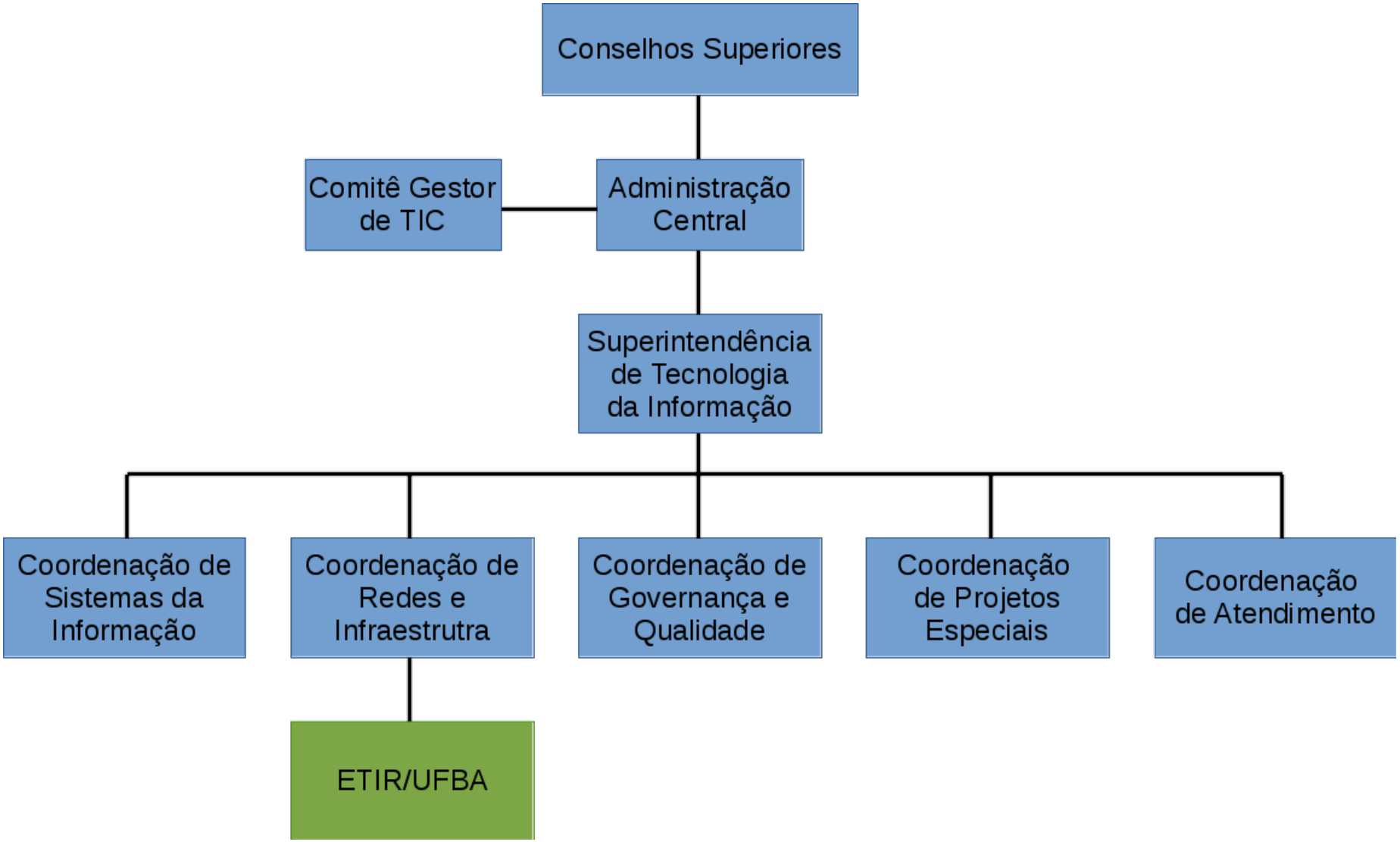
Cibersegurança no ambiente acadêmico

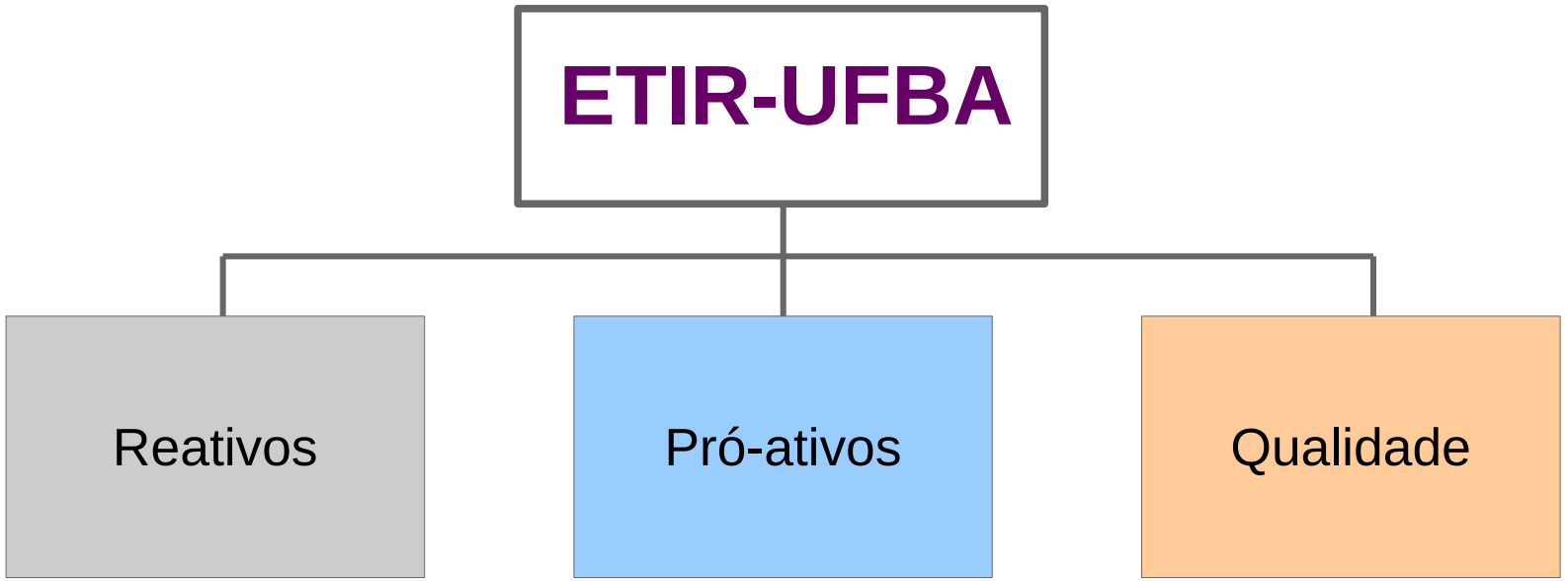
Italo Valcy <italovalcy@ufba.br>
Salvador – BA, 27/Set/2016

