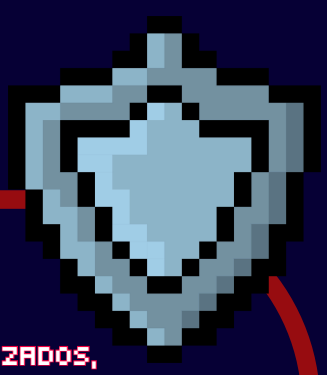
RESUMO DAS POLÍTICAS



POL-SI-0001 — POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
OBJETIVO:
PROTEGER AS INFORMAÇÕES DA EMPRESA CONTRA ACESSOS NÃO AUTORIZADOS, ALTERAÇÕES INDEVIDAS, PERDAS E INDISPONIBILIDADE.
PRINCÍPIOS FUNDAMENTAIS:

CONFIDENCIALIDADE: SÓ PESSOAS AUTORIZADAS ACESSAM A INFORMAÇÃO.

INTEGRIDADE: A INFORMAÇÃO DEVE PERMANECER ÍNTEGRA E CONFIÁVEL.

DISPONIBILIDADE: A INFORMAÇÃO PRECISA ESTAR ACESSÍVEL QUANDO NECESSÁRIO.

RESPONSABILIDADES DOS COLABORADORES:

PROTEGER SENHAS E CREDENCIAIS.

NÃO COMPARTILHAR INFORMAÇÕES SENSÍVEIS SEM AUTORIZAÇÃO.

REPORTAR QUALQUER ATIVIDADE SUSPEITA OU INCIDENTE.

POL-SI-0003 — POLÍTICA DE SEGURANÇA DE ENDPOINT
OBJETIVO:
GARANTIR QUE TODOS OS DISPOSITIVOS (NOTEBOOKS, DESKTOPS, CELULARES CORPORATIVOS, ETC.) ESTEJAM SEGUROS CONTRA AMEAÇAS CIBERNÉTICAS.

REGRAS E BOAS PRÁTICAS:

TODOS OS ENDPOINTS DEVEM ESTAR COM SISTEMA OPERACIONAL E ANTIVÍRUS ATUALIZADOS.

É PROIBIDA A INSTALAÇÃO DE SOFTWARES NÃO AUTORIZADOS.

OS DISPOSITIVOS DEVEM ESTAR PROTEGIDOS POR SENHA FORTE

POP-SI-0002 — PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA
OBJETIVO:
DEFINIR COMO A EMPRESA DEVE IDENTIFICAR, TRATAR E REGISTRAR INCIDENTES DE SEGURANÇA DA INFORMAÇÃO.

FASES DO PROCESSO:

IDENTIFICAÇÃO: PERCEBER COMPORTAMENTOS ANÔMALOS (EX: E-MAIL SUSPEITO, ACESSO FORA DO HORÁRIO).

REGRAS E BOAS PRÁTICAS:
ACIONAR A SUPERVISÃO DE FORMA IMEDIATA

INORPEL
cybersecurity