DATAPREV

Segurança da Informação

A Dataprev

Data centers	DF	SP	RJ
Área	**257**	**384**	**988**
Capacidade elétrica (kVA)	**600**	**900**	**1200**

Capacidade de processamento

RISC	**48** Tflop/s
X86	**116** Tflop/s
Mainframe	**153.000** RPM

Capacidade de armazenamento **6** Petabytes

Sede em Brasília – **3.854** empregados
Presente em todas as capitais
Cinco Unidades de Desenvolvimento

Clientes

MPS
Ministério
da Previdência Social

INSS
Instituto Nacional
do Seguro Social

MTE
Ministério do Trabalho
e Emprego

MDS
Ministério do
Desenvolvimento Social e
Combate à Fome

SRFB
Secretaria da Receita
Federal do Brasil

PGFN
Procuradoria-Geral
da Fazenda Nacional

MPOG
Ministério do Planejamento,
Orçamento e Gestão

Funpresp
Fundação de Previdência
Complementar do Servidor
Público Federal

Previc
Superintendência Nacional
de Previdência Complementar

ANTT
Agência Nacional de Transportes Terrestres

+instituições financeiras
públicas e privadas

Cultura da Segurança da Informação

Visão de fraudes

Antes

Fraudes = alterações indevidas de dados

Hoje

Fraudes = acesso a determinada informação, ataques por DdoS *(Distributed Denial of Service)*

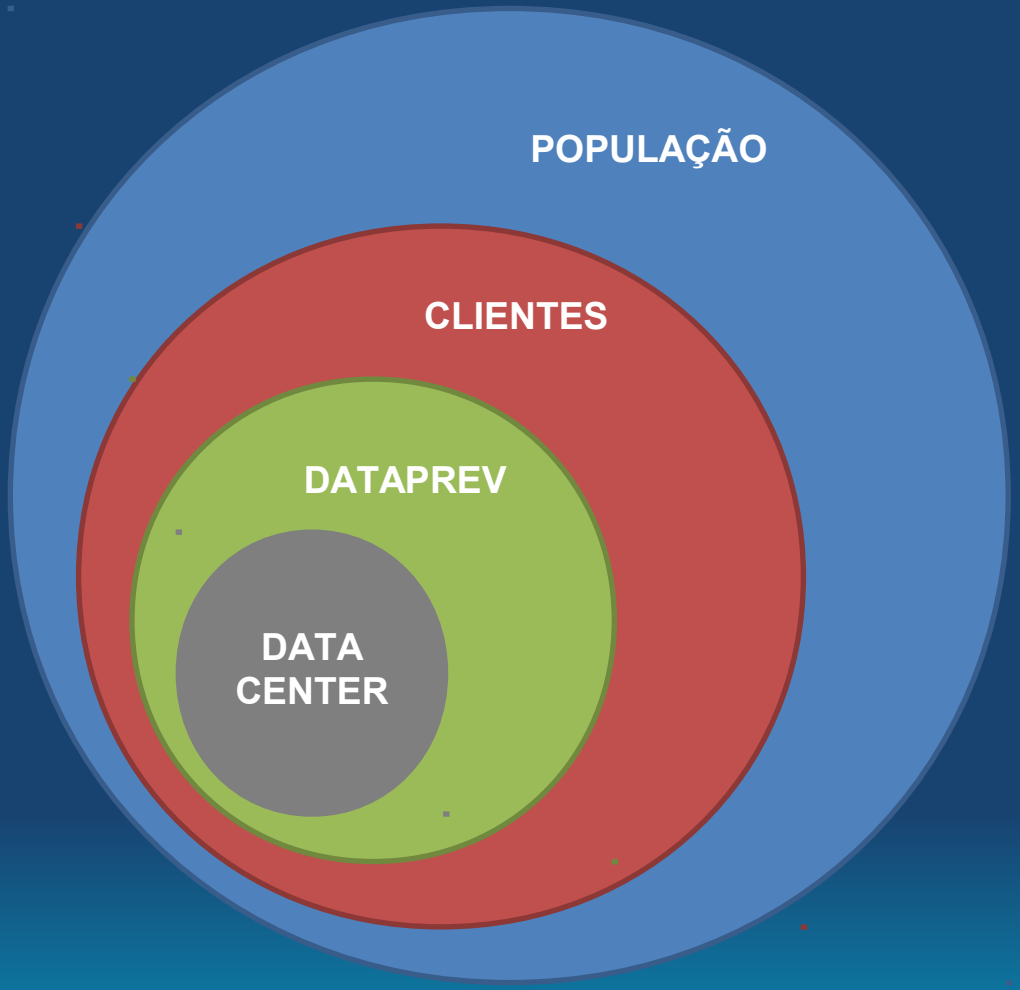
Sistemas "legados"

Não preparados para combate a tipos mais modernos de fraudes

Segurança x acesso

Reconhecer acessos autorizados ou indevidos

Acesso a informação x Proteção de dados



Ações gerais de prevenção contra ameaças à segurança

Parcerias estratégicas de segurança

CTIR.gov, APEGR/MPS, Cert.br

Parceria com a Polícia Federal

Grupo especializado em análise de segurança

Investimento operacional em uma equipe especializada na detecção, investigação e tomada de ações direcionadas contras invasões avançadas.

Conformidade

Investimentos na busca contínua do alinhamento com as melhores práticas do mercado. Alinhamento com órgãos de controle e auditoria - CGU, TCU, MPU.

