

4.5 Gestão da Tecnologia da Informação

No que se refere à Gestão da Tecnologia da Informação e Comunicação (TIC), a Diretoria de Tecnologia da Informação (DTI) foi diretamente impactada pela suspensão de atividades presenciais, tendo seu planejamento estratégico e operacional modificados para dar suporte ao trabalho remoto e as ações educacionais à distância.

Conformidade Legal

Buscando a conformidade legal da governança e gestão de TI, o IFS observa e aplica um vasto conjunto de regras e diretrizes estabelecidas ou referenciadas pelo Governo Federal e órgãos de controle.

Conforme o Decreto 7.579/2011, o IFS integra o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) /MP.

De acordo com a Política de Governança de TIC do IFS (PGTIC), a Auditoria Interna (AUDINT – IFS) é responsável pela análise da conformidade do ambiente de TIC, avaliando e desenvolvendo mecanismos para manutenção da conformidade da área de TIC com os marcos regulatórios que regem a Administração Pública.

Modelo de governança de TI do IFS

As boas práticas de Governança de TI vem sendo implementadas no IFS desde 2014 atendendo às recomendações da Auditoria Interna do IFS, tendo como referência os Levantamentos de Governança de TI / IFS do Tribunal de Contas da União (TCU).

Mais informações: <http://www.ifs.edu.br/governanca-de-ti>

A Política de Governança de TIC/IFS (PGTIC), instituída pela Deliberação N° 63/CGTIC/IFS de 02/10/2017, define princípios, diretrizes e estrutura organizacional referentes a governança e gestão de TIC para a Instituição.

O Sistema de Governança de TIC (SGTIC), está alinhado ao Sistema de Governança Corporativa do IFS e tem como instância principal o Comitê Gestor de TIC – CGTIC.

