriz executiva: Equipamentos devem ser instalados e protegidos para reduzir dano, acesso indevido, observação e interrupção.

Aplicação na Vert Analytics: Posicionamento considera circulação, calor, umidade, energia, cabos, tela, acesso físico e necessidade de manutenção. Equipamentos críticos recebem proteção adicional.

Nota de uso: Não mova ou reconfigure equipamento corporativo sem autorização.

Registros e evidências relacionadas: Inventário; registros de instalação; manutenção; avaliação física.

13.9. SEGURANÇA DE ATIVOS FORA DAS INSTALAÇÕES

Diretriz executiva: Ativos utilizados externamente devem receber proteção equivalente ao risco e à informação tratada.

Aplicação na Vert Analytics: Notebooks, celulares, mídias, documentos e equipamentos em trânsito ou trabalho remoto utilizam controles de custódia, criptografia, acesso e reporte de perda.

Nota de uso: Mantenha ativos sob supervisão, evite deixá-los em veículos e comunique perda ou furto imediatamente.

Registros e evidências relacionadas: Termo de custódia; inventário; criptografia; registros de incidente; trabalho remoto.

13.10. MÍDIAS DE ARMAZENAMENTO

Diretriz executiva: Mídias devem ser autorizadas, inventariadas quando aplicável, protegidas, transportadas e descartadas de forma segura.

Aplicação na Vert Analytics: O uso de mídia removível é restrito conforme risco. Transferências, cópias, retenção e eliminação consideram classificação e rastreabilidade.

Nota de uso: Não conecte mídia desconhecida ou pessoal em equipamento corporativo.

Registros e evidências relacionadas: Procedimento de mídias; inventário; registros de cópia; descarte seguro.



13.11. UTILIDADES DE SUPORTE

Diretriz executiva: Energia, climatização, telecomunicações e demais utilidades devem sustentar a operação e possuir proteção proporcional.

Aplicação na Vert Analytics: Ambientes críticos consideram redundância, autonomia, manutenção, alarmes e contingência. Falhas recorrentes são analisadas como riscos de continuidade.

Nota de uso: Reporte instabilidade ou falha de infraestrutura sem improvisar conexões ou extensões não autorizadas.

Registros e evidências relacionadas: Planos de manutenção; testes; PCN; registros de falha; contratos de suporte.

13.12. SEGURANÇA DE CABEAMENTO

Diretriz executiva: Cabos de energia e dados devem ser protegidos contra danos, interceptação, desconexão e identificação inadequada.

Aplicação na Vert Analytics: Rotas, racks, pontos, patch panels e conexões são organizados, identificados e restritos conforme criticidade.

Nota de uso: Não conecte, desconecte ou altere cabeamento de rede sem autorização técnica.

Registros e evidências relacionadas: Diagramas; inventário; registros de mudança; inspeções; ordens de serviço.

13.13. MANUTENÇÃO DE EQUIPAMENTOS

Diretriz executiva: Equipamentos devem receber manutenção autorizada, registrada e segura, preservando disponibilidade e informações.

Aplicação na Vert Analytics: Antes da manutenção, são avaliados backup, mídia, acesso do técnico, peças, garantia, retorno ao serviço e proteção de dados. Terceiros são acompanhados quando necessário.

Nota de uso: Abra chamado e não entregue equipamento com dados a assistência não autorizada.

Registros e evidências relacionadas: Plano de manutenção; chamados; termos de terceiros; inventário; registros de teste.

13.14. DESCARTE SEGURO OU REUTILIZAÇÃO DE EQUIPAMENTOS

Diretriz executiva: Antes do descarte, devolução, doação ou reutilização, dados e configurações devem ser removidos de modo verificável.



Aplicação na Vert Analytics: O método considera tipo de mídia, sensibilidade, capacidade de sobrescrita, destruição, restauração de fábrica e cadeia de custódia. Licenças e identificações também são tratadas.

Nota de uso: Não doe, venda ou descarte ativo corporativo por conta própria.

Registros e evidências relacionadas: Termo de descarte; certificado de destruição; inventário; registros de sanitização; logística reversa.

14. CONTROLES TECNOLÓGICOS

Proteção técnica de dispositivos, identidades, redes, sistemas, dados e desenvolvimento.

14.1. DISPOSITIVOS DE USUÁRIO FINAL

Diretriz executiva: Endpoints devem ser configurados, atualizados, protegidos e utilizados de acordo com o risco.

Aplicação na Vert Analytics: Notebooks, desktops, celulares e demais dispositivos podem utilizar criptografia, gestão centralizada, proteção contra malware, bloqueio, inventário, backup de dados autorizados e restrições de software. BYOD depende de aprovação formal.

Nota de uso: Não desative proteções, adie atualizações críticas ou compartilhe o dispositivo com pessoas não autorizadas.

Registros e evidências relacionadas: Padrão de endpoint; inventário; EDR/antimalware; registros de atualização; termo de uso.

14.2. DIREITOS DE ACESSO PRIVILEGIADO

Diretriz executiva: Privilégios administrativos devem ser limitados, justificados, protegidos e monitorados.

