POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão 1.0

Data: 28/05/2026

Classificação: Público

HISTÓRICO DE ELABORAÇÃO:

Versão	Elaborador	Notas	Data
1.0	Comitê de segurança da Informação	Elaboração do Documento	12/05/2026

HISTÓRICO DE REVISÃO E APROVAÇÃO:

Versão	Data	Revisor	Aprovador	Status
1.0	28/05/26	Comitê da Direção	Diretor-Presidente	

Aprovado

1. INTRODUÇÃO

A presente Política de Segurança da Informação os princípios, diretrizes, responsabilidades e normas para o tratamento adequado das informações no âmbito da Lottopar, abrangendo a proteção de seus ativos de informação, a disseminação da cultura de segurança entre colaboradores e terceiros, a proteção dos sistemas e a garantia da confidencialidade, integridade e disponibilidade das informações.

Esta política visa, ainda, assegurar a continuidade dos negócios e a conformidade com leis, regulamentos e normas aplicáveis a Administração Pública, bem como mitigar riscos que possam resultar em perdas, prejuízos ou danos de natureza financeira, operacional, legal ou reputacional.

Esta política constitui uma declaração formal do compromisso da organização com a proteção das informações sensíveis, alinhando os princípios de Segurança da Informação e Segurança Cibernética às estratégias de negócio e à governança corporativa.

Esta política e os procedimentos que suportam sua implementação integram o Sistema de Gestão de Segurança da Informação (SGSI) da Lottopar devem ser observados em conjunto com as demais políticas corporativas

Esta Política e os procedimentos que suportam sua implementação integram o Sistema de Gestão de Segurança da Informação – SGSI da LOTTOPAR e devem ser observadas conjuntamente com normas, procedimentos, resoluções e regulamentos internos correlatos.

2. ESCOPO

Esta Política se aplica a todos os servidores públicos, empregados públicos, colaboradores, terceirizados, operadores lotéricos credenciados, integradores, fornecedores, parceiros, prestadores de serviço, consultores, terceiros que possuam acesso às informações, ambientes, sistemas ou infraestrutura da Lottopar.

Aplica-se ainda às informações em meio físico, digital, verbal, audiovisual ou eletrônico, aos ambientes *on-premises*, cloud, híbridos e remotos, aos sistemas corporativos, regulatórios e lotéricos, aos ativos tecnológicos e operacionais e a todo o ciclo de vida da informação.

3. TERMOS E DEFINIÇÕES

Alta Direção: Grupo de executivos com autoridade para definir estratégias, prover recursos e tomar decisões sobre o direcionamento da organização, incluindo a aprovação de políticas, aceitação de riscos e patrocínio do Sistema de Gestão de Segurança da Informação.

Confidencialidade: Garantia de que somente pessoas autorizadas terão acessos às informações e apenas quando houver necessidade.

Integridade: Garantia de que as informações permanecerão exatas e completas e não serão modificadas indevidamente.

Disponibilidade: Garantia de que a informação estará disponível às pessoas autorizadas sempre que for necessário.

Privacidade e Proteção de Dados Pessoais: Fundamento de que os dados pessoais contidos nas informações devem ser protegidos com a adoção de medidas técnicas e organizacionais de Segurança da Informação, nos termos impostos pela Lei nº 13.709/2018, conhecia por LGPD ou Lei Geral de Proteção de Dados.

Ciclo de Vida da Informação: Processo contínuo que abrange criação, processamento, armazenamento, transmissão, arquivamento e destruição final.

Ativo de Informação: Qualquer elemento que possua valor para a organização, incluindo dados, documentos, software, hardware, serviços, pessoas e reputação.

Ambiente Crítico: Ambiente tecnológico cuja indisponibilidade, comprometimento ou manipulação possa afetar operações lotéricas, arrecadação, integridade de apostas, fiscalização, continuidade regulatória e/ou reputação institucional.

Incidente de Segurança da Informação: Evento confirmado ou suspeito que comprometa a confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade das informações.

Operador Lotérico Credenciado: Pessoa jurídica autorizada pela Lottopar a operar modalidades lotéricas regulamentadas.