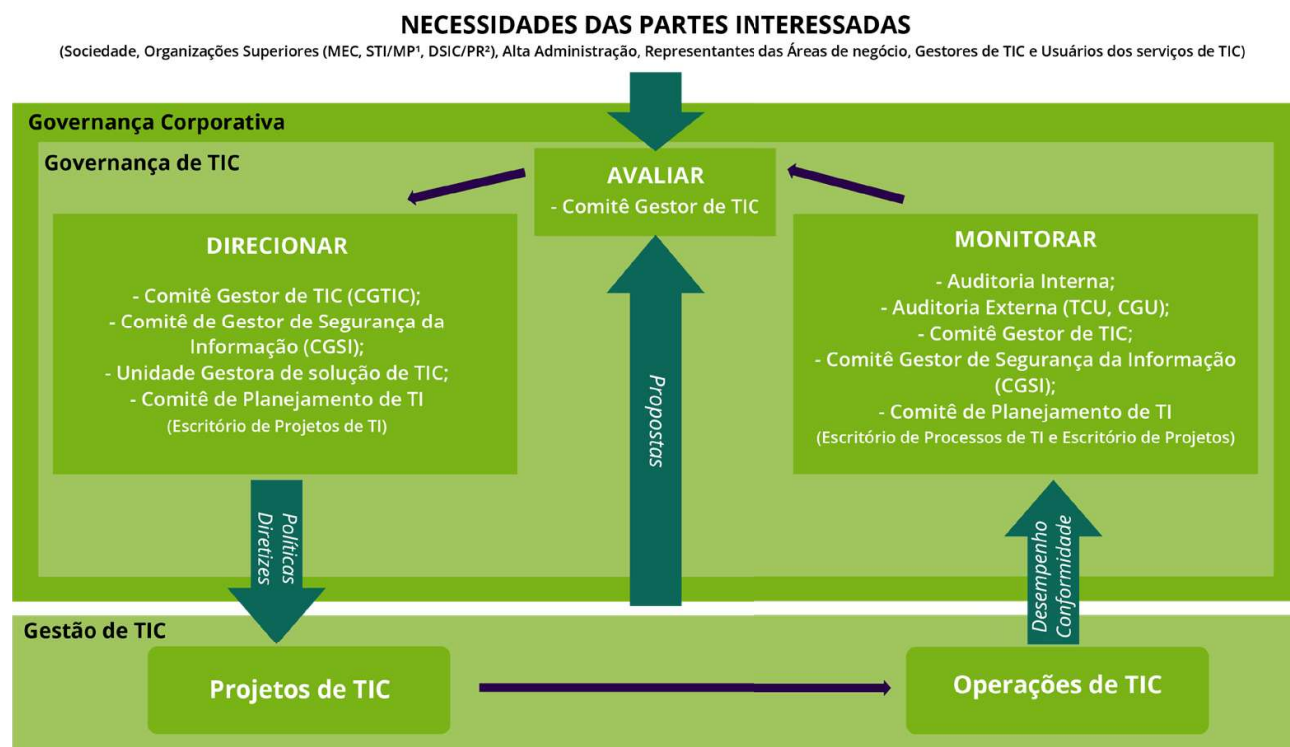


Figura 29 – Sistema de Governança de TI - SGTIC / IFS
Fonte: Deliberação N° 15/2018/CGTIC/IFS de 10/07/2018

A Distribuição dos Direitos Decisórios de TIC entre os Comitês e Estruturas Organizacionais do IFS estão expressas na Tabela a seguir:

Questões de TIC	Distribuição de Direitos decisórios	
	Contribui	Decide
Princípios de TI (Políticas e Diretrizes)	CPlanTI ² e DTI ³	CGTIC ⁴ e CGSI ⁵
Arquitetura de TI	CTI's ⁶ , Cord Sistêmicas de TIC e DTI	CPlanTI
Infraestrutura de TI	CTI's, Cord Sistêmicas de TIC e DTI	CPlanTI
Necessidade de Negócios de Soluções de TI	Todas as unidades organizacionais do IFS	Unidade Gestora de Solução de TI
Investimento e Priorização de TI	CPlanTI e DTI	CGTIC

Tabela 13 – Distribuição dos Direitos Decisórios de TIC entre os Comitês e Estruturas Organizacionais do IFS.
Fonte: Deliberação Nº 15/2018/CGTIC/IFS de 10/07/2018.

O Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC) do Instituto Federal de Sergipe (IFS), instância colegiada de natureza estratégica e deliberativa, de caráter permanente, instituído através da Portaria Nº 3.794/2019/IFS de 06/12/2019, em conformidade com o Decreto nº 9.759 de 11/05/2019, art. 6º e as Portarias nº 788/2019/SGD/ME de 01/09/2019, art. 5º e nº 18.152, de 04/08/2020; é responsável por deliberar sobre políticas, diretrizes e planos relativos à Tecnologia da Informação e Comunicação - TIC e à Governança Digital.

Ele incorpora a função de Comitê de Governança Digital atendendo ao disposto art. 2ª do Decreto Nº10.332 de 28/04/2020 Portaria Nº 18.152, de 04/08/2020.

As reuniões do CGTIC são realizadas em conjunto com o colégio de dirigentes do IFS conforme o Plano Anual de Comunicação.

Mais informações: <http://www.ifs.edu.br/colegiados-dti>

iGG2021 - Governança e Gestão de Segurança e de Tecnologia da Informação Índice de Governança e Gestão de TI