Aplicação na Vert Analytics: Contas privilegiadas são separadas do uso cotidiano, aprovadas, revisadas e utilizadas somente pelo tempo necessário. Atividades críticas podem exigir registro de sessão ou dupla autorização.

Nota de uso: Não use privilégio administrativo para conveniência e não navegue ou leia e-mail com conta privilegiada.

Registros e evidências relacionadas: Inventário de privilégios; PAM ou controles equivalentes; logs; aprovações; recertificações.

14.3. RESTRIÇÃO DE ACESSO À INFORMAÇÃO

Diretriz executiva: Sistemas devem aplicar restrições coerentes com classificação, função, contrato e finalidade.

Aplicação na Vert Analytics: Controles podem atuar em aplicação, banco, API, repositório, relatório, campo, linha, modelo ou ambiente. Restrições também consideram dados pessoais, cliente e projeto.

Nota de uso: Não exporte ou agregue dados para ampliar acesso além do autorizado.

Registros e evidências relacionadas: Matriz de acesso; regras de aplicação; logs; testes de autorização; ROPA.

14.4. ACESSO AO CÓDIGO-FONTE

Diretriz executiva: Código-fonte, scripts, infraestrutura como código, modelos e artefatos de desenvolvimento devem ter acesso restrito e rastreável.

Aplicação na Vert Analytics: Repositórios utilizam identidades individuais, revisão, proteção de branches, gestão de segredos, histórico e segregação. Cópias locais e compartilhamentos externos são controlados.

Nota de uso: Não inclua credenciais ou dados reais no código e não publique repositórios corporativos.

Registros e evidências relacionadas: Repositórios; políticas de branch; revisões; logs; inventário de código; gestão de segredos.

14.5. AUTENTICAÇÃO SEGURA

Diretriz executiva: Mecanismos de autenticação devem resistir a tentativa de fraude, roubo de credencial, automação e reutilização.

Aplicação na Vert Analytics: A arquitetura considera MFA, limitação de tentativas, proteção de sessão, recuperação segura, autenticação de APIs, certificados e mecanismos adequados à criticidade, inclusive em onboarding e biometria.

Nota de uso: Desconfie de solicitações de código de autenticação e confirme canais de recuperação.

Registros e evidências relacionadas: Padrão de autenticação; testes; logs; configurações; análise de risco.

14.6. GESTÃO DE CAPACIDADE

Diretriz executiva: Capacidade de processamento, armazenamento, rede, licenças e serviços deve ser monitorada e planejada.



Aplicação na Vert Analytics: A Vert Analytics acompanha crescimento de dados, transações, documentos, modelos, filas, integrações e uso de nuvem para evitar degradação e indisponibilidade. Limites e alertas suportam expansão controlada.

Nota de uso: Não execute cargas intensivas ou grandes extrações fora da janela e do processo definidos.

Registros e evidências relacionadas: Relatórios de capacidade; monitoramento; planos de expansão; registros de desempenho.

14.7. PROTEÇÃO CONTRA MALWARE

Diretriz executiva: A organização deve prevenir, detectar e responder a códigos maliciosos e comportamentos anômalos.

Aplicação na Vert Analytics: Controles incluem proteção de endpoint, e-mail, navegação, arquivos, servidores, atualizações, restrições de execução e conscientização. Detecções são analisadas e correlacionadas com incidentes.

Nota de uso: Não abra arquivo suspeito, habilite macro desconhecida ou ignore alerta de segurança.

Registros e evidências relacionadas: EDR/antimalware; filtros; logs; incidentes; campanhas de phishing.

14.8. GESTÃO DE VULNERABILIDADES TÉCNICAS

Diretriz executiva: Vulnerabilidades devem ser identificadas, avaliadas, priorizadas e tratadas segundo risco e prazo.

Aplicação na Vert Analytics: O processo abrange ativos, aplicações, APIs, sistemas, bibliotecas, imagens, nuvem e equipamentos. Varreduras, testes autorizados, alertas e avaliações de impacto orientam correção, mitigação ou aceitação formal.

Nota de uso: Não realize varreduras ou testes de invasão sem autorização. Reporte vulnerabilidades de forma responsável.

Registros e evidências relacionadas: Inventário; relatórios de vulnerabilidade; plano de correção; testes; exceções; MR-001.

14.9. GESTÃO DE CONFIGURAÇÃO

Diretriz executiva: Configurações seguras devem ser definidas, aplicadas, registradas e monitoradas.

Aplicação na Vert Analytics: Baselines contemplam sistemas operacionais, bancos, nuvem, redes, aplicações, containers, dispositivos e serviços. Desvios são analisados e mudanças seguem controle.

Nota de uso: Não altere configuração de segurança para resolver problema operacional sem aprovação e registro.

Registros e evidências relacionadas: Baselines; inventário; configuração como código; registros de mudança; verificações de conformidade.

14.10. ELIMINAÇÃO DE INFORMAÇÃO

Diretriz executiva: Informações devem ser eliminadas quando não houver necessidade, obrigação ou retenção autorizada.

Aplicação na Vert Analytics: A eliminação inclui sistemas, bancos, backups conforme ciclo, nuvem, dispositivos, ambientes de teste e cópias de terceiros. Métodos devem ser compatíveis com a mídia e registrados quando necessário.

