

Checklist Mensal de Segurança da Informação

Protegendo Dados, Preservando Futuros

Introdução

Este documento é um farol de proteção no oceano digital, projetado para servidores públicos e funcionários internos que navegam pelas águas turbulentas da segurança da informação no Brasil. Ele guia, protege e assegura a conformidade com as normas mais elevadas, transformando cada verificação mensal em um ato de responsabilidade e cuidado. Ao seguir este checklist, você não apenas protege dados sensíveis, mas também constrói um futuro onde a privacidade é um direito inalienável.

Dados do Documento

Objetivo:	Proteger dados sensíveis e assegurar conformidade com normas de segurança da informação, promovendo verificações mensais que mitiguem riscos e fortaleçam a cultura de proteção de dados no Brasil.
Escopo:	Abrange atividades de segurança da informação realizadas por servidores públicos e funcionários internos, incluindo manuseio de dados sensíveis, uso de dispositivos, comunicação segura, práticas de home office, prevenção contra ameaças digitais comuns no contexto brasileiro e conscientização para um futuro digital seguro.
Base normativa:	ISO/IEC 27001:2022, 27002:2022, 27005:2019, 27017:2015, 27701:2019, 27036:2013, 27018:2019, LGPD

Última atualização feita por Vagner Cordeiro: 20/04/2025

Princípios Fundamentais de Segurança da Informação


- Confidencialidade:** Um escudo invisível que garante que apenas os autorizados acessem o tesouro das informações sensíveis.
- Integridade:** A promessa de que os dados permanecerão puros e verdadeiros, imunes a mãos não autorizadas.
- Disponibilidade:** A certeza de que os sistemas estarão sempre ao alcance, prontos para servir quando o dever chamar.

Quadro de Conformidade LGPD: Pilares para um Futuro Seguro


Pilar	Descrição
Transparência	Garantir clareza no uso e tratamento de dados pessoais, promovendo confiança e ética.
Segurança	Implementar medidas técnicas robustas para proteger dados contra vazamentos e ataques.
Responsabilização	Demonstrar conformidade com a LGPD através de registros e auditorias, assegurando compromisso.

Instruções de Preenchimento


- ☒ Realizar a verificação no primeiro dia útil de cada mês, com diligência e atenção.
- ☒ Marcar com um [X] os itens verificados, selando a conformidade com responsabilidade.
- ☒ Reportar irregularidades ao setor de TI ou ao DPO imediatamente, protegendo o coletivo.
- ☒ Arquivar este documento para eventual auditoria ou conformidade legal, como um registro de compromisso.

#	Item de Verificação	Referência
 1. Documentos e Dados Sensíveis		
1.1	<input type="checkbox"/> Verificar ausência de documentos sensíveis em mesas de trabalho	ISO 27002:2022 (7.7); LGPD Art. 6
1.2	<input type="checkbox"/> Garantir armazenamento seguro de papéis sensíveis em gavetas trancadas	ISO 27002:2022 (7.3)
1.3	<input type="checkbox"/> Garantir destruição adequada de documentos físicos descartados (ex.: triturador)	ISO 27002:2022 (8.10); LGPD Art. 46
1.4	<input type="checkbox"/> Verificar ausência de documentos confidenciais em impressoras ou scanners	ISO 27002:2022 (5.12)
1.5	<input type="checkbox"/> Validar autorização antes de digitalizar documentos sensíveis	ISO 27701:2019 (6.10.2.1); LGPD Art. 46
1.6	<input type="checkbox"/> Confirmar que mídias removíveis não estão expostas em áreas de trabalho	ISO 27002:2022 (7.10)
1.7	<input type="checkbox"/> Conferir se documentos com dados pessoais estão devidamente rotulados	ISO 27002:2022 (5.13)
1.8	<input type="checkbox"/> Avaliar se não houve cópias indevidas de informações sensíveis	ISO 27002:2022 (5.34); LGPD Art. 46
1.9	<input type="checkbox"/> Garantir que documentos digitais estejam protegidos por senha ou criptografia	ISO 27002:2022 (8.24); LGPD Art. 46
1.10	<input type="checkbox"/> Verificar se documentos sensíveis estão armazenados em locais seguros (ex.: servidores autorizados)	ISO 27002:2022 (7.3)
1.11	<input type="checkbox"/> Evitar deixar documentos sensíveis em áreas comuns ou compartilhadas	ISO 27002:2022 (7.7)
1.12	<input type="checkbox"/> Garantir que documentos descartados sejam triturados ou incinerados	ISO 27002:2022 (8.10); LGPD Art. 46
1.13	<input type="checkbox"/> Verificar se pastas compartilhadas têm permissões de acesso restritas	ISO 27002:2022 (8.3)
1.14	<input type="checkbox"/> Garantir que documentos digitais sejam excluídos com segurança após uso (ex.: limpeza de lixeira)	ISO 27002:2022 (8.10); LGPD Art. 46
1.15	<input type="checkbox"/> Evitar impressão de documentos sensíveis sem necessidade justificada	ISO 27002:2022 (7.9); LGPD Art. 46
1.16	<input type="checkbox"/> Garantir que documentos sensíveis não sejam deixados em veículos ou locais externos	ISO 27002:2022 (7.7)
1.17	<input type="checkbox"/> Verificar se arquivos digitais sensíveis estão em pastas com controle de versão	ISO 27002:2022 (8.10)
1.18	<input type="checkbox"/> Evitar uso de impressoras compartilhadas para documentos sensíveis sem supervisão	ISO 27002:2022 (7.9)
1.19	<input type="checkbox"/> Garantir que documentos físicos sensíveis sejam transportados em envelopes lacrados	ISO 27002:2022 (5.14)
1.20	<input type="checkbox"/> Conferir se há backups regulares de documentos digitais sensíveis	ISO 27002:2022 (8.13)