Plano de ação de segurança

Em 2015 estão sendo implementadas ações relativas a:

- Continuidade de negócios: clientes e Dataprev
- Vulnerabilidades nos sistemas
- Desenvolvimento seguro de software
- Controle de acesso entre aplicações
- Cofre de senhas
- Gestão centralizada de registros de eventos (logs)
- Sistema de Gestão de Segurança da Informação (SGSI)
- Gestão de riscos nos ativos de TIC
- Conscientização e capacitação em Segurança da Informação (PCSIC)

Tratamento de incidentes e vulnerabilidades

Incidentes de segurança da informação	2013	2014	2015
Reportados	**66**	**53**	**51**
Fechados	**49**	**41**	**33**

Tratamento de riscos e vulnerabilidades técnicas	2013	2014	2015
Risco aceito	**15,59%**	**14,56%**	**0%**
Tratamento em andamento	**29,40%**	**0%**	**38,03%**
Controles de segurança implementados	**55,01%**	**85,44%**	**61,97%**
Total	**100%**	**100%**	**100%**

Ameaças monitoradas Estratégias de ataque conhecidas

Vazamento de informações
Direcionado a pessoas, processos e tecnologias.

Fraudes eletrônicas
Phishing Scam envolvendo o sistema bancário e serviços da Previdência Social.

Ataques direcionados
Desenvolvidos com foco nos sistemas e serviços oferecidos pela Previdência Social.

Ataques com grande volumetria
Ataques de negação de serviço com grande capacidade e nível de organização.
Ataques até 20% acima da capacidade da rede (1.2 GB).

Sequestro de dados
Preocupação crescente com ataques focados no sequestro de dados.

Ações preventivas Vazamento de informações

Conformidade

Investimentos na busca contínua do alinhamento com as melhores práticas do mercado.

Privacidade dos dados

Mascaramento de dados.

Controle de acesso aos sistemas

Sistema de gestão de acessos de desenvolvimento próprio (GerID).

Garantia de confidencialidade de dados em trânsito

- Criptografia

Entre aplicações e entre a comunicação cliente/servidor.
Redes de longa distância (*backbone*).

Grupo especializado em análise de segurança

Investimento operacional em uma equipe especializada na detecção, investigação e tomada de ações direcionadas contras invasões avançadas.

Ações preventivas Fraudes eletrônicas

Anti-Spam
Revisão contínua de políticas de detecção e bloqueio.

Filtragem de conteúdo
Refinamento de regras.
Investimentos em soluções mais robustas.

Intensificação de ações de conscientização
Programa contínuo com foco no eixo Pessoas.

Comissão de Tratamento de Incidentes (CTIR)
Tratamento de incidentes de segurança.

Análise de códigos maliciosos

Ações preventivas Ataques direcionados

Proteção em camadas

Tecnologias de última geração específicas para proteção dos sistemas e das bases de dados.

Estudo de tendências

Equipe de profissionais dedicada a pesquisas e estudos de tendências e cenários de ataques.

Desenvolvimento seguro de software

Requisitos de segurança definidos em tempo de projeto de desenvolvimento.
Testes de segurança de código.

Ações preventivas Ataques com grande volumetria

Monitoramento proativo da infraestrutura de rede

Centro de Operação da Rede atuando no refinamento de regras e alertas para detecção de incidentes de segurança e na identificação de ataques, não apenas falhas.

Parceria com operadoras

Tratamento do tráfego para contenção de ataques distribuídos de grande volumetria antes da chegada ao perímetro da rede da Dataprev.

Modernização dos data centers

Aumento da capacidade de contenção de ataques.

Proteção em camadas – perímetro de rede

Planejamento e investimentos em tecnologias de proteção/detecção de intrusão, como também voltados a *firewall* de próxima geração para análise de comportamento de aplicações e dos usuários.

Diminuição do tempo para recuperação de incidentes

Ações preventivas Sequestro de dados

Programa de continuidade de negócios

Programa contínuo de planejamento e testes de planos de gerenciamento de incidentes graves, recuperação de desastres, entre outros cenários.

Processos

Processo contínuo de gestão de riscos.
Processo contínuo de gestão de vulnerabilidades técnicas.
Processo contínuo de avaliação de segurança no ambiente de servidores.

Modernização de soluções de proteção de dados

Modernização das soluções de backup tradicionais para um modelo robusto, em camadas.

Investimentos em Segurança da Informação

R$ 235 milhões
contratados

2011	• Solução IPS • Evolução da rede • Ampliação das soluções de firewall • Instalação da sala de monitoramento (NOC)
2012	• Sala-cofre (DC – Distrito Federal) • Solução de firewall de banco de dados
2013	• Sala-cofre (DC – São Paulo)
2014	• Sala-cofre (DC – Rio de janeiro) • Solução Integrada de Controle de Acesso Físico
2015	• Firewall de rede • Solução de criptografia de backbone • Certificados digitais para usuário • Certificados digitais para servidores WEB

Investimentos em Segurança da Informação

Previsão 2015

- Firewall de Aplicação (WAF)
- Solução de proteção de dados

Em estudo para implantação

- Cofre de senhas
- Solução de proteção de intrusão
- Solução de análise estática e dinâmica de código
- Solução de correlacionamento de eventos
- Solução de monitoramento de segurança
- Solução de análise de segurança
- Mascaramento de dados

Rodrigo Assumpção

Presidente

Dataprev

Setembro 2015