Nota de uso: Não mantenha cópias 'por precaução' fora dos prazos e finalidades definidos.

Registros e evidências relacionadas: Matriz de temporalidade; registros de exclusão; contratos; ROPA; certificados de descarte.

14.11. MASCARAMENTO DE DADOS

Diretriz executiva: Dados sensíveis devem ser reduzidos, ofuscados, tokenizados ou anonimizados quando a exposição integral não for necessária.

Aplicação na Vert Analytics: Mascaramento é aplicado em telas, relatórios, suporte, desenvolvimento, testes, analytics e compartilhamentos, respeitando finalidade e risco de reidentificação.

Nota de uso: Utilize visualizações mascaradas e evite copiar dados completos para facilitar testes ou demonstrações.

Registros e evidências relacionadas: Padrão de mascaramento; arquitetura; testes; ROPA; AIPD/DPIA.

14.12. PREVENÇÃO CONTRA VAZAMENTO DE DADOS

Diretriz executiva: A organização deve reduzir a possibilidade de saída não autorizada de informações.

Aplicação na Vert Analytics: Controles podem monitorar e restringir e-mail, web, nuvem, endpoint, impressão, dispositivos, APIs e grandes extrações. Alertas são analisados com respeito à finalidade e às regras de privacidade.

Nota de uso: Não tente contornar bloqueios de envio ou transferência; solicite o canal adequado.

Registros e evidências relacionadas: DLP ou controles equivalentes; classificação; logs; incidentes; exceções.

14.13. BACKUP DE INFORMAÇÕES

Diretriz executiva: Cópias de segurança devem ser planejadas, protegidas, monitoradas e testadas conforme requisitos de recuperação.

Aplicação na Vert Analytics: Escopo, frequência, retenção, criptografia, segregação, imutabilidade quando aplicável e testes são definidos por criticidade. Backup não substitui controles de versionamento e continuidade.

Nota de uso: Salve arquivos nos repositórios aprovados; dados mantidos apenas localmente podem não estar protegidos.

Registros e evidências relacionadas: Política e plano de backup; relatórios; testes de restauração; BIA; inventário.

14.14. REDUNDÂNCIA DE RECURSOS DE PROCESSAMENTO

Diretriz executiva: Recursos críticos devem possuir redundância ou alternativas compatíveis com os objetivos de disponibilidade.

Aplicação na Vert Analytics: A arquitetura avalia componentes, zonas, links, serviços, dados e dependências. Redundância deve ser testada, monitorada e protegida contra falhas comuns.

Nota de uso: Não assuma que um serviço é redundante sem evidência e teste; registre dependências únicas.

Registros e evidências relacionadas: Arquitetura; testes de failover; PCN/PRD; relatórios de disponibilidade; MR-001.

14.15. REGISTRO DE EVENTOS

Diretriz executiva: Eventos relevantes devem ser registrados com conteúdo, proteção, retenção e acesso adequados.

Aplicação na Vert Analytics: Logs apoiam segurança, operação, auditoria e investigação, contemplando autenticação, privilégios, mudanças, acessos, transações, integrações e erros. Dados excessivos ou sensíveis são evitados quando não necessários.

Nota de uso: Não apague ou altere logs. Encaminhe solicitações de acesso pelo processo formal.

Registros e evidências relacionadas: Política de logs; inventário de fontes; retenção; trilhas de auditoria; cadeia de custódia.

14.16. ATIVIDADES DE MONITORAMENTO

Diretriz executiva: Ambientes e atividades devem ser monitorados para identificar comportamentos anômalos, falhas e incidentes.

Aplicação na Vert Analytics: Alertas de infraestrutura, segurança, aplicação, rede, identidades, dados e serviços são correlacionados e priorizados. Limites são ajustados para manter utilidade e reduzir ruído.

Nota de uso: Reporte alertas recorrentes ou comportamentos incomuns; não silencie monitoramento sem autorização.

Registros e evidências relacionadas: Plataformas de monitoramento; regras de alerta; tickets; relatórios; indicadores.

14.17. SINCRONIZAÇÃO DE RELÓGIOS

Diretriz executiva: Sistemas relevantes devem utilizar referências de tempo confiáveis e consistentes.

Aplicação na Vert Analytics: A sincronização melhora correlação de logs, investigação, transações, autenticação, certificados e auditoria. Desvios são monitorados e tratados.

Nota de uso: Não altere manualmente data ou hora de sistemas corporativos.

Registros e evidências relacionadas: Configuração de NTP; monitoramento; logs; testes; inventário.

14.18. USO DE PROGRAMAS UTILITÁRIOS PRIVILEGIADOS

Diretriz executiva: Ferramentas capazes de contornar controles devem ser estritamente limitadas e monitoradas.

Aplicação na Vert Analytics: Utilitários de administração, diagnóstico, extração, recuperação e alteração direta são autorizados por função, registrados e usados em contexto controlado.