#	Item de Verificação	Referência
 2. Segurança no Computador e Navegador		
2.1	<input type="checkbox"/> Bloquear computador ao se ausentar (Windows+L ou equivalente)	ISO 27002:2022 (7.7)
2.2	<input type="checkbox"/> Verificar navegador atualizado (ex.: Chrome, Firefox, Edge)	ISO 27002:2022 (8.8)
2.3	<input type="checkbox"/> Confirmar ausência de software instalado sem aprovação do TI	ISO 27002:2022 (5.10)
2.4	<input type="checkbox"/> Garantir não conexão de dispositivos pessoais ao computador corporativo	ISO 27002:2022 (7.10)
2.5	<input type="checkbox"/> Desativar cookies desnecessários no navegador	ISO 27701:2019 (6.10.2.2); LGPD Art. 46
2.6	<input type="checkbox"/> Verificar que senhas não estão salvas no navegador	ISO 27002:2022 (5.17)
2.7	<input type="checkbox"/> Confirmar antivírus ativo e atualizado em todos os dispositivos	ISO 27002:2022 (8.7)
2.8	<input type="checkbox"/> Garantir não uso de dispositivos pessoais para atividades corporativas	ISO 27002:2022 (8.1); LGPD Art. 46
2.9	<input type="checkbox"/> Limpar arquivos temporários do computador regularmente	ISO 27002:2022 (8.10)
2.10	<input type="checkbox"/> Verificar ausência de TI sombra (aplicativos não autorizados)	ISO 27002:2022 (5.23); LGPD Art. 46
2.11	<input type="checkbox"/> Garantir que o sistema operacional esteja atualizado com os últimos patches	ISO 27002:2022 (8.8)
2.12	<input type="checkbox"/> Evitar uso de navegadores desatualizados ou não suportados (ex.: Internet Explorer antigo)	ISO 27002:2022 (8.8)
2.13	<input type="checkbox"/> Verificar se extensões do navegador são confiáveis e autorizadas	ISO 27002:2022 (5.10)
2.14	<input type="checkbox"/> Garantir que o firewall do computador esteja ativo e configurado	ISO 27002:2022 (8.20)
2.15	<input type="checkbox"/> Evitar salvar arquivos corporativos em desktops ou locais não seguros	ISO 27002:2022 (8.10); LGPD Art. 46
2.16	<input type="checkbox"/> Garantir que atualizações de segurança sejam aplicadas em todos os aplicativos	ISO 27002:2022 (8.8)
2.17	<input type="checkbox"/> Evitar uso de sistemas operacionais não suportados (ex.: Windows XP)	ISO 27002:2022 (8.8)
2.18	<input type="checkbox"/> Verificar se há proteção contra ransomware ativa no antivírus	ISO 27002:2022 (8.7)
2.19	<input type="checkbox"/> Garantir que arquivos corporativos sejam salvos apenas em servidores seguros	ISO 27002:2022 (8.10); LGPD Art. 46
2.20	<input type="checkbox"/> Evitar uso de computadores compartilhados para acessar dados sensíveis	ISO 27002:2022 (7.7); LGPD Art. 46