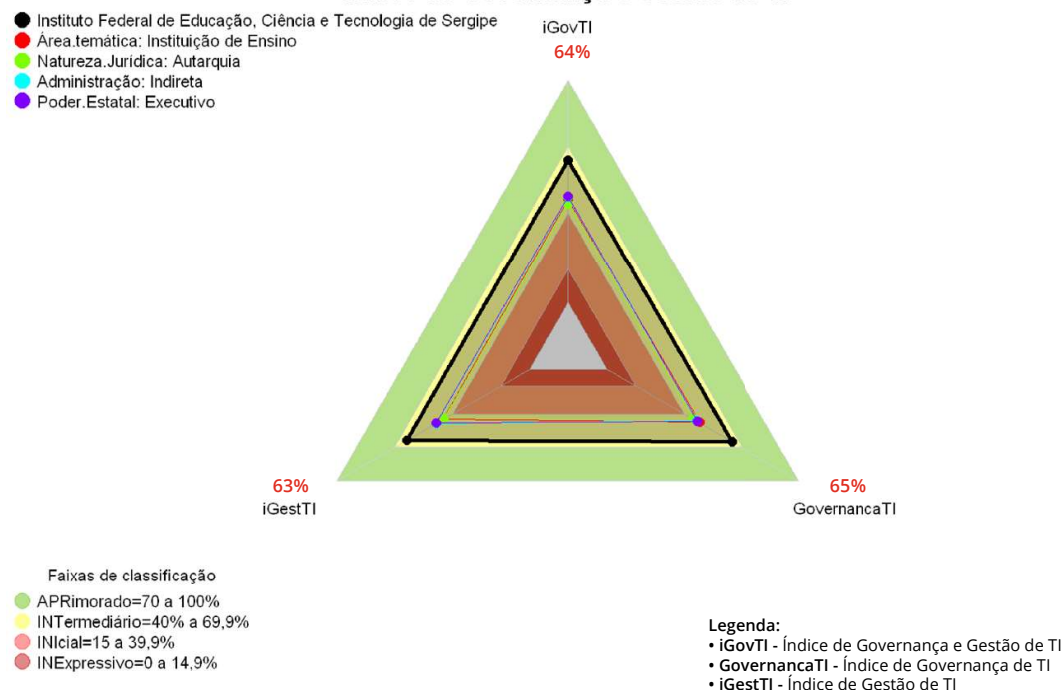


Figura 30 – Resultado para iGovTI (índice de Governança e Gestão de TI)
Fonte: Relatório Individual/Auto avaliação 2021 – IFS/TCU

Em 2021 no Levantamento de Governança e Gestão Públicas – TCU o IFS alcançou 64,21% no índice de governança e gestão de TI (iGovTI), 63,6% no índice de capacidade em gestão de TI (iGestTI) e 65% em Governança de TI (GovTI), ficando em 4º lugar (iGovTI) na Rede Federal de Educação Profissional e Tecnológica.

Mais informações: <http://www.ifs.edu.br/noticias-dti/6865-levantamentos-de-govtic-ifs-2>

O Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC 2022-2024 define como a área de TI, representada pela DTI, contribuirá para o alcance dos objetivos estratégicos.

Mais informações: <http://www.ifs.edu.br/plano-diretor-de-tecnologia-da-informacao>

Contratações mais relevantes de recursos em TI

Diante do cenário de pandemia, algumas contratações foram realizadas para dar suporte ao ensino remoto.

Planejamento da contratação de TIC - Executado Em 2021				
ID	Descrição do projeto	Ano de execução	Status	Grau de prioridade
1	Contratação de Sustentação, Suporte e Manutenção Evolutiva dos Sistemas SIG/UFRN	2021	Planejamento concluído	Alta
2	Serviços de Outsourcing de Impressão	2021	Planejamento concluído	Alta
3	Aquisição de Ativos de Rede	2021	Planejamento concluído	Alta
4	Anti-vírus Corporativo	2021	Planejamento concluído	Alta
5	Aquisição de Certificados Digitais ICP Brasil	2021	Planejamento concluído	Alta

Tabela 14 - Planejamento da contratação de TIC - Executado em 2021.
Fonte: DTI

Aquisições/Contratações efetuadas em 2021				
ID	Descrição do projeto	Ano de execução	Status	Grau de prioridade
1	Solução de Computação em Nuvem	2021	Contrato efetuado	Alta
2	Aquisição de Ativos de Rede	2021	Aquisição efetuada	Alta
3	Aquisição de Processadores de Dados	2021	Aquisição efetuada	Média

Tabela 15 - Aquisições/Contratações efetuadas em 2021.
Fonte: DTI

Pesquisa de satisfação dos chamados abertos no GLPI

Em 2021 a equipe de TI registrou chamados variando entre 227 a 348 por mês. Os índices de satisfação dos usuários foram sempre próximos de 90%, alcançando picos de 95%, o que demonstra alto nível de resolutividade dos casos.

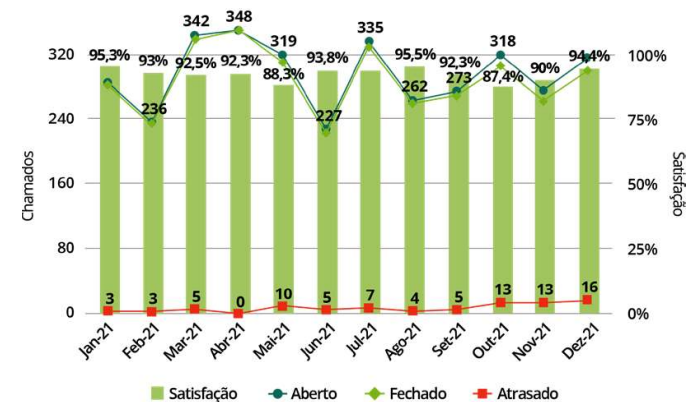


Gráfico 41 - Satisfação dos usuários com chamados abertos no GLPI
Fonte: DTI

Os principais chamados abertos no GLPI estiveram relacionados aos sistemas de informação, em seguida com redes e internet.