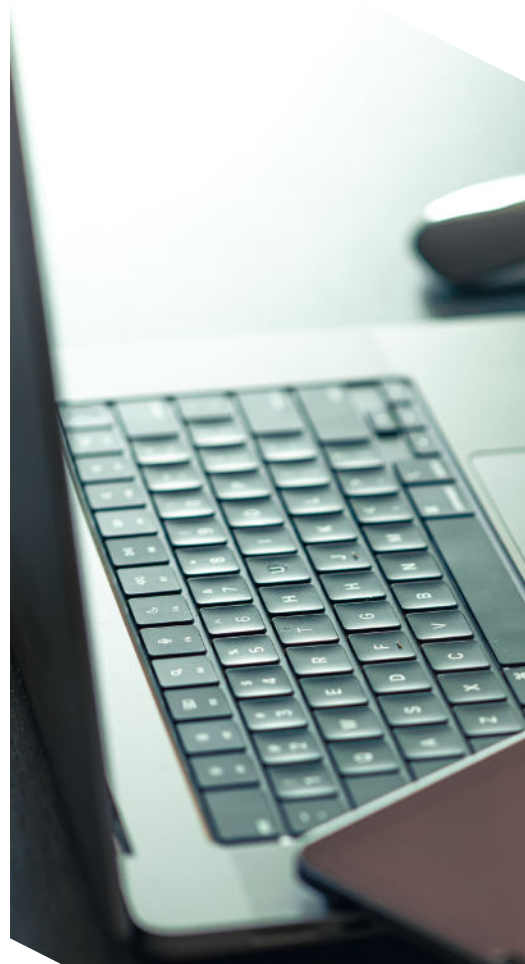
Nota de uso: Não execute ferramentas administrativas portáteis ou desconhecidas em ativos corporativos.

Registros e evidências relacionadas: Lista de utilitários; privilégios; logs; registros de uso; gestão de software.

14.19. INSTALAÇÃO DE SOFTWARE EM SISTEMAS OPERACIONAIS

Diretriz executiva: Instalações em produção devem ser autorizadas, testadas e rastreáveis.

Aplicação na Vert Analytics: Somente software aprovado, licenciado e proveniente de fonte confiável pode ser instalado. Alterações seguem gestão de mudanças, verificação de integridade e plano de reversão.



Nota de uso: Não instale software por conta própria, mesmo gratuito, em equipamento ou ambiente corporativo.

Registros e evidências relacionadas: Catálogo de software; licenças; registros de mudança; inventário; testes.

14.20. SEGURANÇA DE REDES

Diretriz executiva: Redes devem ser arquitetadas, configuradas e monitoradas para proteger comunicações e serviços.

Aplicação na Vert Analytics: Controles incluem filtragem, segmentação, proteção de borda, acesso remoto, administração segura, detecção, hardening e documentação. Conexões com clientes, nuvem e terceiros são avaliadas.

Nota de uso: Não conecte equipamento, roteador, ponto de acesso ou túnel não autorizado.

Registros e evidências relacionadas: Diagramas de rede; regras de firewall; logs; inventário; testes; mudanças.

14.21. SEGURANÇA DE SERVIÇOS DE REDE

Diretriz executiva: Requisitos de segurança, capacidade e níveis de serviço de rede devem ser definidos e acompanhados.

Aplicação na Vert Analytics: Serviços internos e terceirizados contemplam autenticação, criptografia, disponibilidade, monitoramento, suporte, responsabilidades e incidentes.

Nota de uso: Utilize VPN e outros serviços de rede conforme orientação; não substitua por solução pessoal.

Registros e evidências relacionadas: Catálogo de serviços; SLA; contratos; configurações; relatórios de disponibilidade.

14.22. SEGREGAÇÃO DE REDES

Diretriz executiva: Usuários, sistemas e serviços com riscos distintos devem ser separados logicamente ou fisicamente.

Aplicação na Vert Analytics: Segmentação pode separar produção, desenvolvimento, teste, administração, visitantes, dispositivos, clientes e cargas sensíveis. Fluxos necessários são explicitamente autorizados.

Nota de uso: Não tente criar ponte, compartilhamento ou rota entre redes sem aprovação.

Registros e evidências relacionadas: Arquitetura; VLANs e regras; matriz de fluxo; testes; registros de mudança.

14.23. FILTRAGEM DE ACESSO À WEB

Diretriz executiva: O acesso a conteúdo web deve ser protegido contra ameaças e uso incompatível.

Aplicação na Vert Analytics: Filtros, reputação, inspeção e políticas de navegação podem bloquear conteúdo malicioso, fraude, comando e controle, download arriscado e categorias não autorizadas. Exceções são justificadas.

Nota de uso: Não utilize proxy ou serviço alternativo para contornar bloqueio.

Registros e evidências relacionadas: Política de acesso web; logs; filtros; exceções; incidentes.

14.24. USO DE CRIPTOGRAFIA

Diretriz executiva: Criptografia deve proteger confidencialidade, integridade, autenticidade e não repúdio quando requerido.

Aplicação na Vert Analytics: Padrões definem algoritmos, protocolos, chaves, certificados, armazenamento, rotação, revogação e responsabilidades. A aplicação considera dados em trânsito, repouso, backup, endpoint, APIs e assinaturas.