#	Item de Verificação	Referência
 3. . E-mails e Comunicação Segura		
3.1	<input type="checkbox"/> Evitar abertura de e-mails ou links suspeitos	ISO 27002:2022 (6.8)
3.2	<input type="checkbox"/> Marcar e-mails sensíveis como confidenciais	ISO 27002:2022 (5.14)
3.3	<input type="checkbox"/> Garantir envio de dados pessoais apenas com criptografia (ex.: e-mails seguros)	ISO 27002:2022 (8.24)
3.4	<input type="checkbox"/> Evitar compartilhar dados pessoais via WhatsApp ou telefone sem validação	ISO 27002:2022 (5.34)
3.5	<input type="checkbox"/> Usar apenas e-mail oficial para comunicações corporativas	ISO 27002:2022 (5.10)
3.6	<input type="checkbox"/> Reportar e-mails de phishing ao setor de TI imediatamente	ISO 27002:2022 (6.8)
3.7	<input type="checkbox"/> Evitar responder a solicitações de dados pessoais não verificadas	ISO 27701:2019 (6.3.2.2)
3.8	<input type="checkbox"/> Verificar remetentes antes de abrir anexos em e-mails	ISO 27002:2022 (6.8)
3.9	<input type="checkbox"/> Garantir não uso de aplicativos de mensagens não autorizados para comunicações corporativas	ISO 27002:2022 (5.10)
3.10	<input type="checkbox"/> Evitar responder a mensagens solicitando pagamentos via Pix sem validação	ISO 27002:2022 (6.8)
3.11	<input type="checkbox"/> Garantir que e-mails com dados sensíveis sejam excluídos após uso	ISO 27002:2022 (8.10)
3.12	<input type="checkbox"/> Verificar se comunicações via videoconferência são seguras (ex.: Zoom, Teams)	ISO 27002:2022 (6.7)
3.13	<input type="checkbox"/> Evitar compartilhar tela com informações sensíveis em videoconferências	ISO 27002:2022 (5.14)
3.14	<input type="checkbox"/> Garantir que mensagens corporativas não sejam encaminhadas para terceiros	ISO 27002:2022 (5.14)
3.15	<input type="checkbox"/> Evitar uso de e-mails pessoais para comunicações relacionadas ao trabalho	ISO 27002:2022 (5.10)
3.16	<input type="checkbox"/> Garantir que videoconferências usem senhas e salas de espera	ISO 27002:2022 (6.7)
3.17	<input type="checkbox"/> Evitar envio de dados sensíveis em e-mails sem autenticação do destinatário	ISO 27002:2022 (5.14)
3.18	<input type="checkbox"/> Verificar se e-mails de trabalho não estão sendo sincronizados em dispositivos pessoais	ISO 27002:2022 (8.1); LGPD Art. 46
3.19	<input type="checkbox"/> Garantir que mensagens de texto (SMS) corporativas sejam criptografadas	ISO 27002:2022 (8.24)
3.20	<input type="checkbox"/> Evitar uso de plataformas de mensagens públicas para assuntos corporativos	ISO 27002:2022 (5.10); LGPD Art. 46