STI
Superintendência de
Tecnologia da Informação | UFBA

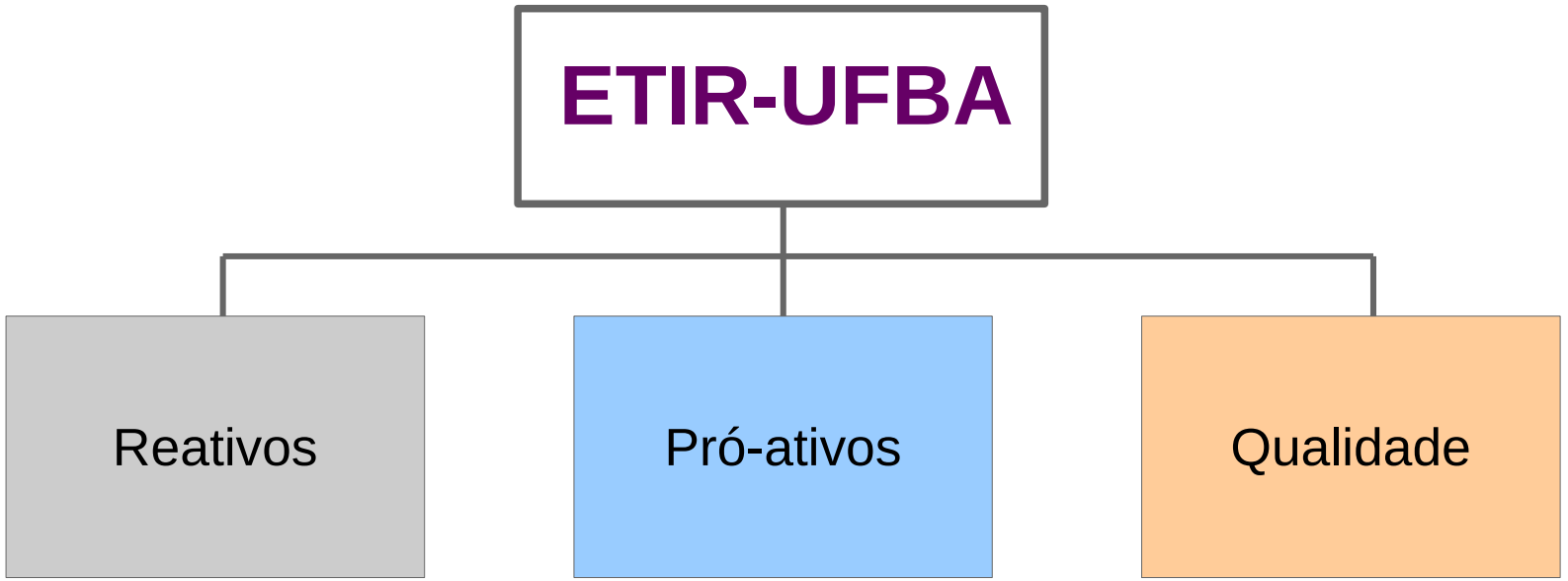
Estrutura do ETIR-UFBA



Serviços do ETIR-UFBA



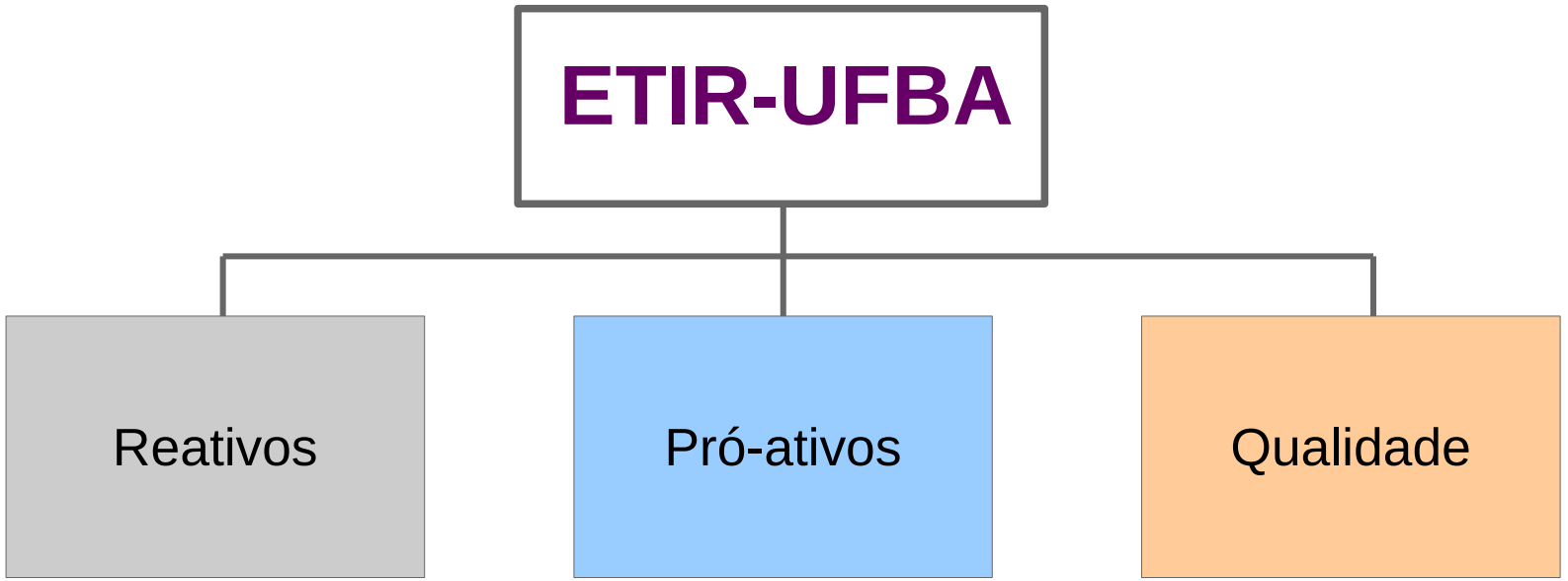
Serviços do ETIR-UFBA



Serviços Reativos

- Tratamento de Incidentes
- Análise Forense
- Envio de notificações de incidentes
- Ações corretivas e de mitigação

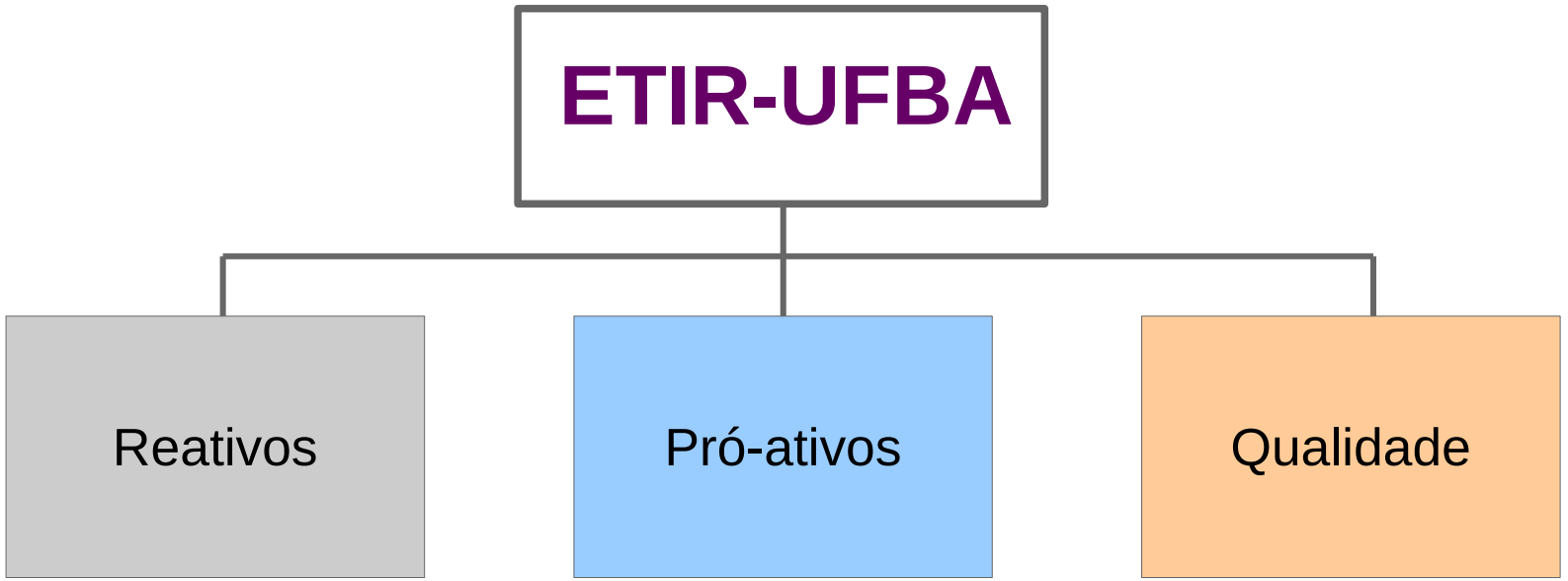
Serviços do ETIR-UFBA



Serviços Pró-ativos

- Distribuição de Alertas, Recomendações e Estatísticas
- Monitoramento e prevenção de atividade maliciosa
- Gestão de Vulnerabilidades
- Auditoria de Sistemas de Informação
- Desenvolvimento de Ferramentas