Nota de uso: Utilize apenas mecanismos aprovados; não crie chaves ou senhas compartilhadas sem gestão adequada.

Registros e evidências relacionadas: Política criptográfica; inventário de certificados; cofre de chaves; configurações; registros de rotação.

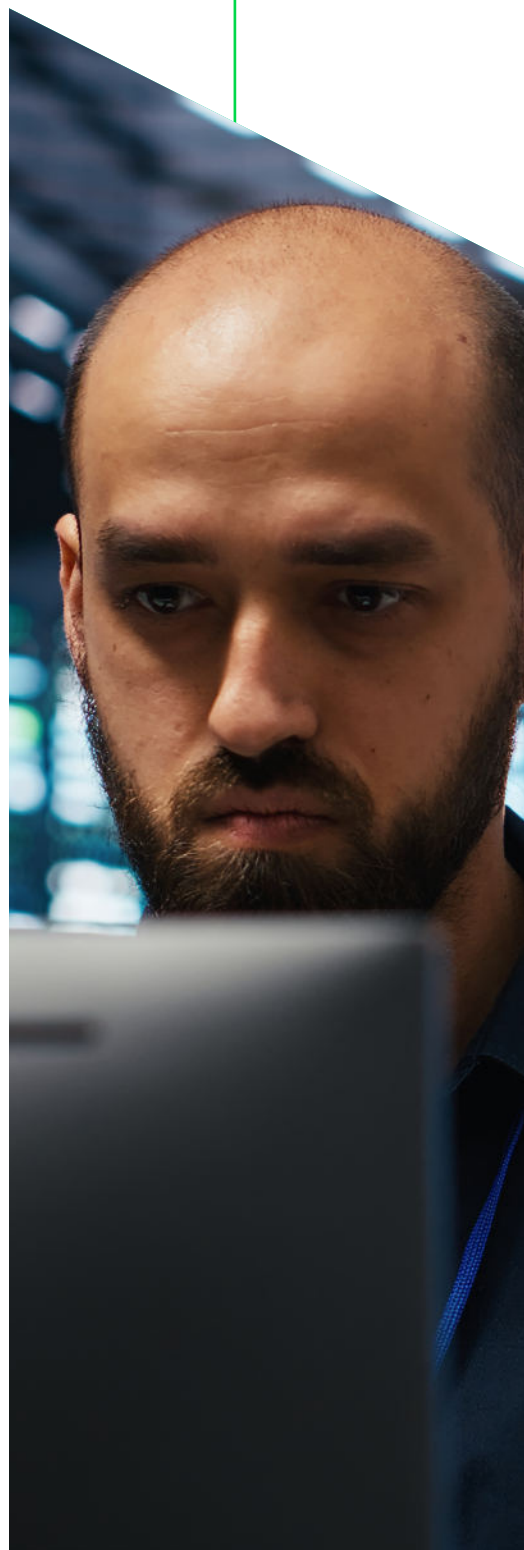
14.25. CICLO DE VIDA DE DESENVOLVIMENTO SEGURO

Diretriz executiva: Segurança e privacidade devem integrar planejamento, desenho, construção, teste, implantação, manutenção e retirada de sistemas.

Aplicação na Vert Analytics: O ciclo considera requisitos, ameaça, arquitetura, código, dependências, dados, IA, integrações, testes, mudanças e operação. Critérios de aceite impedem liberação sem riscos conhecidos tratados.

Nota de uso: Incorpore segurança desde a primeira decisão técnica; correção tardia não substitui desenho seguro.

Registros e evidências relacionadas: SDLC seguro; checklists; threat modeling; revisões; testes; termos de aceite.



14.26. REQUISITOS DE SEGURANÇA DE APLICAÇÕES

Diretriz executiva: Requisitos de segurança devem ser definidos antes da aquisição ou desenvolvimento de aplicações.

Aplicação na Vert Analytics: Autenticação, autorização, validação, logs, privacidade, criptografia, disponibilidade, interfaces, prevenção a fraude e tratamento de erro são proporcionais ao risco e ao contexto do cliente.

Nota de uso: Registre requisitos verificáveis e critérios de aceite; não use expressões vagas como 'sistema seguro'.

Registros e evidências relacionadas: Especificações; histórias e critérios; AIPD/DPIA; arquitetura; testes de aceite.

14.27. ARQUITETURA SEGURA E PRINCÍPIOS DE ENGENHARIA

Diretriz executiva: Soluções devem utilizar princípios de defesa em profundidade, menor privilégio, confiança mínima, simplicidade e falha segura.

Aplicação na Vert Analytics: Arquiteturas de dados, IA, APIs, nuvem e integração consideram fronteiras, dependências, segregação, resiliência, observabilidade e proteção por padrão. Decisões relevantes são registradas.

Nota de uso: Evite atalhos arquiteturais que criem dependência única, privilégio excessivo ou exposição desnecessária.

Registros e evidências relacionadas: Padrões de arquitetura; diagramas; decisões arquiteturais; revisões; MR-001.

14.28. CODIFICAÇÃO SEGURA

Diretriz executiva: Código deve ser produzido e revisado segundo práticas que reduzam vulnerabilidades e exposição de dados.