#	Item de Verificação	Referência
 4. Senhas e Acessos		
4.1	<input type="checkbox"/> Confirmar senha forte (mínimo 12 caracteres, com letras, números e símbolos)	ISO 27002:2022 (5.17)
4.2	<input type="checkbox"/> Garantir que senhas não foram compartilhadas com colegas ou terceiros	ISO 27002:2022 (6.3)
4.3	<input type="checkbox"/> Trocar senha se não alterada nos últimos 3 meses	ISO 27002:2022 (5.17)
4.4	<input type="checkbox"/> Acessar apenas sistemas autorizados para suas funções específicas	ISO 27002:2022 (8.3)
4.5	<input type="checkbox"/> Utilizar autenticação multifator (MFA) em todos os sistemas disponíveis	ISO 27002:2022 (8.5)
4.6	<input type="checkbox"/> Evitar uso de Wi-Fi público para acesso a sistemas corporativos	ISO 27017:2015 (5.1.1)
4.7	<input type="checkbox"/> Verificar ausência de senhas anotadas em locais visíveis (ex.: post-its)	ISO 27002:2022 (5.17)
4.8	<input type="checkbox"/> Reportar tentativas de login suspeitas ao setor de TI	ISO 27002:2022 (6.8)
4.9	<input type="checkbox"/> Garantir que senhas não sejam reutilizadas em diferentes sistemas	ISO 27002:2022 (5.17)
4.10	<input type="checkbox"/> Evitar salvar senhas em aplicativos ou documentos desprotegidos	ISO 27002:2022 (5.17)
4.11	<input type="checkbox"/> Verificar se contas inativas foram desativadas pelo setor de TI	ISO 27002:2022 (5.18)
4.12	<input type="checkbox"/> Garantir que sessões sejam encerradas ao final do expediente	ISO 27002:2022 (8.5)
4.13	<input type="checkbox"/> Evitar usar senhas padrão ou fáceis (ex.: "123456", "senha")	ISO 27002:2022 (5.17)
4.14	<input type="checkbox"/> Garantir que senhas sejam alteradas após suspeita de comprometimento	ISO 27002:2022 (5.17)
4.15	<input type="checkbox"/> Verificar se permissões de acesso foram revisadas pelo TI recentemente	ISO 27002:2022 (5.18)
4.16	<input type="checkbox"/> Garantir que senhas sejam alteradas após uso temporário (ex.: acesso emergencial)	ISO 27002:2022 (5.17)
4.17	<input type="checkbox"/> Evitar uso de senhas em dispositivos compartilhados sem logout	ISO 27002:2022 (8.5)
4.18	<input type="checkbox"/> Verificar se há políticas de expiração de sessão em sistemas corporativos	ISO 27002:2022 (8.5)
4.19	<input type="checkbox"/> Garantir que senhas não sejam enviadas por e-mail ou mensagens	ISO 27002:2022 (5.17)
4.20	<input type="checkbox"/> Evitar uso de senhas padrão fornecidas por fornecedores ou sistemas	ISO 27002:2022 (5.17)

#	Item de Verificação	Referência
 5. Conformidade LGPD e Prevenção		
5.1	<input type="checkbox"/> Garantir coleta de dados pessoais com consentimento explícito	ISO 27701:2019 (6.2.2.1); LGPD Art. 7
5.2	<input type="checkbox"/> Reportar solicitações de titulares (ex.: exclusão de dados) ao DPO	ISO 27701:2019 (6.3.2.2); LGPD Art. 18
5.3	<input type="checkbox"/> Evitar acesso a redes sociais no ambiente de trabalho	ISO 27002:2022 (5.10)
5.4	<input type="checkbox"/> Orientar colegas sobre boas práticas de proteção de dados	ISO 27002:2022 (6.3)
5.5	<input type="checkbox"/> Ler e seguir a política de segurança da organização	ISO 27002:2022 (5.1)
5.6	<input type="checkbox"/> Reportar incidentes (ex.: perda de dados) ao gestor ou TI	ISO 27002:2022 (6.8); LGPD Art. 48
5.7	<input type="checkbox"/> Evitar uso de serviços de nuvem pessoais para dados corporativos	ISO 27017:2015 (5.1.1); LGPD Art. 46
5.8	<input type="checkbox"/> Verificar proteção de dados em contratos com fornecedores	ISO 27036:2013 (4.2.2); LGPD Art. 39
5.9	<input type="checkbox"/> Garantir não uso de ferramentas não autorizadas no trabalho	ISO 27002:2022 (5.23); LGPD Art. 46
5.10	<input type="checkbox"/> Confirmar participação no último treinamento de segurança	ISO 27002:2022 (6.3)
5.11	<input type="checkbox"/> Garantir que dados pessoais coletados sejam mínimos (princípio da necessidade)	ISO 27701:2019 (6.2.2.1); LGPD Art. 6
5.12	<input type="checkbox"/> Verificar se há registros de acessos a dados sensíveis (logs)	ISO 27002:2022 (8.15); LGPD Art. 48
5.13	<input type="checkbox"/> Evitar compartilhar dados pessoais em grupos de mensagens	ISO 27002:2022 (5.14); LGPD Art. 46
5.14	<input type="checkbox"/> Garantir que backups de dados sensíveis sejam armazenados com segurança	ISO 27002:2022 (8.13); LGPD Art. 46
5.15	<input type="checkbox"/> Reportar qualquer acesso não autorizado a dados pessoais ao DPO	ISO 27002:2022 (6.8); LGPD Art. 48
5.16	<input type="checkbox"/> Garantir que dados pessoais sejam tratados apenas para finalidades específicas	LGPD Art. 6
5.17	<input type="checkbox"/> Verificar se há plano de resposta a incidentes de segurança ativo	ISO 27002:2022 (6.8); LGPD Art. 48
5.18	<input type="checkbox"/> Evitar armazenamento de dados pessoais além do prazo necessário	LGPD Art. 16
5.19	<input type="checkbox"/> Garantir que dados pessoais não sejam usados para fins discriminatórios	LGPD Art. 6
5.20	<input type="checkbox"/> Verificar se há políticas de retenção e descarte de dados implementadas	ISO 27002:2022 (8.10); LGPD Art. 46