Serviços do ETIR-UFBA

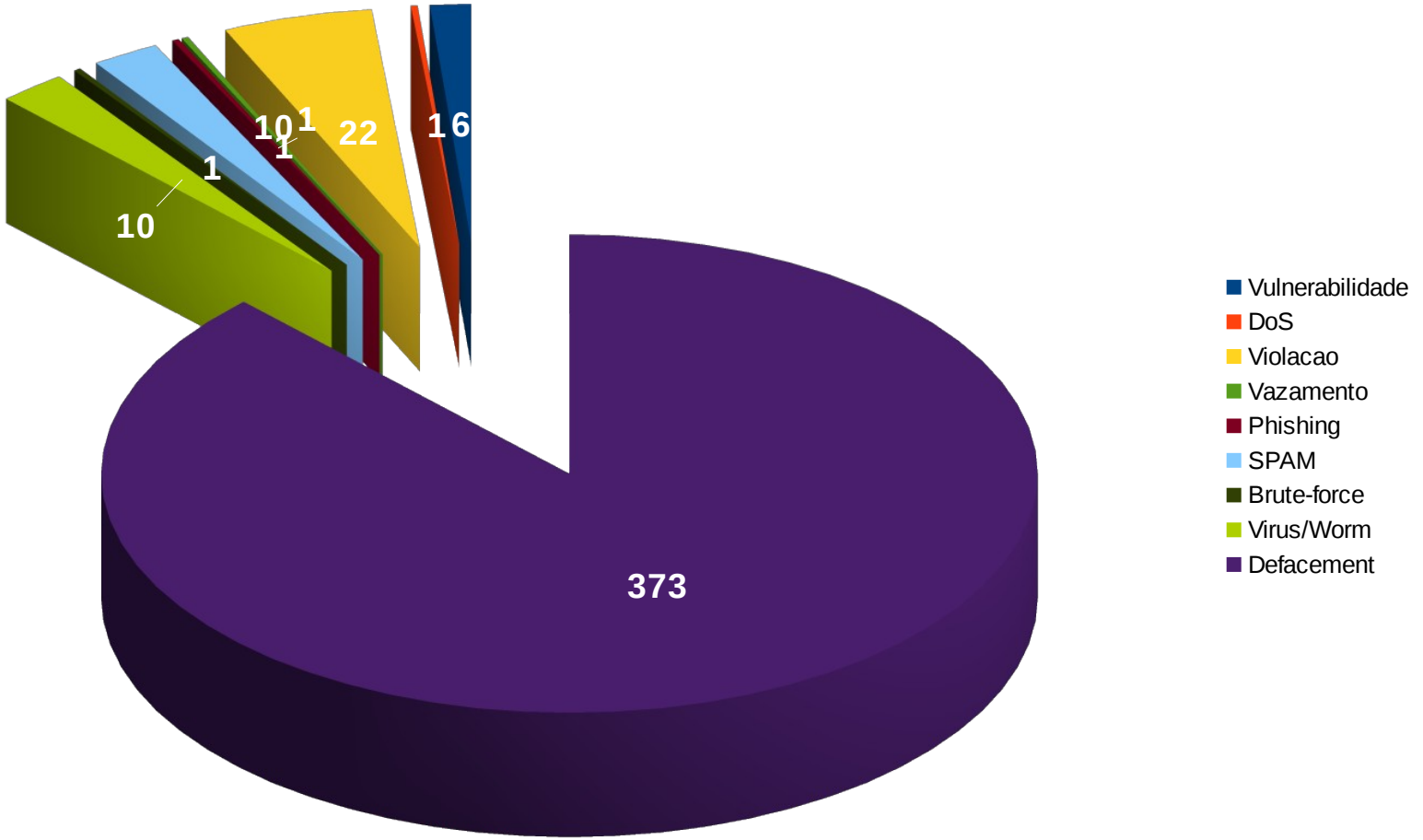


Serviços Qualidade

- Cooperação com outras equipes de segurança da informação
- Gestão de riscos de segurança da informação
- Disseminação da cultura de segurança da informação
- Apoio na definição e escrita de normas e políticas de Segurança da Informação para outros setores da Universidade

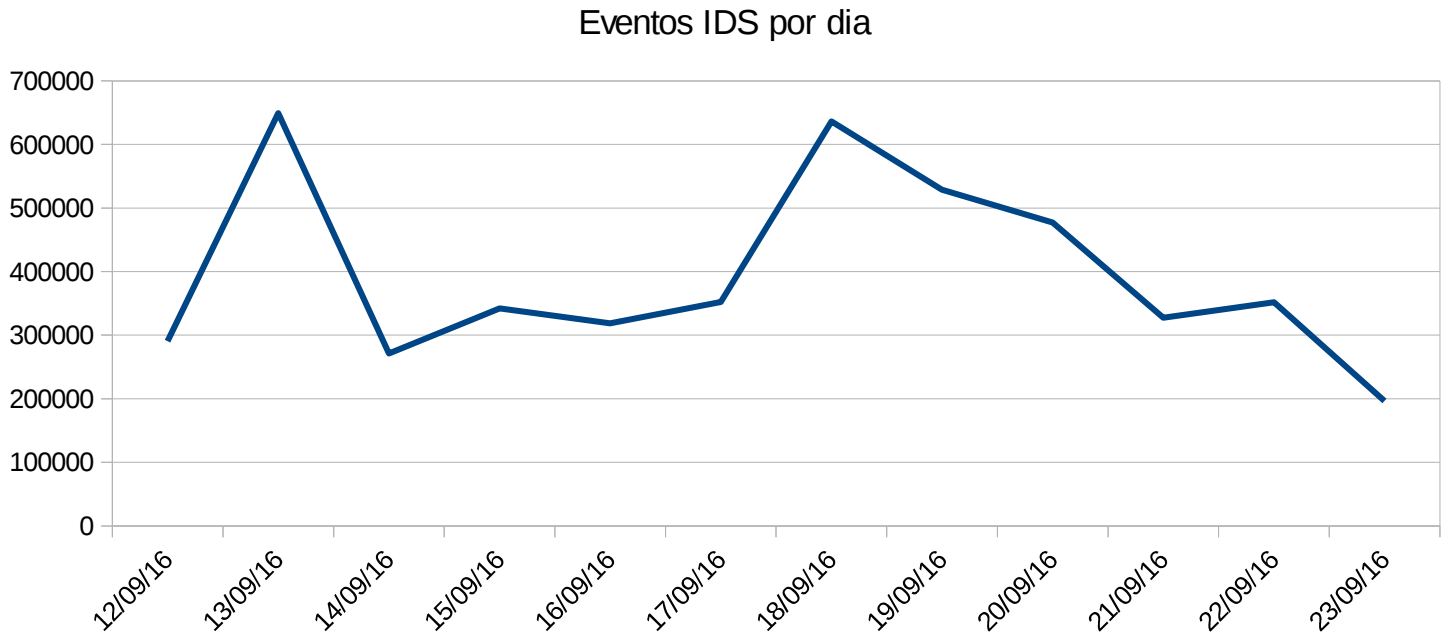
Estatísticas de Incidentes

- Incidentes originados na UFBA em 2016



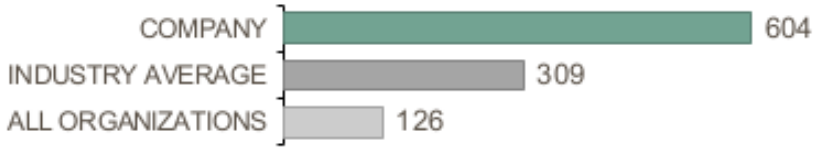
Ataques contra a UFBA

- Ataques contra UFBA (recebidos no IDS)

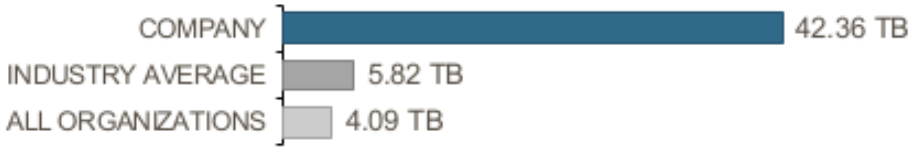


Aplicações de alto risco

Number of Applications on Network

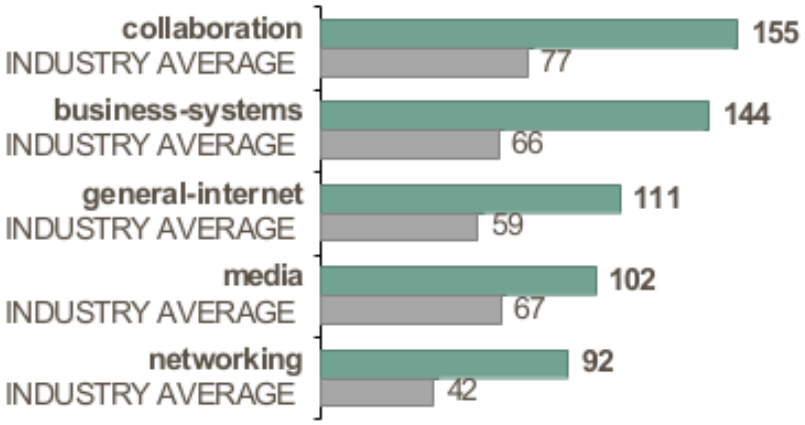


Bandwidth Consumed by Applications



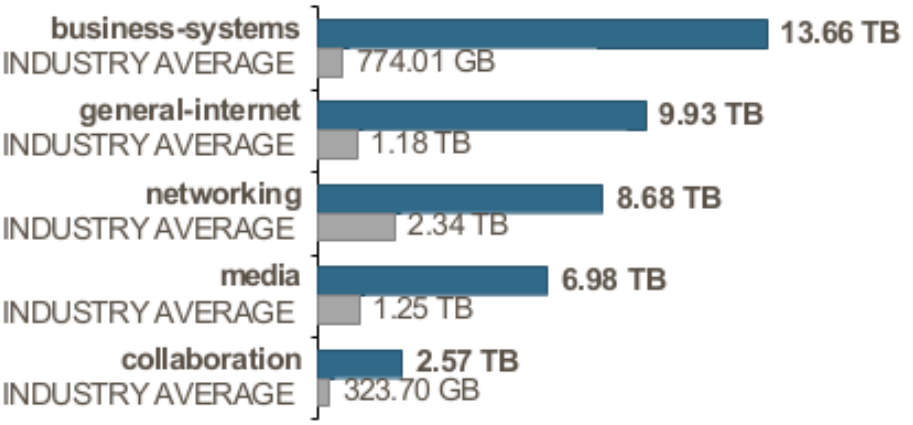
Categories with the Most Applications

The following categories have the most applications variants, and should be reviewed for business relevance.