Aplicação na Vert Analytics: Diretrizes abrangem validação, tratamento de erro, autenticação, autorização, segredos, injeção, criptografia, dependências, logging e uso seguro de modelos e APIs. Revisões e ferramentas apoiam o processo.

Nota de uso: Nunca inclua dados reais, segredos ou chaves no código; corrija alertas de segurança conforme prioridade.

Registros e evidências relacionadas: Guia de codificação segura; revisão de código; SAST; inventário de dependências; treinamentos.

14.29. TESTES DE SEGURANÇA EM DESENVOLVIMENTO E ACEITAÇÃO

Diretriz executiva: Sistemas devem ser testados quanto a requisitos e vulnerabilidades antes da entrada em produção.

Aplicação na Vert Analytics: Testes podem incluir análise estática, dinâmica, dependências, configuração, autorização, APIs, abuso, privacidade, carga e pentest autorizado. Resultados críticos impedem liberação até tratamento ou aceite formal.

Nota de uso: Não teste produção ou dados de clientes fora do escopo autorizado.

Registros e evidências relacionadas: Plano e evidências de teste; relatórios; correções; aceite de risco; critérios de liberação.

14.30. DESENVOLVIMENTO TERCEIRIZADO

Diretriz executiva: Desenvolvimento realizado por terceiros deve seguir requisitos, supervisão, propriedade e segurança equivalentes aos internos.

Aplicação na Vert Analytics: Contratos definem práticas, acesso, código, dados, testes, dependências, vulnerabilidades, propriedade intelectual, entrega e suporte. A Vert Analytics mantém capacidade de revisão e aceite.

Nota de uso: Não forneça acesso ou dados a desenvolvedor externo sem contrato, aprovação e ambiente apropriado.

Registros e evidências relacionadas: Contrato de desenvolvimento; plano de projeto; revisões; testes; termo de aceite; inventário.

14.31. SEPARAÇÃO ENTRE DESENVOLVIMENTO, TESTE E PRODUÇÃO

Diretriz executiva: Ambientes devem ser separados para reduzir alteração indevida, exposição de dados e conflito de acesso.

Aplicação na Vert Analytics: Produção possui controles mais restritos; promoções seguem pipeline e aprovação. Dados reais em teste são evitados, mascarados ou formalmente autorizados. Acesso direto é excepcional.

Nota de uso: Não copie base de produção para teste ou altere produção para facilitar desenvolvimento.

Registros e evidências relacionadas: Arquitetura de ambientes; matriz de acesso; pipelines; mascaramento; registros de implantação.

14.32. GESTÃO DE MUDANÇAS

Diretriz executiva: Mudanças devem ser avaliadas, autorizadas, testadas, comunicadas e reversíveis conforme risco.

Aplicação na Vert Analytics: O processo considera impacto em segurança, privacidade, continuidade, capacidade, contratos, documentação e clientes. Mudanças emergenciais são registradas e revisadas posteriormente.

Nota de uso: Não implemente mudança fora do fluxo por pressão de prazo; acione o rito emergencial quando necessário.

Registros e evidências relacionadas: Requisições de mudança; aprovações; testes; plano de rollback; atas CAB; evidências de implantação.

14.33. INFORMAÇÕES DE TESTE

Diretriz executiva: Dados usados em teste devem ser selecionados e protegidos para evitar exposição e resultados inválidos.

Aplicação na Vert Analytics: Preferem-se dados sintéticos, anonimizados ou mascarados. Quando dados reais forem indispensáveis, acesso, finalidade, retenção e eliminação são formalmente controlados.

Nota de uso: Não utilize planilhas ou bases reais por conveniência em demonstrações e testes.

Registros e evidências relacionadas: Padrão de dados de teste; mascaramento; ROPA; AIPD/DPIA; registros de eliminação.

14.34. PROTEÇÃO DE SISTEMAS DURANTE TESTES DE AUDITORIA

Diretriz executiva: Testes de auditoria devem ser planejados para não comprometer disponibilidade, integridade, confidencialidade ou desempenho.

Aplicação na Vert Analytics: Escopo, janela, acesso, dados, monitoramento, backup, reversão e comunicação são definidos previamente. Evidências são coletadas com menor impacto e acesso temporário.

Nota de uso: Auditorias não autorizam mudanças ou testes destrutivos fora do escopo aprovado.

Registros e evidências relacionadas: Plano de auditoria; autorização de teste; logs; backup; relatório; revogação de acesso.

15. INTEGRAÇÃO COM PROTEÇÃO DE DADOS, IA E DECISÕES AUTOMATIZADAS

A segurança da informação e a proteção de dados pessoais são tratadas de forma integrada. Projetos que envolvam dados pessoais, biometria, reconhecimento facial, documentos, perfis, prevenção a fraudes, decisões automatizadas ou inteligência artificial devem considerar finalidade, base legal, necessidade, transparência, qualidade, não discriminação, segurança, prevenção e responsabilização.