#	Item de Verificação	Referência
 6. Proteção contra Ameaças e Práticas de Home Office		
6.1	<input type="checkbox"/> Evitar responder a mensagens de redes sociais que solicitem dados pessoais	ISO 27002:2022 (6.8)
6.2	<input type="checkbox"/> Reportar mensagens suspeitas de golpes via Pix ao setor de TI	ISO 27002:2022 (6.8)
6.3	<input type="checkbox"/> Garantir uso de VPN em conexões remotas (ex.: home office)	ISO 27002:2022 (6.7)
6.4	<input type="checkbox"/> Evitar uso de dispositivos pessoais não autorizados em home office	ISO 27002:2022 (6.7); LGPD Art. 46
6.5	<input type="checkbox"/> Verificar segurança de impressoras e scanners usados em home office	ISO 27002:2022 (7.9)
6.6	<input type="checkbox"/> Garantir que reuniões virtuais não sejam gravadas sem autorização	ISO 27002:2022 (5.14); LGPD Art. 46
6.7	<input type="checkbox"/> Evitar compartilhar tela com informações sensíveis em videoconferências	ISO 27002:2022 (5.14)
6.8	<input type="checkbox"/> Garantir que dispositivos usados em casa tenham antivírus ativo	ISO 27002:2022 (8.7)
6.9	<input type="checkbox"/> Evitar abrir links ou QR Codes suspeitos em mensagens pessoais	ISO 27002:2022 (6.8)
6.10	<input type="checkbox"/> Reportar qualquer incidente de segurança ocorrido em home office	ISO 27002:2022 (6.8); LGPD Art. 48
6.11	<input type="checkbox"/> Garantir que impressoras domésticas não armazenem dados sensíveis	ISO 27002:2022 (7.9)
6.12	<input type="checkbox"/> Evitar uso de redes Wi-Fi abertas ou públicas em deslocamentos	ISO 27017:2015 (5.1.1); LGPD Art. 46
6.13	<input type="checkbox"/> Garantir que dispositivos pessoais usados em casa estejam protegidos por senha	ISO 27002:2022 (8.1); LGPD Art. 46
6.14	<input type="checkbox"/> Evitar deixar dispositivos desbloqueados em casa durante o trabalho remoto	ISO 27002:2022 (6.7)
6.15	<input type="checkbox"/> Verificar se o roteador doméstico tem senha forte e criptografia WPA3	ISO 27002:2022 (8.20)
6.16	<input type="checkbox"/> Garantir que dispositivos usados em casa não sejam compartilhados com terceiros	ISO 27002:2022 (8.1); LGPD Art. 46
6.17	<input type="checkbox"/> Evitar uso de dispositivos corporativos em redes domésticas não seguras	ISO 27002:2022 (6.7); LGPD Art. 46
6.18	<input type="checkbox"/> Verificar se há atualizações de segurança no roteador doméstico	ISO 27002:2022 (8.20)
6.19	<input type="checkbox"/> Garantir que documentos impressos em casa sejam armazenados com segurança	ISO 27002:2022 (7.9); LGPD Art. 46
6.20	<input type="checkbox"/> Evitar uso de aplicativos de videoconferência não autorizados	ISO 27002:2022 (5.10); LGPD Art. 46