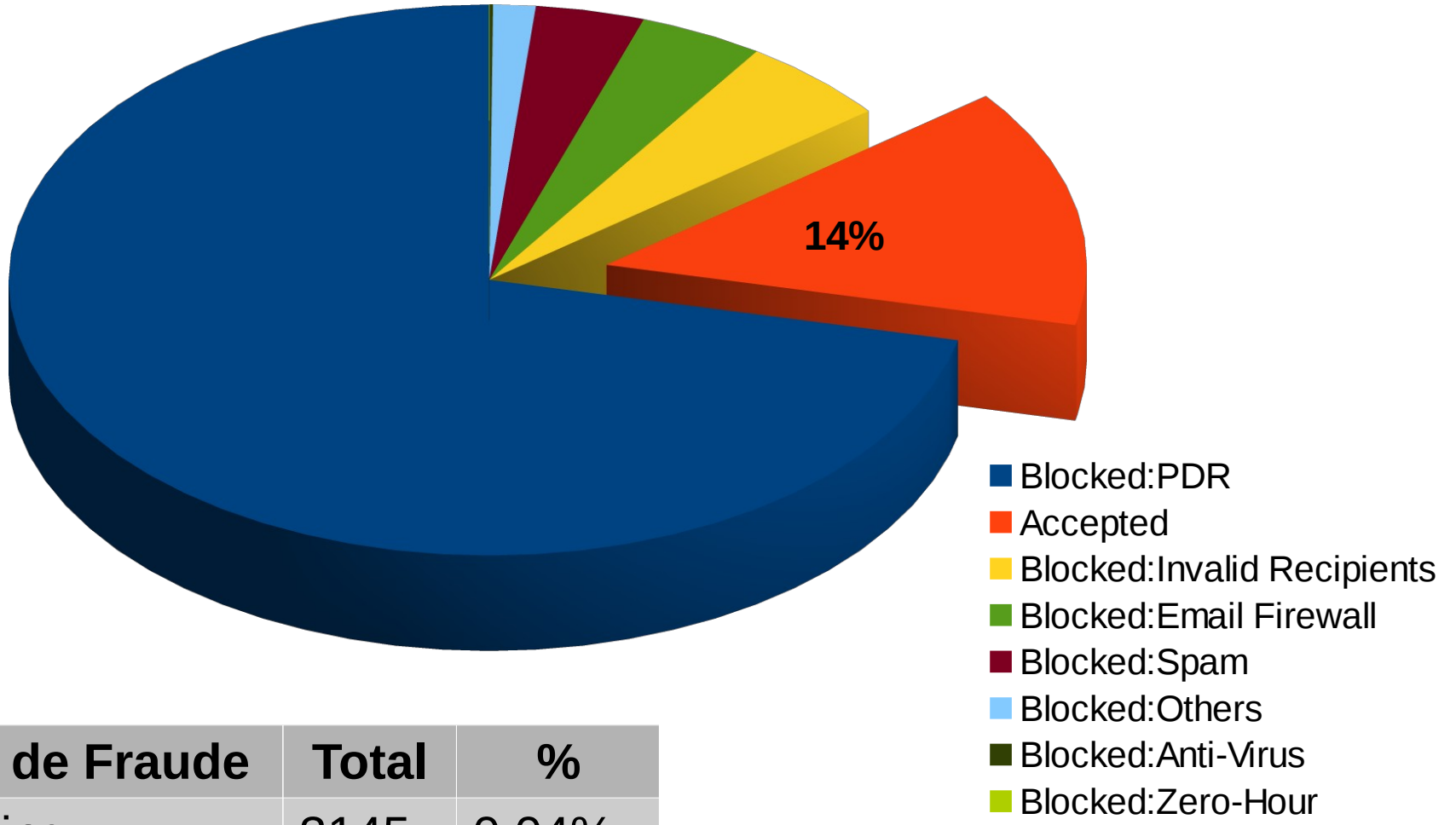
Categories Consuming the Most Bandwidth

Bandwidth consumed by application category shows where application usage is heaviest, and where you could reduce operational resources.