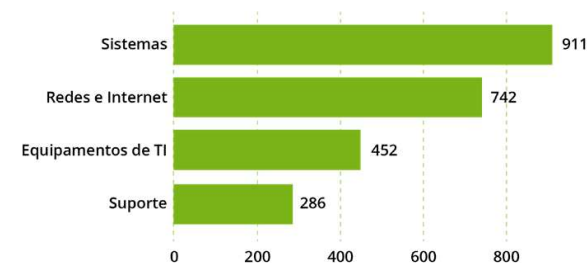


Gráfico 42 - Chamados realizados à equipe de TI.
Fonte: DTI

Os profissionais de TI do IFS foram bastante demandados em 2021, com destaque nos campi para Itabaiana, que superou 300 chamados resolvidos no exercício. Na Reitoria foram registradas 4.805 resoluções de demandas de TI em sistemas, equipamentos, suporte operacionais, redes e internet.



Gráficos 43 - Chamados resolvidos pela equipe de TI.
Fonte: DTI

Principais iniciativas (sistemas e projetos) e resultados na área de TI por cadeia de valor.

Gerenciais:

- Recriação do Comitê Gestor de TIC.
- Recriação do Comitê Gestor de Segurança da Informação e Comunicação.
- Levantamento de resultados do PDTIC.
- Elaboração do PDTIC (2022 – 2024).
- Criação do Núcleo de Banco de dados.
- Criação do Escritório de Gestão de Contratações de TIC.

Número/Ano	Ementa
030/2021	Aprova a indicação da autoridade máxima da área de TIC do IFS para atuar como Gestor do Contrato 01.2022

029/2021	Aprova a acumulação dos papéis de Fiscal Requisite e Técnico do Contrato nº 04/2020/Campus Tobias Barreto_outsourcing de impressão
028/2021	Aprova a acumulação dos papéis de Fiscal Requisite e Técnico do Contrato nº 01/2019/Campus Tobias Barreto_links dedicados de internet
027/2021	Adequa o § 3º do Art. 29 da IN SGD/ME Nº 01/2019 ao contexto institucional
026/2021	Define o cronograma de contratações de TIC exercício 2022
025/2021	Aprova a repactuação do cronograma de aquisições de TIC 2021
024/2021	Convalida a deliberação 23, que aprovou ad referendum a acumulação dos papéis de Integrante Requisite e Técnico. Observações: Convalida a Resolução nº 023/2021, de 27 de Agosto de 2020
023/2021	Aprova ad referendum a acumulação dos papéis de Integrante Requisite e Técnico Observações: Convalidada pela Resolução nº 024/2021, de 20 de Setembro de 2021.
022/2021	Aprova o Regimento Interno do CGTIC
021/2021	Aprova o termo de transição de fiscal ou gestor de contrato de TIC
020/2021	Atualiza a Política de utilização dos programas Google for Education - IN 03/2016
019/2021	Aprova a adequação do mapeamento referente à instituição da equipe de planejamento da contratação no âmbito do IFS
018/2021	Aprova a prorrogação da vigência do PDTIC 2015-2020 até dezembro de 2021
017/2021	Aprova o plano de comunicação 2021 do CGTIC
016/2021	Convalida a deliberação CGTIC nº 11 que aprova, ad referendum, o plano de dados abertos 2021-2022 Observações: Convalida a Resolução nº 011/2021, de 18 de Janeiro de 2021.

015/2021	Convalida a deliberação 10.2020 que aprova, ad referendum, o plano de transformação digital para o período 2021-2022 Observações: Convalida a Resolução nº 010/2020, de 30 de Dezembro de 2020.
014/2021	Convalida a deliberação 09.2020 que aprova, ad referendum, a inclusão no PDTIC vigente da contratação de serviço de sustentação e manutenção dos sistemas SIG-IFRN Observações: Convalida a Resolução nº 009/2020, de 23 de Dezembro de 2020.
013/2021	Aprova o Plano de comunicação do CPLanTI
012/2021	Convalida a criação do Comitê Gestor de TIC
011/2021	Aprova ad referendum o Plano de Dados Abertos - IFS 2021-2022 Observações: Convalidada POR Resolução nº 016/2021, de 5 de Fevereiro de 2021.
010/2021	Aprova, ad referendum, o Plano de Transformação Digital do IFS para o período 2021-2022. Observações: Convalidada pela Resolução nº 015/2021, de 5 de Fevereiro de 2021.