#	Item de Verificação	Referência
 7. Conscientização e Boas Práticas		
7.1	<input type="checkbox"/> Evitar clicar em links de promoções ou descontos suspeitos	ISO 27002:2022 (6.8)
7.2	<input type="checkbox"/> Reportar mensagens de engenharia social (ex.: falsas promoções) ao TI	ISO 27002:2022 (6.8)
7.3	<input type="checkbox"/> Garantir que dispositivos móveis usados no trabalho tenham bloqueio de tela	ISO 27002:2022 (8.1); LGPD Art. 46
7.4	<input type="checkbox"/> Evitar uso de aplicativos de mensagens para enviar dados sensíveis	ISO 27002:2022 (5.14); LGPD Art. 46
7.5	<input type="checkbox"/> Verificar se backups corporativos são feitos regularmente pelo TI	ISO 27002:2022 (8.13)
7.6	<input type="checkbox"/> Garantir que dispositivos pessoais não sejam usados em redes corporativas	ISO 27002:2022 (8.1); LGPD Art. 46
7.7	<input type="checkbox"/> Evitar baixar aplicativos não confiáveis em dispositivos corporativos	ISO 27002:2022 (5.10)
7.8	<input type="checkbox"/> Participar de treinamentos de segurança da informação sempre que oferecidos	ISO 27002:2022 (6.3)
7.9	<input type="checkbox"/> Garantir que dados pessoais tratados sejam anonimizados quando possível	ISO 27701:2019 (6.11); LGPD Art. 13
7.10	<input type="checkbox"/> Evitar uso de dispositivos USB pessoais para transferir dados corporativos	ISO 27002:2022 (7.10); LGPD Art. 46
7.11	<input type="checkbox"/> Verificar se há atualizações de segurança em aplicativos corporativos	ISO 27002:2022 (8.8)
7.12	<input type="checkbox"/> Garantir que informações sensíveis não sejam exibidas em monitores visíveis	ISO 27002:2022 (7.7)
7.13	<input type="checkbox"/> Evitar discutir informações sensíveis em locais públicos (ex.: cafés)	ISO 27002:2022 (6.8)
7.14	<input type="checkbox"/> Garantir que dispositivos corporativos não sejam usados por terceiros	ISO 27002:2022 (8.1); LGPD Art. 46
7.15	<input type="checkbox"/> Reportar qualquer comportamento suspeito de colegas ao gestor ou TI	ISO 27002:2022 (6.8)
 8. Gestão de Incidentes e Resposta		
8.1	<input type="checkbox"/> Garantir que incidentes de segurança sejam documentados detalhadamente	ISO 27002:2022 (6.8); LGPD Art. 48
8.2	<input type="checkbox"/> Verificar se há um plano de resposta a incidentes ativo e atualizado	ISO 27002:2022 (6.8)
8.3	<input type="checkbox"/> Evitar divulgar detalhes de incidentes de segurança a terceiros não autorizados	ISO 27002:2022 (5.14); LGPD Art. 48
8.4	<input type="checkbox"/> Garantir que incidentes de vazamento de dados sejam reportados em até 72 horas	LGPD Art. 48
8.5	<input type="checkbox"/> Verificar se há backups recentes para recuperação após incidentes	ISO 27002:2022 (8.13)
8.6	<input type="checkbox"/> Evitar uso de dispositivos comprometidos até avaliação pelo TI	ISO 27002:2022 (6.8)
8.7	<input type="checkbox"/> Garantir que incidentes sejam analisados para prevenir reincidências	ISO 27002:2022 (6.8)
8.8	<input type="checkbox"/> Verificar se há um canal oficial para reportar incidentes de segurança	ISO 27002:2022 (6.8)
8.9	<input type="checkbox"/> Evitar compartilhar informações de incidentes em redes sociais	ISO 27002:2022 (5.14)
8.10	<input type="checkbox"/> Garantir que medidas corretivas sejam implementadas após incidentes	ISO 27002:2022 (6.8)