E-mail - Resumo de Mensagens

Período de 01/07 à 16/07/16

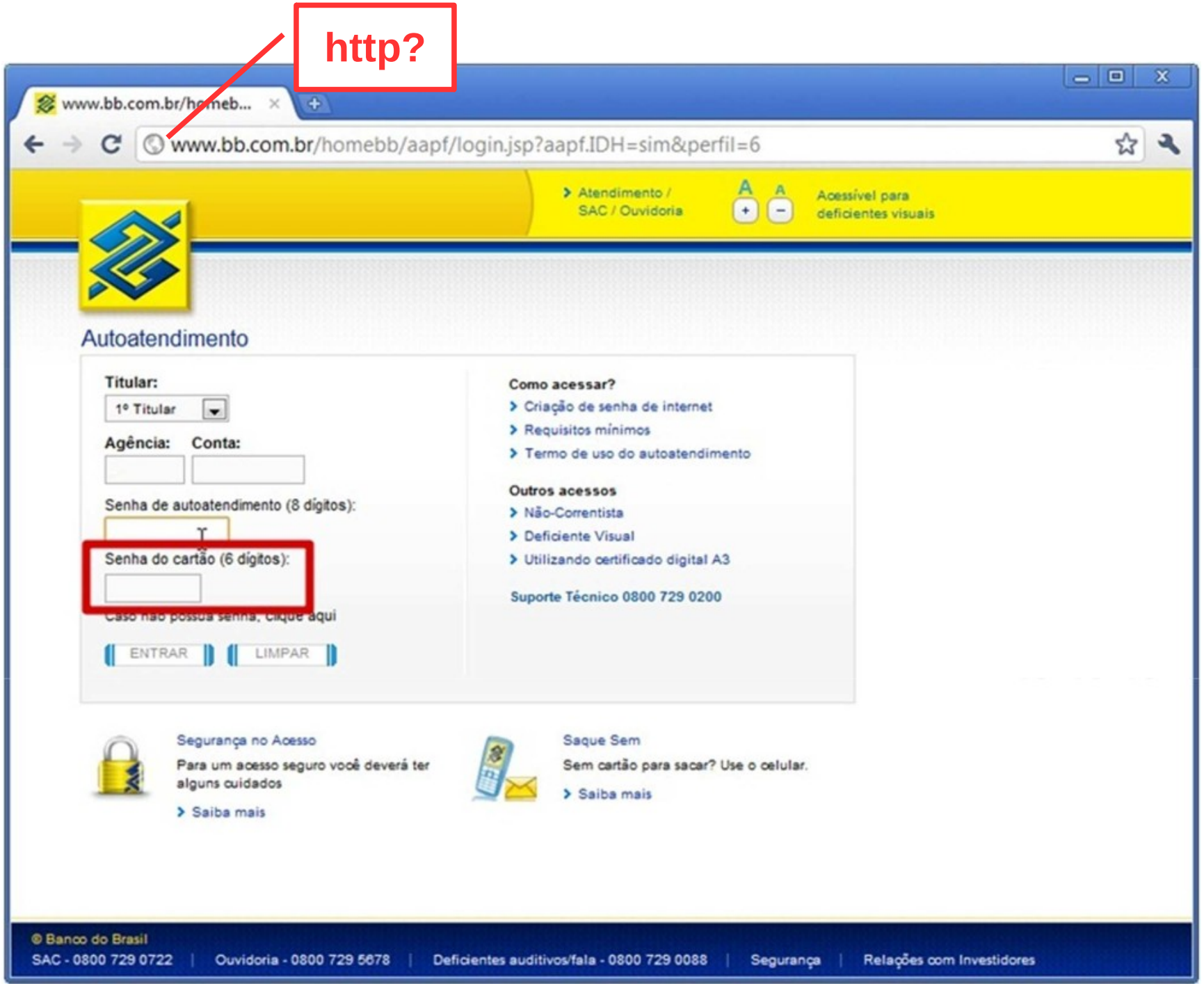


Tipo de Fraude	Total	%
Phishing	3145	0.04%
Malware	8634	0.12%

URLs maliciosas nas fraudes

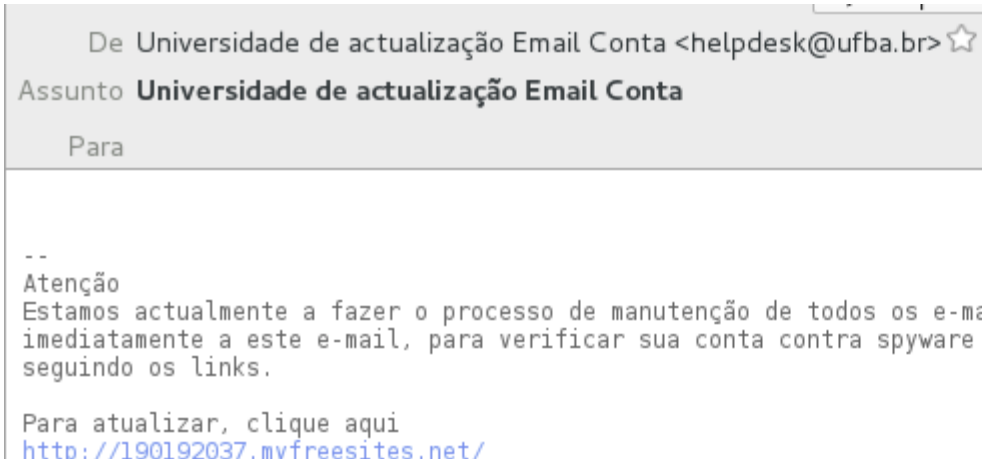
Período de 01/07 à 16/07/16

- Mensagens filtradas: 11294
- Mensagens entregues: 897
- Defesa de URL, com reescrita de 43%
  - Cliques Bloqueados: 19
  - Cliques permitidos: 8
  - Total de cliques: 27
- Grande parte dos ataques são direcionados


http?
www.bb.com.br/homebb/aapf/login.jsp?aapf.IDH=sim&perfil=6
Atendimento / SAC / Ouvidoria
Acessível para deficientes visuais
Autoatendimento
Titular:
1º Titular
Agência:
Conta:
Senha de autoatendimento (8 dígitos):
Senha do cartão (6 dígitos):
Caso não possua senha, clique aqui
ENTRAR
LIMPAR
Como acessar?
Criação de senha de internet
Requisitos mínimos
Termo de uso do autoatendimento
Outros acessos
Não-Correntista
Deficiente Visual
Utilizando certificado digital A3
Suporte Técnico 0800 729 0200
Segurança no Acesso
Para um acesso seguro você deverá ter alguns cuidados
Saiba mais
Saque Sem
Sem cartão para sacar? Use o celular.
Saiba mais
© Banco do Brasil
SAC - 0800 729 0722
Ouvidoria - 0800 729 5678
Deficientes auditivos/fala - 0800 729 0088
Segurança
Relações com Investidores

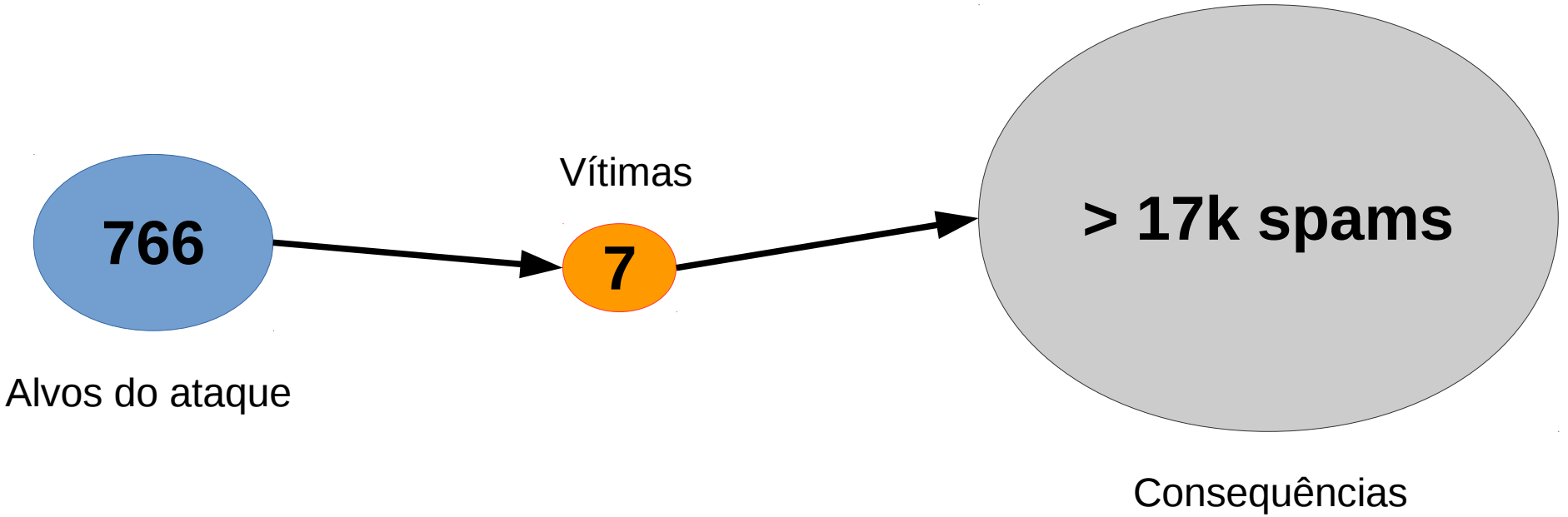
Exemplo de phishing

- Caso de phishing direcionado aos usuários da UFBA
  - Falsificação do From + Página forjada do webmail