4. *DOCUMENTOS RELACIONADOS*

POL-SGSI-002 Política de Gestão de Riscos

POL-SGSI-003 Política de Gestão de Identidade e Acesso

POL-SGSI-004 Política de Segurança Física e Ambiental

POL-SGSI-005 Política de Classificação, Rotulagem, Tratamento e Transferência de Informação

POL-SGSI-006 Política de Gestão de Ativos

POL-SGSI-007 Política de Uso Aceitável

POL-SGSI-008 Política de Trabalho Remoto

POL-SGSI-009 Política de Hardening

POL-SGSI-010 Política de Gestão de Vulnerabilidades

POL-SGSI-011 Política de Gestão de Mudanças

POL-SGSI-012 Política de Monitoramento de Ativos

POL-SGSI-013 Política de Backup

POL-SGSI-014 Política de Criptografia e Gestão de Chaves Criptográficas

POL-SGSI-015 Política de Segurança em Recursos Humanos

POL-SGSI-016 Política de Segurança no Relacionamento com Fornecedores

OBJETIVOS DE SEGURANÇA DA INFORMAÇÃO

Todas as informações gerenciadas pela organização, em qualquer formato (escrito, falado, gravado eletronicamente ou impresso), são protegidas contra modificação, destruição ou divulgação não autorizada, seja acidental ou intencional, durante todo o seu ciclo de vida. O objetivo final da Segurança da Informação é assegurar que informações, dados e sistemas de TI sigam os princípios de:

- **Confidencialidade:** Garantir que as informações sejam acessadas apenas por pessoas autorizadas.

- **Integridade:** Assegurar que os dados sejam precisos e completos, protegendo-os contra alterações não autorizadas.
- **Disponibilidade:** Garantir que as informações estejam acessíveis sempre que necessário, sem interrupções.
- **Conformidade:** Cumprir rigorosamente as leis e regulamentações aplicáveis, como a LGPD.
- **Responsabilidade Compartilhada:** Envolver todos os colaboradores e parceiros na proteção das informações.
- **Cultura de Segurança:** Promover a conscientização e o treinamento contínuo para fortalecer a postura de segurança em todos os níveis da organização.

Os objetivos de Segurança da Informação, alinhados ao Sistema de Gestão de Segurança da Informação (SGSI), são:

I. Estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

II. Estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

III. Estabelecer competências e responsabilidades quanto à segurança da informação;

IV. Nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;

V. Promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional da Lottopar.

CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

A organização classifica as informações com base no impacto potencial decorrente de acesso, uso, divulgação, alteração ou destruição, seguindo critérios legais, regulatórios, contratuais e de negócio.

A classificação é aplicada durante todo o ciclo de vida da informação, compreendendo criação, armazenamento, processamento, transmissão, arquivamento e descarte, de modo a definir os controles de proteção apropriados.

SEGURANÇA DE REDE

Os ativos de rede e computação, incluindo *firewalls*, roteadores, *switches* e *access points*, possuem controles formais de restrição de acesso para usuários e administradores, bem como mecanismos de segmentação de rede e controle de tráfego. Esses controles suportam o isolamento lógico entre ambientes, sistemas e conjuntos de dados, com o objetivo de reduzir o risco de acesso não autorizado, movimentação lateral e exposição de informações.

HARDENING

Os ativos de tecnologia da informação, incluindo servidores, estações de trabalho, dispositivos de rede, sistemas operacionais, aplicações e serviços, mantêm configurações de acordo com padrões de *hardening* definidos pela organização, com o objetivo de reduzir a superfície de ataque e minimizar vulnerabilidades.

As configurações de *hardening* incluem, quando aplicável:

- Remoção ou desativação de serviços, portas, protocolos e contas desnecessárias;
- Aplicação de políticas de configuração segura (baseline de segurança);
- Restrições de acesso administrativo e uso de autenticação forte;
- Configuração de logs e monitoramento de eventos de segurança;
- Aplicação tempestiva de patches e atualizações de segurança;

TESTE DE SEGURANÇA

A Lottopar realiza testes de segurança periódicos nos ativos de informação, sistemas, aplicações e infraestrutura de rede, com o objetivo de identificar vulnerabilidades, falhas de configuração e exposições a riscos de segurança.

