



**PREFEITURA MUNICIPAL DE SÃO DOMINGOS DO NORTE**  
**CONTROLADORIA GERAL**  
**CNPJ 36.350.312/0001-72**

**Of. n.º 014/2021 - SEMCONT**

São Domingos do Norte/ES, 05 de maio de 2021.

**Da: Controladoria Geral do Município de São Domingos do Norte/ES.**

*Gilsandra Iara Marino*

**Ao Setor Comercial da E&L**

Prezados Senhores

Em virtude que todos os dados e Sistemas foram apagados do computador desta Controladoria, após ser infectado por vírus e um desligamento súbito, verificado por técnico de informática contratado, que emitiu um laudo, onde perdi tudo que havia inclusive os sistemas instalados da E&L Web e Desktop do controle interno, Sistema de Contabilidade e Sistema de protocolo. Solicito os bons préstimos, no sentido de efetuar a reinstalação com a máxima urgência.

Atenciosamente,

  
**Gilsandra Iara Marino**  
**Controladora Geral do Município**  
**Portaria 8.053/2021**



AVENIDA HONORIO FRAGA N°405 CENTRO, SÃO DOMINGOS DO NORTE-ES  
CNPJ-18000553/0001-00 TELEFONE: 27 9 9955-0342

## LAUDO TÉCNICO

**Descrição do Problema Relato:** O computador não iniciava o Sistema Operacional, entrando em um loop infinito entre Tela Azul e Reparação de Disco.

### Problemas Encontrados:

- **Infecção Por Malwares:**

TrojanDropper:JS/Manigpe.A 01/05/2021	Grave ▼
Worm:Win32/Vobfus.Bllinf 01/05/2021	Grave ▼
Exploit:Java/Obfuscator.R 01/05/2021	Grave ▼
Exploit:JS/Blacole.MQ 01/05/2021	Grave ▼
Exploit:JS/Pdfupf.D 01/05/2021	Grave ▼
MonitoringTool:Win32/EliteKeylogger 01/05/2021	Grave ▼
Worm:BAT/Gus.A 01/05/2021	Grave ▼
Trojan:Win32/Pdfphish.T 01/05/2021	Grave ▼
Trojan:BAT/Hideproc.C 01/05/2021	Grave ▼
Trojan:DOS/Killmbr 01/05/2021	Grave ▼
TrojanDownloader:JS/Renos.B 01/05/2021	Grave ▼
TrojanDownloader:O97M/EncDoc.AVP!MTB 01/05/2021	Grave ▼

Trojan:JS/Pdfjsc.Y 01/05/2021	Grave ∨
Exploit:JS/Pdfupf.D 02/05/2021	Grave ∨
PWS:HTML/Phish.LC 02/05/2021	Grave ∨
TrojanDownloader:VBS/Zriptew.A 02/05/2021	Grave ∨
MonitoringTool:Win32/EliteKeylogger 02/05/2021	Grave ∨
Trojan:O97M/Obfuse.AE 02/05/2021	Grave ∨

- **Dados Corrompidos pelos malwares acima.**

#### **Procedimentos Realizados:**

- **Backup dos Dados;**
- **Formatação do Sistema Operacional;**
- **Recuperação do Backup, que infelizmente estava comprometido pelos arquivos maliciosos;**
- **Tentativa de recuperar os dados corrompidos diretamente do HD comprometido;**
- **Dados recuperados porém corrompidos.**

#### **Conclusão**

Algum arquivo Malicioso supracitado (PDF's, Imagens, arquivos diversos baixados de sites não-confiáveis), foi executado no computador, ocasionando problemas de dados Corrompidos, tanto do lado de arquivos do Usuário, quanto aos arquivos do Sistema Operacional.



---

LUCAS MARRANE SILER | 147.558.937.98

Técnico em Informática