Exemplo de phishing

- Caso de phishing direcionado aos usuários da UFBA



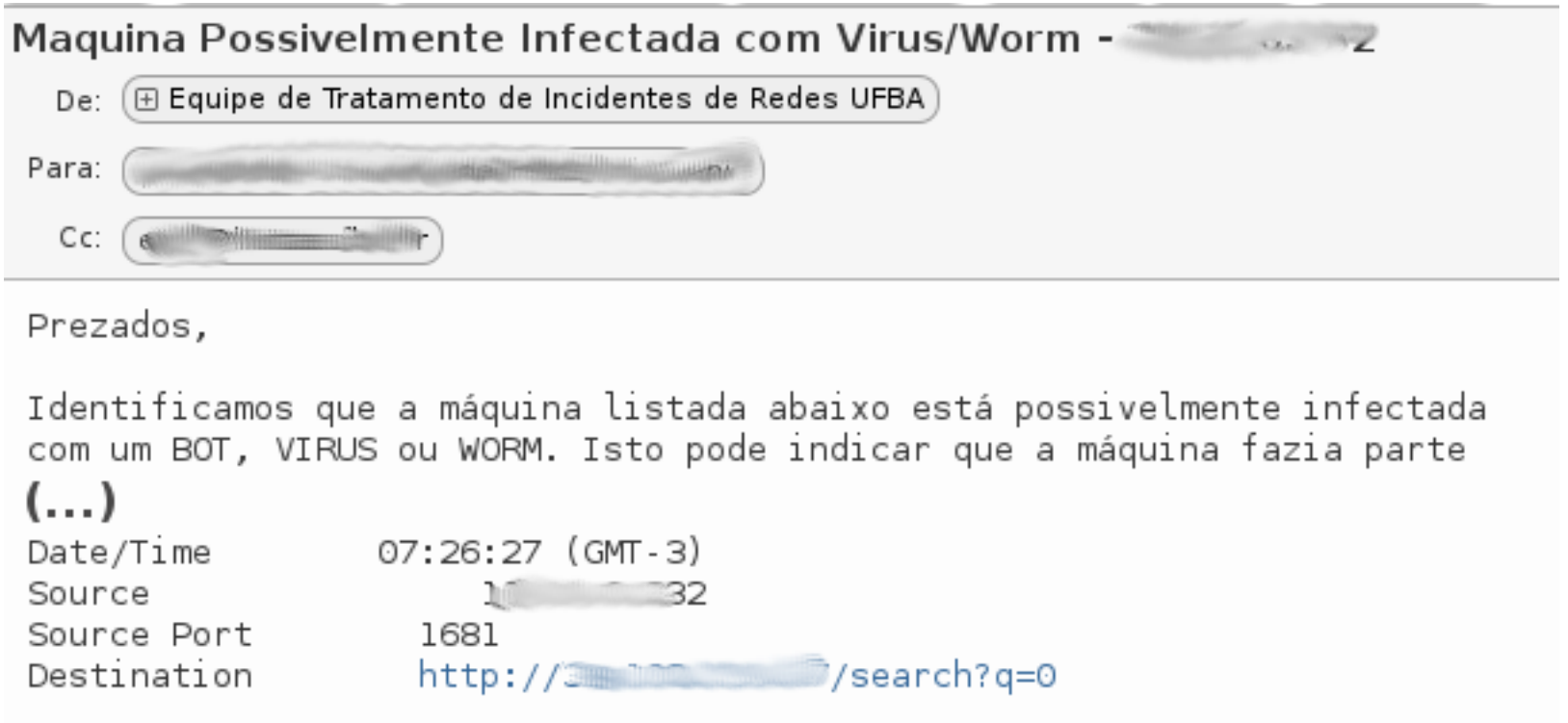
Código Malicioso na Rede UFBA

- Hosts protegidos na UFBA **3274** / 13911
- Já tivemos **895** eventos de vírus em 2016
  - **173** infecções por mídias externas
- Consequências de uma máquina infectada:
  - Atividade maliciosa na máquina
  - Propagação em outras máquinas
  - Lentidão na máquina e na rede UFBA
  - Perda de dados

Casos recentes

1) máquina infectada com vírus

- Infecção com Conficker
- Equipamento médico – sistema de raio X



Maquina Possivelmente Infectada com Virus/Worm - [redacted]

De: Equipe de Tratamento de Incidentes de Redes UFBA

Para: [redacted]

Cc: [redacted]

Prezados,

Identificamos que a máquina listada abaixo está possivelmente infectada com um BOT, VIRUS ou WORM. Isto pode indicar que a máquina fazia parte

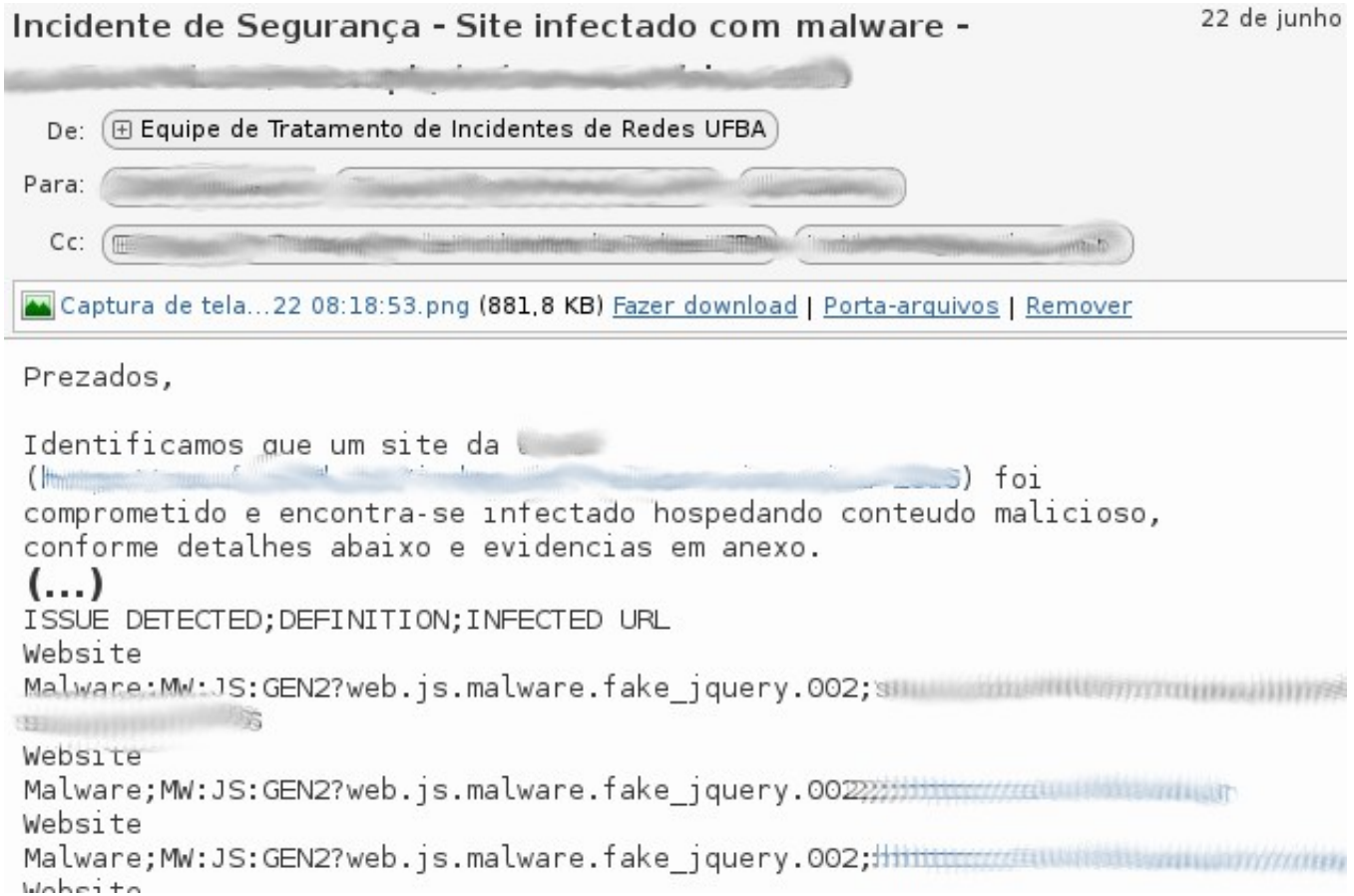
(...)

Date/Time 07:26:27 (GMT-3)
Source [redacted]32
Source Port 1681
Destination http://[redacted]/search?q=0

Casos recentes

2) site propagando vírus

- Vírus Fake JS / jQuery.php



Incidente de Segurança - Site infectado com malware - [redacted] 22 de junho

De: Equipe de Tratamento de Incidentes de Redes UFBA

Para: [redacted]

Cc: [redacted]

Captura de tela...22 08:18:53.png (881,8 KB) Fazer download | Porta-arquivos | Remover

Prezados,

Identificamos que um site da [redacted]
([redacted]) foi
comprometido e encontra-se infectado hospedando conteudo malicioso,
conforme detalhes abaixo e evidencias em anexo.

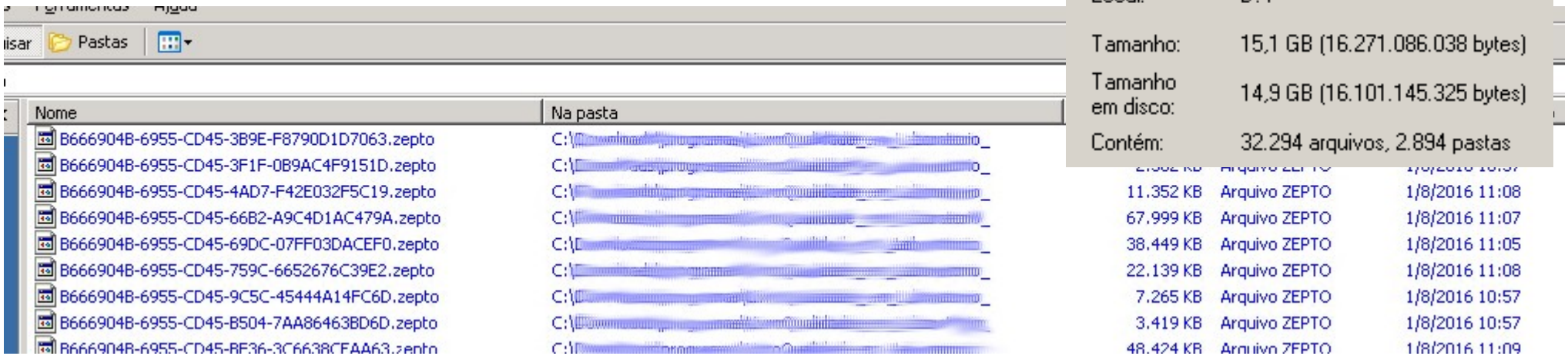
(...)

