INFOAGRO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão 1.0 – Publicada pela PESAGRO-RIO
Última atualização: 11/12/2025

VISÃO GERAL

O QUÊ?
Conjunto de normas, processos e tecnologias para proteger informações contra acesso, alteração ou destruição não autorizada.

POR QUÊ?
Cumprir lei (LGPD), proteger pesquisadores, evitar fraudes, manter reputação, garantir operações contínuas.

QUEM?
Todos: servidores, pesquisadores, fornecedores. Responsabilidade coletiva.

QUEM DECIDE? – ESTRUTURA DE GOVERNANÇA

Segurança não é responsabilidade de uma pessoa. É estrutura com papéis claros.

Diretor
Responsabilidade principal: aprova política, aloca orçamento, decisões estratégicas
Reporta ao: Presidente

CISO
Responsabilidade principal: Coordena implementação, responde incidentes, avalia riscos
Reporta ao: Diretor

Gestor TI
Responsabilidade principal: Implementa controles técnicos, mantém infraestrutura
Reporta ao: CISO

DPO

Responsabilidade principal: Garante conformidade LGPD, privacidade de dados

Reporta ao: CISO

Comitê

Responsabilidade principal: Delibera sobre riscos, aprova planos, supervisiona

Reporta ao: Diretor

2. CLASSIFICAÇÃO DE INFORMAÇÕES

Informações diferentes = proteções diferentes. Use escala abaixo:

NÍVEL	EXEMPLOS	RISCOS DE VAZAR	CONTROLES MÍNIMOS
PÚBLICA	Boletins, eventos, editais	Nenhum	Publicar em sites
INTERNA	Procedimentos, cronogramas	Baixo	Autenticação
CONFIDENCIAL	Propriedade intelectual, contratos	Alto	MFA + Crptografia
SIGILOSO	Dados sensíveis pessoais	Crítico	Máxima proteção

3. O QUE FAZER SE DESCOBRIR UM INCIDENTE?

Resposta rápida é crítica. Siga 6 fases:

1. DETECTAR

- **30 min**
- Comportamento suspeito?
- Alertas dispararam?Vazamento descoberto?
-

2. RELATAR

1 hora

Email: security-incident@pesagro-rio.gov.br

Telefone: [número]

Nunca ignore!

3. INVESTIGAR

<24h

- CISO ativa equipe
- Analisa: O quê? Como? Quando?
- Coleta evidências

4. COMUNICAR

3 dias úteis

- Se vazou dados: notifique ANPD
- Transparência obrigatória

5. REMEDIAR

Dias/Semanas

- Feche vulnerabilidade
- Recupere sistemas

6. APRENDER

Pós-incidente

- Reunião de lições aprendidas
- Evite repetição

4. CONTROLE DE ACESSO

Regra: Ninguém acessa nada por padrão.

Acesso liberado APENAS se:

- TEM NECESSIDADE OPERACIONAL
  Função requer acesso | Justificativa documentada
- TEM AUTORIZAÇÃO FORMAL
  Gerente aprovou por escrito | Doc em arquivo
- AUTENTICAÇÃO FORTE
  Senha 12+ caracteres | MFA para dados críticos
- RASTREADO COMPLETAMENTE
  Logs de acesso | Quem, quê, quando, onde

Não faça: usar senha de colega, acessar dados sem necessidade, negligenciar logout.

5. CRIPTOGRAFIA

Criptografia = matemática que torna dados ilegíveis sem chave. Como um cofre

Cenário: Dados em repouso (armazenamento)
O que fazer:

- AES-256: padrão obrigatório
- Dados confidenciais SEMPRE criptografados
- Chaves em cofre seguro

Cenário: Dados em trânsito (pela rede)
O que fazer:

- TLS 1.2+: criptografia de canal
- HTTPS (não HTTP)
- VPN para acesso remoto

6. TREINAMENTO OBRIGATÓRIO

Tecnologia protege sistemas. Pessoas precisam ser educadas.