- Os testes de segurança incluem, quando aplicável:
- Varreduras de vulnerabilidades (*vulnerability scanning*) internas e externas;
- Testes de intrusão (*pentest*) em aplicações, redes e infraestrutura;
- Revisões de configuração e *hardening* de sistemas e dispositivos de rede;
- Testes de controles de segurança, incluindo autenticação, autorização e segregação de ambientes.

CONTROLES DE SEGURANÇA

A Lottopar possui mecanismos de proteção contra malware em todos os ativos de tecnologia da informação, incluindo servidores, estações de trabalho e dispositivos portáteis, com o objetivo de prevenir, detectar e responder a ameaças maliciosas.

Adicionalmente, a Lottopar mantém mecanismos de monitoramento e registro de eventos de segurança, incluindo logs de sistemas, aplicações, dispositivos de rede e soluções de segurança, para detecção de incidentes e suporte à investigação forense.

RELACIONAMENTO COM TERCEIROS

A Lottopar estabelece controles de Segurança da Informação para terceiros que tenham acesso a informações, sistemas ou infraestrutura, incluindo requisitos contratuais de confidencialidade, proteção de dados e conformidade regulatória.

Os terceiros são avaliados quanto a riscos de segurança, e seus acessos são concedidos, monitorados e revogados conforme a necessidade e o término do relacionamento contratual.

GESTÃO DE RISCOS

A Lottopar mantém um processo estruturado e contínuo de gestão de riscos de Segurança da Informação, incluindo a identificação de ativos, ameaças, vulnerabilidades e impactos potenciais aos negócios.

Os riscos são avaliados de acordo com critérios definidos de probabilidade e impacto, e tratados por meio de ações de mitigação, transferência, aceitação ou eliminação do risco. A aceitação de riscos residuais foi formalmente aprovada pela gestão responsável.

O processo de gestão de riscos é revisado periodicamente e sempre que ocorrerem mudanças significativas no ambiente de tecnologia, processos ou requisitos regulatórios.

GESTÃO DE VULNERABILIDADES

A organização estabelece e mantém um processo contínuo de gestão de vulnerabilidades em sistemas, aplicações, redes, dispositivos e infraestrutura, incluindo ambientes *on-premises*, *cloud* e *endpoints*. Esse processo abrange a identificação, análise, classificação, priorização e tratamento de vulnerabilidades técnicas e de configuração.

As vulnerabilidades são identificadas por meio de varreduras automatizadas, testes de segurança, avaliações técnicas, boletins de fabricantes e fontes de inteligência de ameaças. A priorização considera o nível de risco ao negócio, levando em conta criticidade do ativo, exposição, impacto potencial e probabilidade de exploração.

O tratamento das vulnerabilidades inclui a aplicação de correções, atualizações, *hardening*, segmentação, desativação de serviços desnecessários e/ou implementação de controles compensatórios quando a correção imediata não for possível. As ações são documentadas, rastreadas e revisadas periodicamente. Vulnerabilidades críticas são tratadas dentro de prazos definidos pela organização, com acompanhamento e reporte à gestão.

GESTÃO DE CONTINUIDADE

A Lottopar mantém um programa de gestão de continuidade de negócios e recuperação de desastres, com o objetivo de minimizar o impacto de incidentes que afetem a disponibilidade de informações, sistemas, processos críticos e serviços essenciais.

A organização define planos formais de Continuidade de Negócios (BCP) e Recuperação de Desastres (DRP), incluindo responsabilidades, procedimentos de resposta, estratégias de recuperação, níveis mínimos de serviço, objetivos de tempo de recuperação (RTO) e pontos de recuperação de dados (RPO).

A organização testa os planos periodicamente por meio de simulações, exercícios técnicos ou testes completos, e os revisa sempre que ocorrem mudanças significativas no ambiente tecnológico, processos de negócio ou requisitos regulatórios. A organização documenta os resultados dos testes e os utiliza para a melhoria contínua da capacidade de resiliência.

GESTÃO DE INCIDENTES DE SEGURANÇA

A organização estabelece e mantém um processo formal de gestão de incidentes de Segurança da Informação, abrangendo a identificação, registro, classificação, resposta, contenção, erradicação, recuperação e análise pós-incidente.

Todos os colaboradores, terceiros e partes interessadas reportam imediatamente qualquer evento suspeito ou incidente confirmado por meio dos canais de comunicação.