ISSUE DETECTED;DEFINITION;INFECTED URL
Website
Malware;MW:JS:GEN2?web.js.malware.fake_jquery.002;[redacted]
Website
Malware;MW:JS:GEN2?web.js.malware.fake_jquery.002[redacted]
Website
Malware;MW:JS:GEN2?web.js.malware.fake_jquery.002;[redacted]

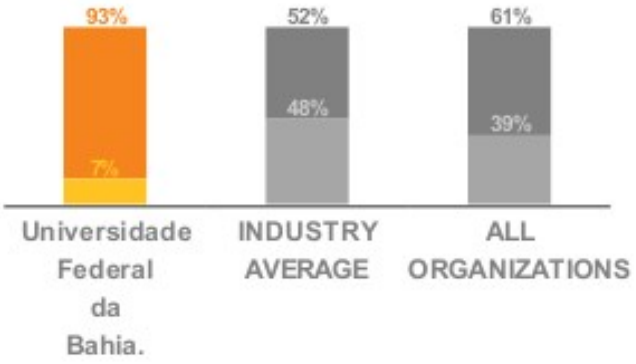
Casos recentes

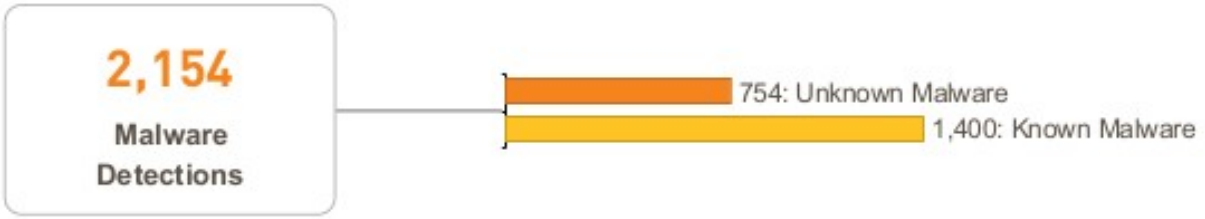
3) Ransomware – sequestro de dados via criptografia

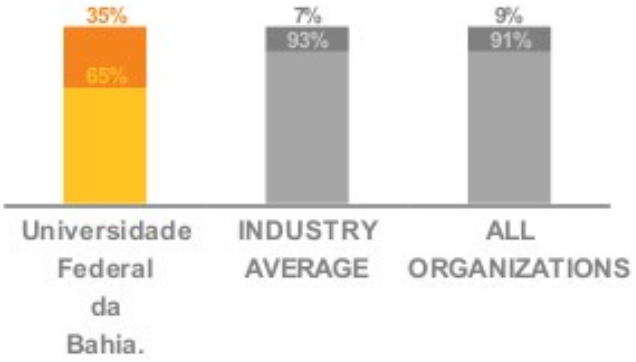
- Máquina infectada por pendrive
- Criptografia de arquivos via compartilhamento windows
- Resgate solicitado 0,5 BTC = R$ 980,00
- Solução foi restaurar o backup do que possível



Ameaças rede UFBA







Desfiguração de páginas web

- A UFBA possui cerca de **1800 sites** web ativos
  - Sites institucionais
  - Grupos de pesquisa
  - Eventos
  - Revistas, Blogs
- Considerando sites de usuário, cerca de **87 / 720** (12%) com vuln. média ou crítica
  - Desses sites, mais de 260 são estáticos (HTML)

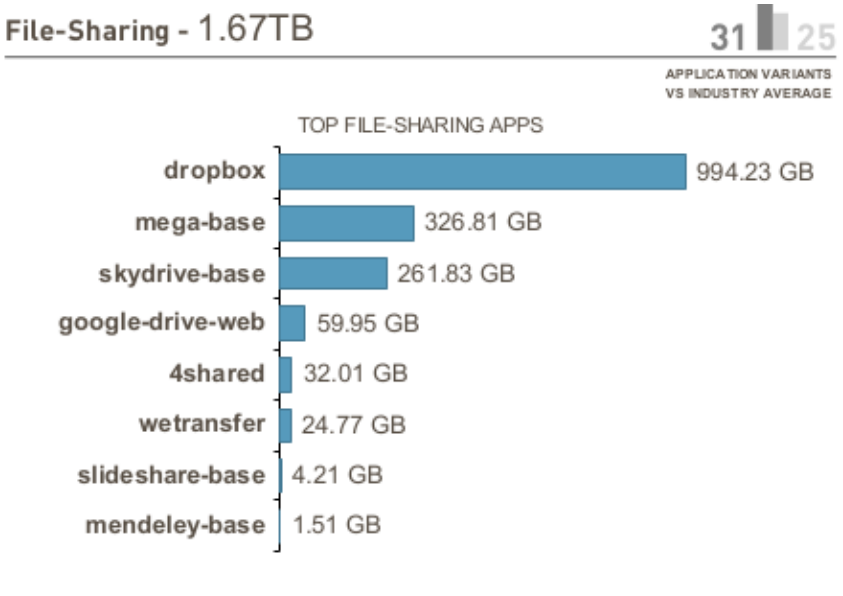
Desfiguração de páginas web

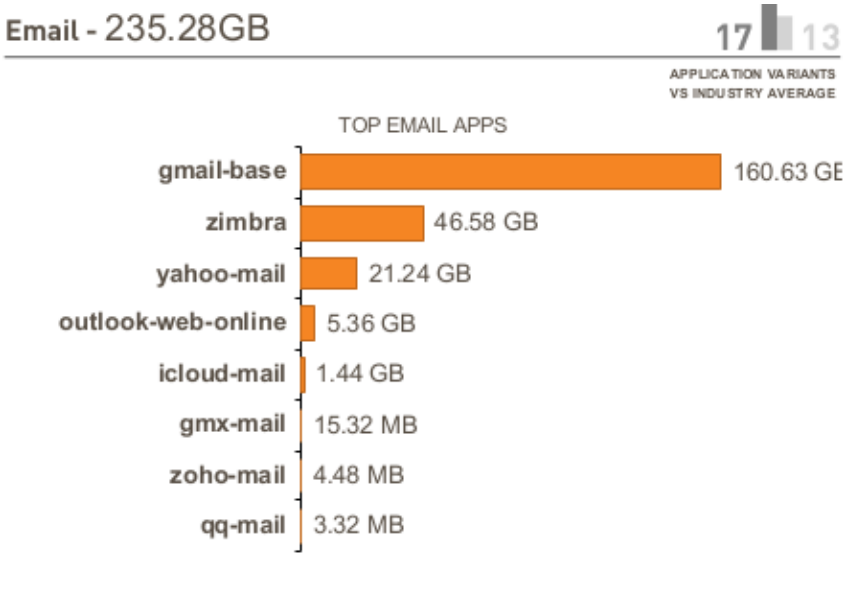
- Qual a natureza desses problemas?
  - Sites antigos e com desenv. descontinuado
  - Falta de qualificação em desenv. seguro
  - Uso de tecnologias inseguras ou desatualizadas
  - Falhas simples e conhecidas
  - Ameaças avançadas e desconhecidas