Tabela 16 - Principais iniciativas e resultados da TI
Fonte: DTI

Finalísticas:

- Melhorias no sistema de gestão acadêmica – SIGAA, a partir da implementação de novas funcionalidades e novos módulos.
- Implantação de sistema de sorteio para processo seletivo institucional não presencial.
- Sustentação e suporte de sistemas.
- Implantação do Sistemas Ágatha para gestão de riscos.
- Integração do sistema Pergamum com o LDAP (Lightweight Directory Access Protocol).
- Adesão ao serviço de nuvem para garantir disponibilidade dos nossos sistemas.
- Implantação de ambiente de produção para disponibilização do SEI – Sistema de processos eletrônicos.

Suporte/Operacional:

- Implementação e adequação de Firewalls para conter ataques cibernéticos.
- Implementação de meio para acesso remoto privativo à rede institucional.
- Atualização de softwares cruciais para mitigar vulnerabilidades.
- Reestruturação do anel óptico do campus São Cristóvão.
- Disponibilização de telefone na guarita do Campus São Cristóvão.
- Força tarefa para realização de mudança das sedes dos Campi Glória e Propriá com o objetivo de diminuir despesas.

Principais Resultados alcançados

Dentre outras, foi graças a essas iniciativas que o Instituto Federal de Sergipe foi bem-sucedido em se adaptar às condições impostas, dando segurança institucional e de recursos para que os serviços continuassem a ser prestados à sociedade.

No final do ano de 2021 foi possível iniciar um processo seletivo para novos alunos totalmente on-line, aditável e seguro, através do sistema de sorteio implantado. Além disso, o SEI – sistema de processos eletrônicos está pronto e em funcionamento, trazendo transparência, agilidade, comodidade e economia nos trâmites dos processos institucionais.

A recriação dos comitês reaproximou a alta gestão do Instituto Federal de Sergipe do ambiente operacional da TI, melhorando a comunicação entre as áreas e sincronizando as ações em busca do melhor atendimento dos objetivos institucionais.

Segurança da informação

O ano de 2021 reservou desafios no quesito Segurança da Informação. Assistimos diversos órgãos públicos e empresas sofrerem ataques cibernéticos que deixaram seus serviços de TI indisponíveis por dia, algumas tiveram que pagar resgate para conseguir reaver seus dados.

A cada dia a complexidade do ambiente do IFS aumenta devido a entrada de novos sistemas em funcionamento. Para cada sistema há um perfil personalizado para acesso.

Apesar do crescimento na quantidade de ataques sofridos, o Instituto Federal de Sergipe não sofreu nenhuma invasão nos últimos anos. Além disso, foi capaz de responder com eficiência ao surgimento de novas ameaças e fraquezas em seus sistemas.

Para mitigar os riscos e procurar problema de segurança que podem ter ocorrido é gerado um relatório mensal a fim de verificar anomalias na rede do IFS.

Avaliação de ameaças cibernéticas

Data do relatório: 25 de fevereiro de 2022 08:40
Intervalo de dados: 2022-02-18 00:00:00 2022-02-24 23:59:59 GMT-3 (FAZ local)

Sumário executivo

Ataques IPS detectados: 7.205
Aplicações de alto risco usadas: 10
Malware/botnets detectados: 4
Sites maliciosos detectados: 49

No ano passado, mais de 2.100 empresas foram violadas como resultado de más práticas de segurança interna e segurança de conteúdo latente do fornecedor. O custo médio de uma violação de segurança corporativa é estimado em US\$ 3,5 milhões e está aumentando 15% ano a ano. Invasões, malware/botnets e aplicativos maliciosos representam coletivamente um grande risco para a rede da sua empresa. Esses mecanismos de ataque podem dar aos invasores acesso aos seus arquivos e informações de banco de dados mais confidenciais. O FortiGuard Labs mitiga esses riscos fornecendo segurança de conteúdo premiada e é consistentemente classificado entre os líderes do setor por terceiros objetivos, como NSS Labs, VB 100 e AV Comparatives.