Ingresso (02 horas)
O que aprender: visão geral, classificação, senhas, phishing, reportar incidentes

Anual (01 hora)
O que aprender: reciclagem obrigatória, ameaças novas, boas práticas

Por função
O que aprender: Pesquisadores: dados pessoais | TI: acesso | Gestores: responsabilidades

Phishing (trimestral)
O que aprender: Simulação realista. Objetivo: educar, não punir

7. COMO MEDIMOS SUCESSO?

Segurança não é "fazer e esquecer". Medimos progresso:

DISPONIBILIDADE

- > 99.5% uptime | Max 3.6h downtime/mês
- Monitorado continuamente

PATCHES

- 100% patches críticas em 7 dias | Zero vulnerabilidades abertas
- Relatório mensal

TREINAMENTO

- > 95% colaboradores atualizados | Redução phishing
- Auditado semestral

INCIDENTES

- Redução contínua de erros | Resposta <30 min (críticos)
- Tempo real

8. ERROS COMUNS – O QUE NÃO FAZER

— Mesma senha para múltiplos sistemas
Se uma vazar, todas estarão comprometidas

— Compartilhar senha com colega
Você fica responsável pelas ações dele

— Deixar computador desbloqueado
Qualquer um pode acessar seus dados

— Escrever senha em papel visível
Qualquer um vê passando por perto

- Clicar em link de email suspeito
  Pode instalar malware ou roubar credenciais

- Enviar dados confidenciais por email comum
  Email não é criptografado

- Ignorar avisos de segurança
  Avisos existem para alertar sobre riscos reais

- Não reportar incidente suspeito
  Atraso piora o dano

9. CONTATOS DE EMERGÊNCIA

INCIDENTE CRÍTICO

Segurança em risco AGORA
Email: security-incident@pesagro-rio.gov.br
Telefone 24/7:
Chat emergência:

DÚVIDAS SOBRE SEGURANÇA

Política, controles, acesso
Email: ciso@pesagro-rio.gov.br
Horário: 09h-17h seg-sex

CONFORMIDADE LGPD

Privacidade, direitos de titulares
Email: dpo@pesagro-rio.gov.br
Tempo resposta: <10 dias

10. O QUE ACONTECE SE EU VIOLAR A POLÍTICA?

Segurança é levada a sério. Violações têm consequências proporcionadas:

TIPO	EXEMPLOS	SANÇÃO
LEVE (negligência)	Senha em papel, email errado, atraso treinamento	Advertência formal + retraining
MODERADA (risco)	Compartilhar credenciais, dados confidenciais sem criptografia	Suspensão 3-10 dias
GRAVE (dano real)	Vazar dados intencionalmente, r oubar, criar backdoor	Demissão com justa causa + ação criminal

CHECKLIST FINAL – VOCÊ ENTENDEU?

- Conheço as 4 níveis de classificação (Pública, Interna, Confidencial, Sigiloso).
- Sei que MFA (código + senha) é obrigatório para dados críticos.
- Entendo que criptografia protege dados em repouso e TLS protege em trânsito.
- Conheço o fluxo de resposta a incidente (6 fases).
- Nunca compartilharei senha, mesmo com colega de confiança.
- Treinamento é obrigatório (ingresso 2h + anual 1h).
- Conheço os contatos para reportar incidente.
- Violação grave = demissão + ação criminal.
- LGPD protege dados pessoais e ANPD fiscaliza.
- Vou reportar incidentes imediatamente.

Se marcou tudo = Você está pronto para trabalhar com segurança!

DPO (Data Protection Officer | Encarregado de Proteção de Dados)
Marcelo Andrade Penido
marcelo.penido@pesagro.rj.gov.br
Alameda São Boaventura, 770 – Fonseca – CEP 24120-191 – Niterói – RJ
(22) 2771-1515