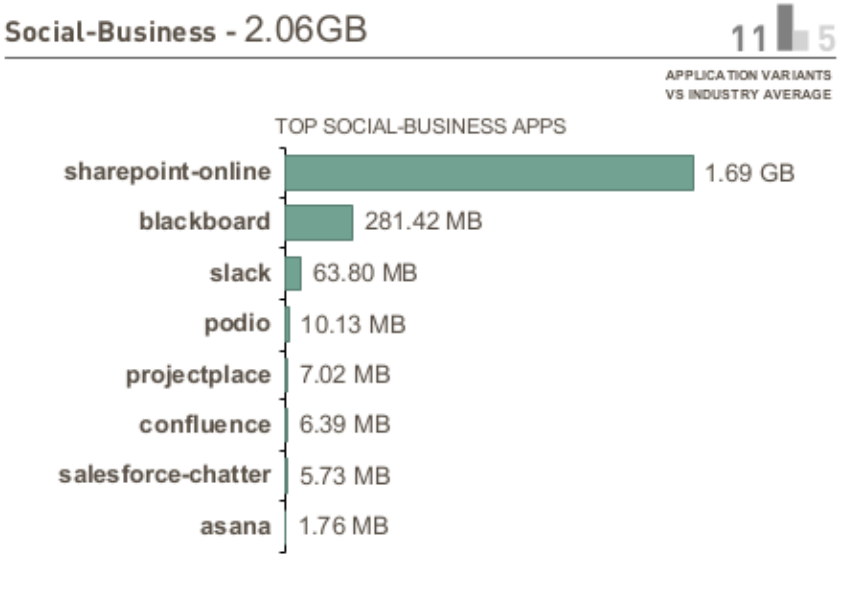
Uso de nuvem pública

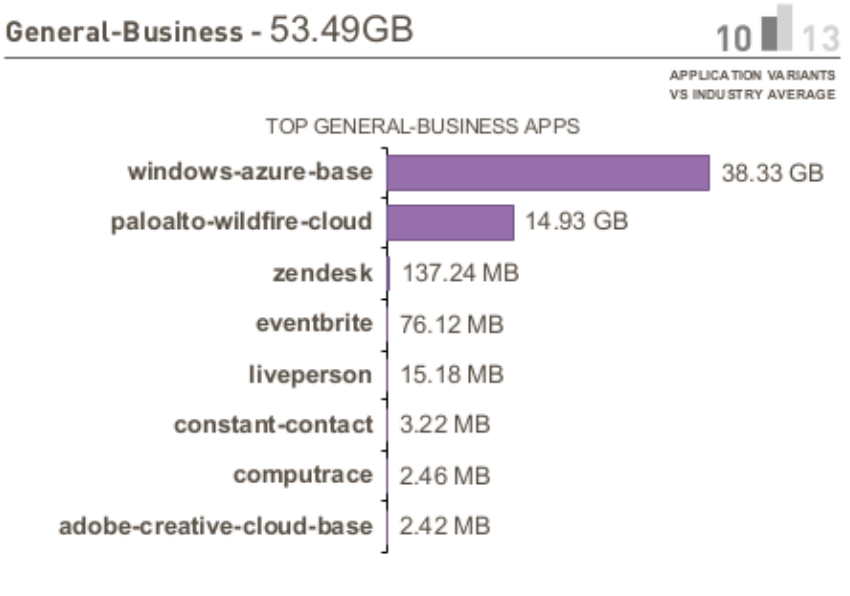
- A comunidade UFBA faz uso massivo de serviços de nuvem pública
  - Ferramentas de compartilhamento de arquivo
  - Ferramentas de escritório
  - E-mail
  - Redes sociais, IM, audio/vídeo

Uso de nuvem pública









Nuvem pública – Termo de Uso

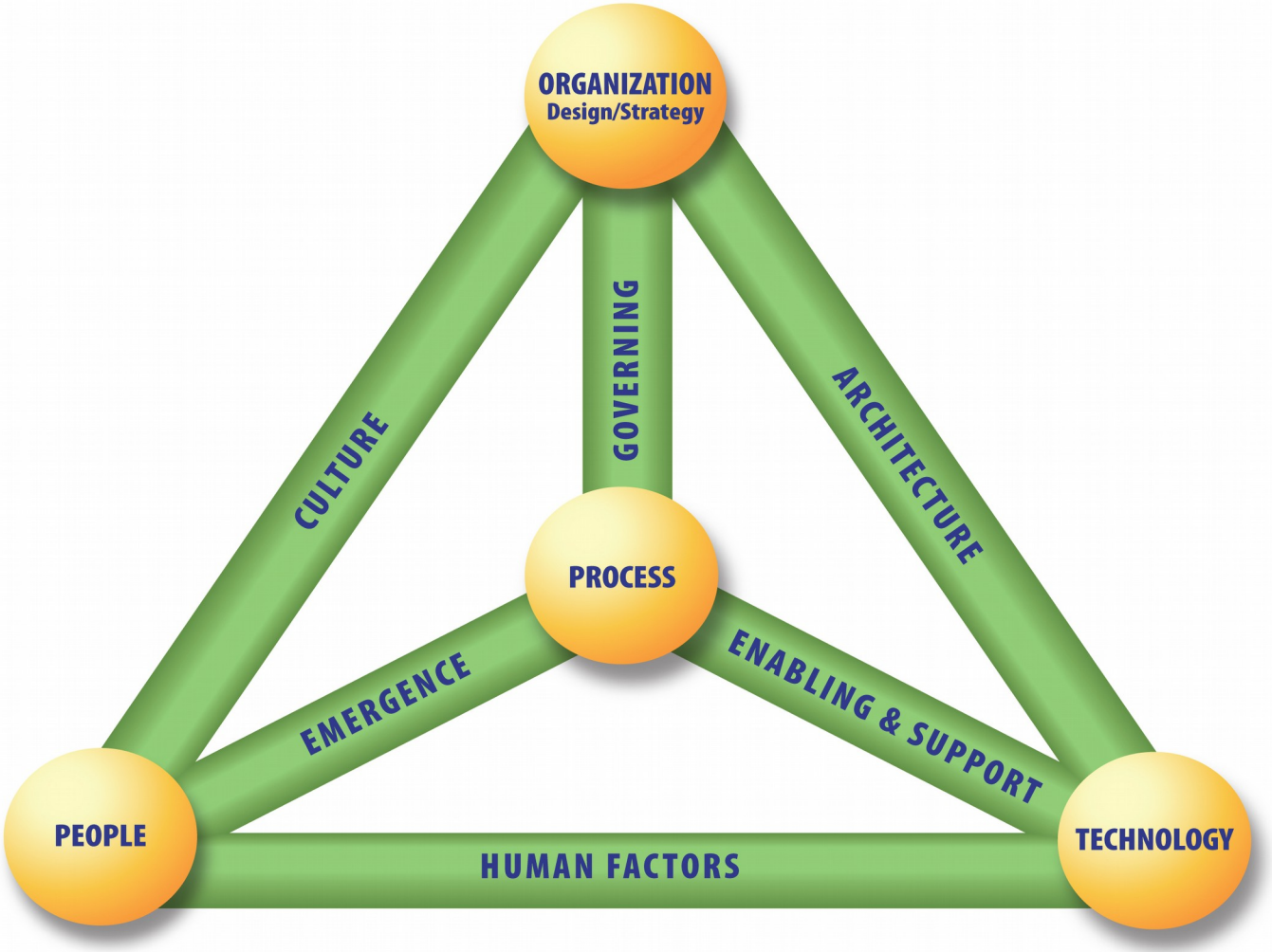
- Exemplo: https://www.google.com/intl/pt-BR/policies/terms/

Quando você faz upload, submete, armazena, envia ou recebe conteúdo a nossos Serviços ou por meio deles, você concede ao Google (e àqueles com quem trabalhamos) uma licença mundial para usar, hospedar, armazenar, reproduzir, modificar, criar obras derivadas (...) para os fins restritos de operação, promoção e melhoria de nossos Serviços e de desenvolver novos Serviços. Essa licença perdura mesmo que você deixe de usar nossos Serviços (…). Certifique-se de que você tem os direitos necessários para nos conceder a licença de qualquer conteúdo que você enviar a nossos Serviços.

Uso de nuvem pública

- Desafios:
  - Termos de uso e Proteção do Conhecimento Científico
  - Tratamento de Informações confidenciais
  - Como garantir a autenticidade das informações?
- Por outro lado...
  - Estamos preparados para fornecer os serviços com as mesmas características? Queremos isso?
  - Temos os recursos de TI necessários?
  - Temos pessoal suficiente e preparado?

Quais ações podem empregadas nesse cenário?



Fonte: ISACA, BMIS triangle.

Ações de disseminação da cultura de Segurança

- Vamos realizar outros **encontros de segurança na Universidade**, nos institutos, nas unidades adminitrativas
- Promover **capacitações** na área de SIC para usuários finais e para o corpo técnico
- Produção de **materiais de conscientização** direcionados para nosso cenário
- Necessidade de ações para **ouvir a comunidade**
- Buscar **aproximação com outras unidades** (ex: DCC, ICI, Direito etc)

Tecnologia

- A UFBA investe em ferramentas e tecnologias para Cibersegurança
  - Soluções de proteção (Firewall, Anti-Vírus, Anti-Spam)
  - Ampliação da capacidade (Disco, CPU, Mem.)
  - Certificação digital
  - Comunicação audio/visual
- Precisamos transformar os desafios em oportunidades de inovação e pesquisa
- Precisamos desenvolver tecnologias
  - Software Livre

Políticas e Processos

- Estamos trabalhando na aprovação e implantação da **POSIC da UFBA**
  - **Apoio e compromisso da alta gestão** são indispensáveis
- Desenvolvimento de **termos de uso** para os serviços de TIC
- Necessidade de **processos** em todo ciclo de vida da informação
- Precisamos analisar criticamente, **auditar** e melhorar os processos existentes

Onde posso obter mais informações?

- Site do GSIC / UFBA:
  - https://gsic.ufba.br
- Site do CERT.Bahia
  - https://certbahia.pop-ba.rnp.br
- Portal da STI / UFBA
  - http://www.sti.ufba.br

*“Se você colocar uma **chave debaixo do tapete** permitirá que um ladrão encontre-a. Os **cibercriminosos** estão usando todas as ferramentas da tecnologia à sua disposição para **hackear contas das pessoas**. Se eles sabem que há uma chave escondida em algum lugar, eles **farão de tudo para encontrá-la**.”*

Obrigado! Dúvidas?

VI Encontro de Segurança em Informática do CERT Bahia

Italo Valcy
<italovalcy@ufba.br>

REALIZAÇÃO: CERT B@hia

CO-PROMOÇÃO: Safernet

APOIO: POP-BA, UFBA, RNP