Os incidentes são tratados por equipes designadas, com preservação de evidências para fins de investigação, auditoria e atendimento a requisitos legais e regulatórios. As lições aprendidas devem ser documentadas e utilizadas para aprimorar controles, processos e políticas de segurança.

GESTÃO DE PESSOAS

A organização aplica controles de Segurança da Informação durante todo o ciclo de vida dos colaboradores e terceiros, incluindo processos de contratação, movimentação interna e desligamento.

A organização realiza verificações de antecedentes conforme aplicável, assinatura de termos

de confidencialidade e responsabilidade, e definição clara de obrigações relacionadas à proteção da informação.

Os colaboradores recebem treinamento inicial e recorrente em Segurança da Informação, privacidade e conformidade regulatória. No desligamento ou mudança de função, os acessos são revogados e os ativos devolvidos conforme procedimentos formais.

GESTÃO DE ACESSOS

A organização aplica controles de Segurança da Informação durante todo o ciclo de vida dos colaboradores e terceiros, incluindo processos de contratação, movimentação interna e desligamento.

São realizadas verificações de antecedentes conforme aplicável, assinatura de termos de confidencialidade e responsabilidade, e definição clara de obrigações relacionadas à proteção da informação.

Os colaboradores recebem treinamento inicial e recorrente em Segurança da Informação, privacidade e conformidade regulatória. No desligamento ou mudança de função, os acessos são revogados e os ativos devolvidos conforme procedimentos formais.

GESTÃO E UTILIZAÇÃO DE ATIVOS E INFORMAÇÕES

Os ativos de informação e tecnologia são utilizados exclusivamente para fins profissionais e de acordo com as políticas e procedimentos internos.

Os usuários são responsáveis pela proteção das informações sob sua custódia, incluindo dados confidenciais, pessoais e regulados. É proibida a divulgação não autorizada de informações, bem como o uso indevido de ativos corporativos.

A Lottopar mantém políticas de uso aceitável, mesa limpa, tela limpa e proteção de dispositivos, incluindo criptografia e controle de mídia removível.

MONITORAMENTO E REGISTRO DE EVENTOS

A organização possui mecanismos de monitoramento contínuo de eventos de segurança em sistemas, redes, aplicações e dispositivos, incluindo a coleta, centralização, retenção e análise de logs.

Os registros são protegidos contra alteração e exclusão não autorizadas, e mantidos conforme requisitos legais, regulatórios e contratuais.

O monitoramento permite a detecção de atividades suspeitas, acessos não autorizados, falhas de controle e incidentes de segurança, com capacidade de resposta oportuna.

MEDIDAS DISCIPLINARES

O descumprimento das políticas, normas e procedimentos de Segurança da Informação pode resultar na aplicação de medidas disciplinares, administrativas, contratuais ou legais, conforme a gravidade da violação e a legislação aplicável.

As sanções seguem os procedimentos internos da Administração Pública e legislação pertinente, podendo incluir advertências, suspensão, exoneração e/ou outras medidas cabíveis.

A organização reserva-se o direito de adotar ações legais em caso de violações que resultem em danos, exposição de informações ou não conformidade regulatória.

5. REVISÃO E CONFORMIDADE

A organização revisa periodicamente suas políticas, normas, procedimentos e controles de Segurança da Informação para assegurar sua adequação, eficácia e alinhamento com requisitos legais, regulatórios, contratuais e melhores práticas do mercado. As revisões ocorrem, no mínimo, de forma anual ou sempre que houver mudanças significativas no ambiente tecnológico, processos de negócio, estrutura organizacional ou requisitos de conformidade.

A organização monitora a conformidade com esta política meio de auditorias internas, avaliações de terceira parte, revisões de gestão e indicadores de desempenho. A organização registra não conformidades identificadas, trata cada uma delas por meio de planos de ação e as acompanha até sua resolução. A alta direção recebe informações sobre o status de conformidade e riscos relevantes, de modo a suportar a tomada de decisão.

6. DISPOSIÇÕES FINAIS

Os casos omissos serão deliberados pela Alta Administração, com apoio do Comitê de Segurança da Informação e das áreas técnicas competentes.

Esta Política entra em vigor na data de sua aprovação formal pela autoridade competente da LOTTOPAR.