Aplicativos detectados: 303
Categoria de aplicativo principal: Network.Service
Site principal: def.dev-nano.com
Aplicativo mais usado: SSL
Sites visitados: 28138
Top Categoria da Web: Tecnologia da Informação

O uso de aplicativos do usuário e os hábitos de navegação podem não apenas ser indicativos de uso ineficiente de recursos corporativos, mas também podem indicar a falta de aplicação adequada das políticas de uso corporativo. A maioria das empresas reconhece que o uso pessoal dos recursos corporativos é aceitável. Mas há muitas áreas cinzentas nas quais as empresas devem ficar de olho, incluindo: uso de aplicativos para evitar

Figura 31 – Relatório de cyber ataques.
Fonte: DTI

Com esse relatório é possível ver quais aplicações estão sendo atacadas e que usuários estão contaminados por vírus ou por malwares. Assim, prevenindo o IFS de perda de dados, disseminação de vírus e ataque hacker que deixe o instituto inoperante.

Segurança e Prevenção de Ameaças

Aplicativos de alto risco

A equipe de pesquisa do FortiGuard atribui uma classificação de risco de 1 a 5 a um aplicativo com base nas características comportamentais do aplicativo. A classificação de risco pode ajudar os administradores a identificar rapidamente os aplicativos de alto risco e tomar uma decisão melhor sobre a política de controle de aplicativos. Os aplicativos listados abaixo receberam uma classificação de risco de 4 ou superior.

Aplicativos de alto risco

Risco	Nome da Aplicação	Categoria	Tecnologia	Do utilizador	Largura de banda	Sessão
4	Proxy.HTTP	Procuração	Protocolo de rede	78	5,90 MB	1.864
4	SurfEasy.VPN	Procuração	Servidor cliente	1	832 B	442
4	MELAS5	Procuração	Protocolo de rede	6	149,46 KB	204
4	Cloudflare.1.1.1.1.VPN	Procuração	Servidor cliente	1	20,16 KB	64
4	CryptoTab. Mineração	Interesse geral	Servidor cliente	1	285,52 KB	47
4	OKHTTP.Biblioteca.VP	Procuração	Servidor cliente	2	23,29 KB	10
N						
4	Telnet	Acesso remoto	Servidor cliente	18.524	0 B	95.551
4	Rsh	Acesso remoto	Servidor cliente	21	23,13 GB	58.982
4	TeamViewer	Acesso remoto	Servidor cliente	11	29,66 MB	19.326
4	RDP	Acesso remoto	Servidor cliente	755	566,59 MB	12.479
4	Qualquer mesa	Acesso remoto	Servidor cliente	21	22,73 MB	9.537
4	VNC	Acesso remoto	Servidor cliente	547	0 B	3.077
4	BitTorrent	P2P	Pessoa para pessoa	6	235,61 KB	489
4	Rxccc	Acesso remoto	Servidor cliente	43	0 B	164
4	Login	Acesso remoto	Servidor cliente	18	0 B	32
4	SolarWinds	Cloud.IT	Servidor cliente	1	282,31 KB	15
4	Microsoft.Quick-Assist	Acesso remoto	Servidor cliente	2	1,09 MB	4

Malware, Botnets e Spyware/Adware

Existem vários canais que os ciberdelinquentes usam para distribuir malware. Os métodos mais comuns motivam os usuários a abrir um arquivo infectado em um anexo de e-mail, baixar um arquivo infectado ou clicar em um link que leve a um site malicioso. Durante a avaliação de segurança, a Fortinet identifica vários eventos relacionados a malware e botnet que indicam downloads de arquivos maliciosos ou conexões a sites de comando e controle de botnet.

Principais malwares, botnets e spyware/adware detectados

Nome do malware	Tipo	Inserção	Vítima	Fonte	Contar
Murai.Botnet	Vírus	HTTP	7	81	97
Bladabini.Botnet	Vírus	HTTPS	6	1	13
GHbt.Rat.Botnet	Vírus	HTTP	5	1	8

Dispositivos e hosts em risco

Com base nos tipos de atividade exibidos por um host individual, podemos aproximar a confiabilidade de cada cliente individual. Essa reputação do cliente é baseada em fatores-chave, como sites navegados, aplicativos usados e destinos de entrada/saída utilizados. Por fim, podemos criar uma pontuação geral de ameaças observando a atividade agregada usada por cada host individual.

A maioria dos dispositivos e hosts em risco

Dispositivo	Pontuação
hpsps.ifs.edu.br	65.099.050
172.20.0.42	54.384.520
172.28.16.114	26.656.410
10.61.0.67	24.861.025
192.168.70.3	16.362.670
10.63.0.2	14.923.920
10.71.0.12	13.049.810
TERMINO	12.772.530
MALA	12.266.055
TÁLIA	12.033.000

Figura 32 - Segurança e prevenção de ameaças.
Fonte: DTI