- ▶ **Dados e modelos:** bases de treinamento, dados de entrada, prompts, parâmetros, saídas, modelos e logs são ativos e recebem classificação, proprietário, controle de acesso e retenção.
- ▶ **Revisão humana:** resultados automatizados que possam produzir impacto relevante devem possuir validação, supervisão e mecanismos de contestação quando aplicáveis.
- ▶ **Minimização:** devem ser utilizados somente os dados necessários, preferindo anonimização, mascaramento ou dados sintéticos em desenvolvimento e teste.
- ▶ **Transparência:** usuários e clientes recebem informações adequadas sobre tratamento e canais de exercício de direitos, respeitados segredos comerciais e requisitos de segurança.
- ▶ **Terceiros e nuvem:** provedores de modelos, APIs e infraestrutura são avaliados quanto a uso de dados, retenção, subcontratados, localização, segurança e encerramento.
- ▶ **Testes e monitoramento:** soluções são avaliadas quanto a abuso, fraude, segurança, qualidade, deriva, falhas, vieses e impactos de privacidade, conforme risco.

16. INDICADORES, MONITORAMENTO E ANÁLISE CRÍTICA

Dimensão	Exemplos de acompanhamento
Riscos	Percentual de riscos tratados no prazo; riscos acima do apetite; eficácia dos controles.
Acessos	Tempo de concessão e revogação; revisões concluídas; privilégios sem justificativa.
Vulnerabilidades	Tempo de correção por criticidade; ativos cobertos; reincidência.
Incidentes	Quantidade, severidade, tempo de detecção, reporte, contenção e recuperação.
Continuidade	Disponibilidade; cumprimento de RTO/RPO; testes e ações pendentes.
Pessoas	Treinamentos concluídos; avaliações; simulações; eventos reportados.
Fornecedores	Avaliações realizadas; pendências contratuais; SLA; incidentes de terceiros.
Privacidade	ROPA revisados; AIPDs; solicitações de titulares; incidentes com dados.
Auditorias	Não conformidades; planos em atraso; eficácia de ações corretivas.
Documentação	Documentos revisados no prazo; registros completos; versões obsoletas identificadas.

17. COMUNICAÇÃO DE EVENTOS, INCIDENTES E SOLICITAÇÕES

Reporte cedo. Preserve evidências. Evite exposição adicional.

Qualquer suspeita é melhor comunicada rapidamente do que investigada isoladamente. O reporte de boa-fé é incentivado e deve ser protegido contra a retaliação.

Suporte e eventos de segurança: suporte@vertanalytics.com.br

Privacidade e direitos dos titulares: privacidade@vertanalytics.com.br

Canal de Conformidade: [\[Acessar Canal de Conformidade\]](#)

Contato institucional: vert@vertanalytics.com.br

Comunicações à ANPD, titulares, clientes, autoridades, imprensa ou público são realizadas somente por funções autorizadas, após avaliação técnica, jurídica, contratual e de privacidade. Quando um incidente com dados pessoais puder acarretar risco ou dano relevante, a organização observará os prazos e requisitos regulatórios aplicáveis.

18. EXCEÇÕES, NÃO CONFORMIDADES E CONSEQUÊNCIAS

Exceções a esta Política devem ser justificadas, avaliadas quanto a risco, aprovadas por autoridade competente, limitadas em escopo e tempo e acompanhadas por controles compensatórios. A inexistência de solução ideal não autoriza o descumprimento informal.

Violações podem resultar em orientação, correção, restrição ou revogação de acesso, medidas contratuais ou disciplinares, responsabilização civil, administrativa ou penal e comunicação a partes competentes, conforme gravidade, intenção, impacto e legislação. A resposta deve ser justa, documentada e proporcional.

19. DOCUMENTAÇÃO RELACIONADA

Documento/artefato	Finalidade
MR-001	Matriz de Riscos de Segurança da Informação e Privacidade.
SoA e Matriz GAP	Declaração de Aplicabilidade e avaliação de atendimento aos controles ISO/IEC 27001 e ISO/IEC 27701.
Matriz de Partes Interessadas	Necessidades, expectativas, requisitos e formas de monitoramento.
Matriz Integrada de Comunicação, Classificação e Temporalidade	Regras de classificação, compartilhamento, retenção e descarte.
ROPA, AIPD/DPIA e Mapa de Dados LGPD	Registros de tratamento, fluxos de dados e avaliações de impacto.
PCN e planos de recuperação	Continuidade de negócios, contingência e prontidão de TIC.
SWOT-001	Análise de contexto e ações do SGSI/SGPI.
AIA-001	Avaliação de aspectos e impactos ambientais, incluindo contexto climático aplicável.
Base de requisitos legais, normativos e contratuais	Legislação, normas, regulamentos e obrigações de clientes.
Procedimentos, SIPOCs e FO-001 a FO-160	Detalhamento operacional, responsabilidades, registros e evidências.
Programa de conscientização e EAD	Capacitação, reciclagem, avaliação e sensibilização.
Política de Privacidade do site	Transparência sobre tratamento de dados pessoais em canais digitais.

20. REFERÊNCIAS EXTERNAS

ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. [Acessar referência](#)

ISO/IEC 27001:2022/Amd 1:2024. Emenda relacionada à consideração de mudanças climáticas no contexto e nas partes interessadas. [Acessar referência](#)

Lei nº 13.709/2018. Lei Geral de Proteção de Dados Pessoais - LGPD. [Acessar referência](#)

Lei nº 12.965/2014. Marco Civil da Internet. [Acessar referência](#)

Resolução CD/ANPD nº 15/2024. Regulamento de Comunicação de Incidente de Segurança. [Acessar referência](#)

Site institucional da Vert Analytics. Informações públicas sobre atuação, missão, visão, valores, serviços e contatos. **[Acessar referência]**

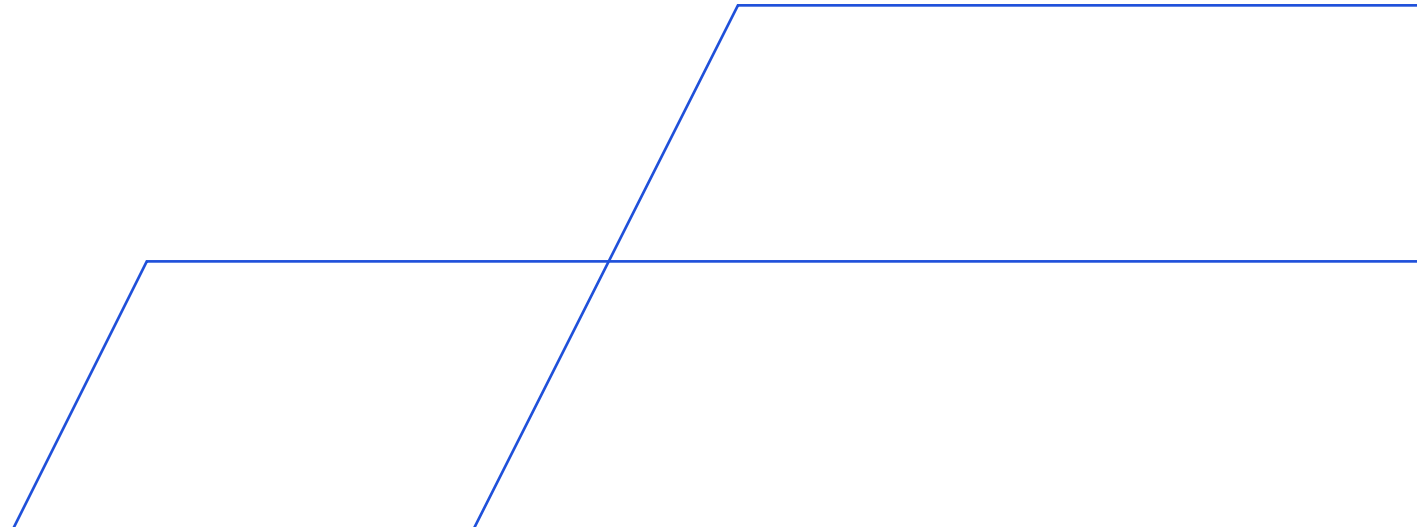
Política de Privacidade da Vert Analytics. Informações públicas sobre tratamento de dados pessoais em canais digitais. **[Acessar referência]**

Nota de direitos autorais

Esta Política apresenta interpretação e aplicação executiva próprias. Ela não substitui a aquisição, leitura e uso autorizado das normas ISO/IEC aplicáveis, nem reproduz seu conteúdo normativo integral.

21. GLOSSÁRIO ESSENCIAL

Termo	Definição
Ativo	Informação, dado, sistema, serviço, pessoa, dispositivo, infraestrutura, conhecimento ou outro recurso com valor para a organização.
AIPD/DPIA	Avaliação de impacto à proteção de dados pessoais, utilizada para analisar riscos e medidas de tratamento.
ECM	Ambiente corporativo de gestão de conteúdo e documentos; na Vert Analytics, a consulta oficial ocorre no repositório institucional/Outline Wiki.
Incidente de segurança	Evento confirmado que compromete ou ameaça confidencialidade, integridade, disponibilidade ou autenticidade.
Informação pessoal identificável	Informação que identifica ou pode identificar uma pessoa natural, direta ou indiretamente.
Menor privilégio	Concessão do mínimo de acesso necessário, pelo menor tempo compatível com a atividade.
ROPA	Registro das operações de tratamento de dados pessoais.
SGSI	Sistema de Gestão de Segurança da Informação.
SGPI	Sistema de Gestão de Privacidade da Informação.
SoA	Declaração de Aplicabilidade que registra controles aplicáveis, justificativas e situação de implementação.



22. CONTROLE DE VERSÕES, APROVAÇÃO E VIGÊNCIA

Versão	Data	Elaboração	Aprovação	Descrição
1.0	16/03/2026	Comitê SGSI/ SGPI	Alta Direção	Emissão inicial do documento no padrão do sistema de gestão.
1.1	13/07/2026	Comitê SGSI/ SGPI	Alta Direção	Ampliação para edição pública e executiva, com diretrizes para os 93 controles da ISO/IEC 27001:2022.

Vigência: a partir da aprovação e publicação, permanecendo válida até substituição por versão posterior.

Consulta oficial: ECM institucional / Outline Wiki. Cópias impressas são consideradas não controladas.





SEU TIME DE
RESULTADOS EM DADOS