



# GESTÃO DE RISCOS COM BASE NO MONITORAMENTO DE AMEAÇAS

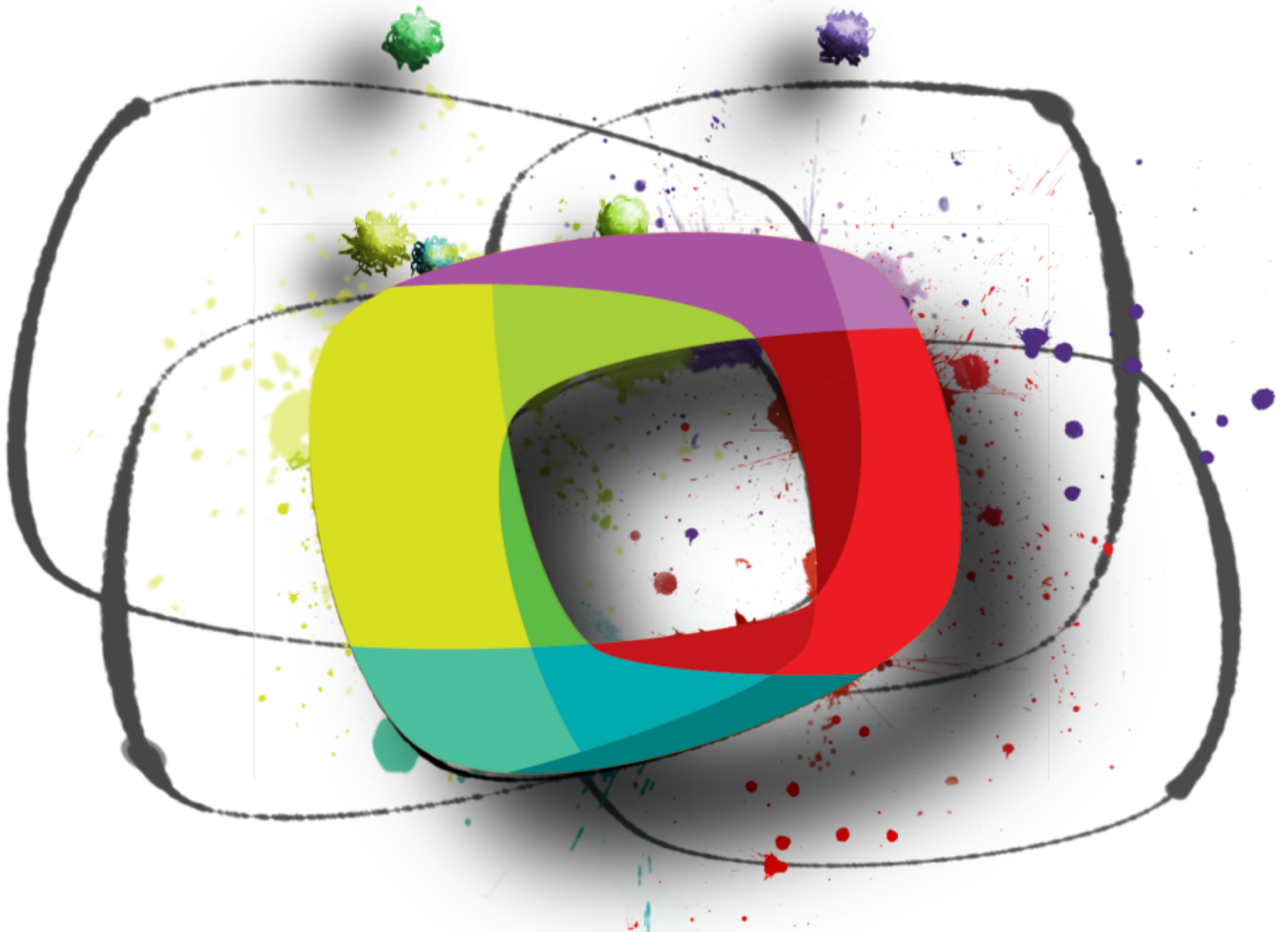
**Leandro Bennaton**

✉ [leandro.bennaton@corp.terra.com.br](mailto:leandro.bennaton@corp.terra.com.br)

Twitter: @bennaton

**Carlos H. Borella Jr.**

✉ [carlos.borella@corp.terra.com.br](mailto:carlos.borella@corp.terra.com.br)



# LEANDRO BENNATON

- Chief Security Officer responsável por Segurança e Conformidade de sistemas para LatAm, USA e Espanha na empresa **TERRA**
- Chief Security Ambassador na **ELEVEN PATHS**

Pós-Graduado em Gerenciamento de Segurança da Informação

Palestrante internacional de Segurança

Atuação nos grupos de trabalho de:

AntiSpam, Qualidade da Banda Larga e IPv6 conduzidos pelo Comitê Gestor Internet Brasil.



# CARLOS H. BORELLA JR.

- Security & Compliance Consultant responsável pelas avaliações de Segurança Tecnológica, Auditoria e Compliance para Latino América, Estados Unidos e Espanha na empresa **TERRA**

Pós-Graduado em Segurança da Informação e MBA em Gestão de Tecnologia

Certificações Internacionais:

CISSP, CISA, BS Lead Auditor (ISO/IEC 27001)





Criado em 1999, o **Terra** é referências em conteúdo digital em países de **língua hispânica e portuguesa**



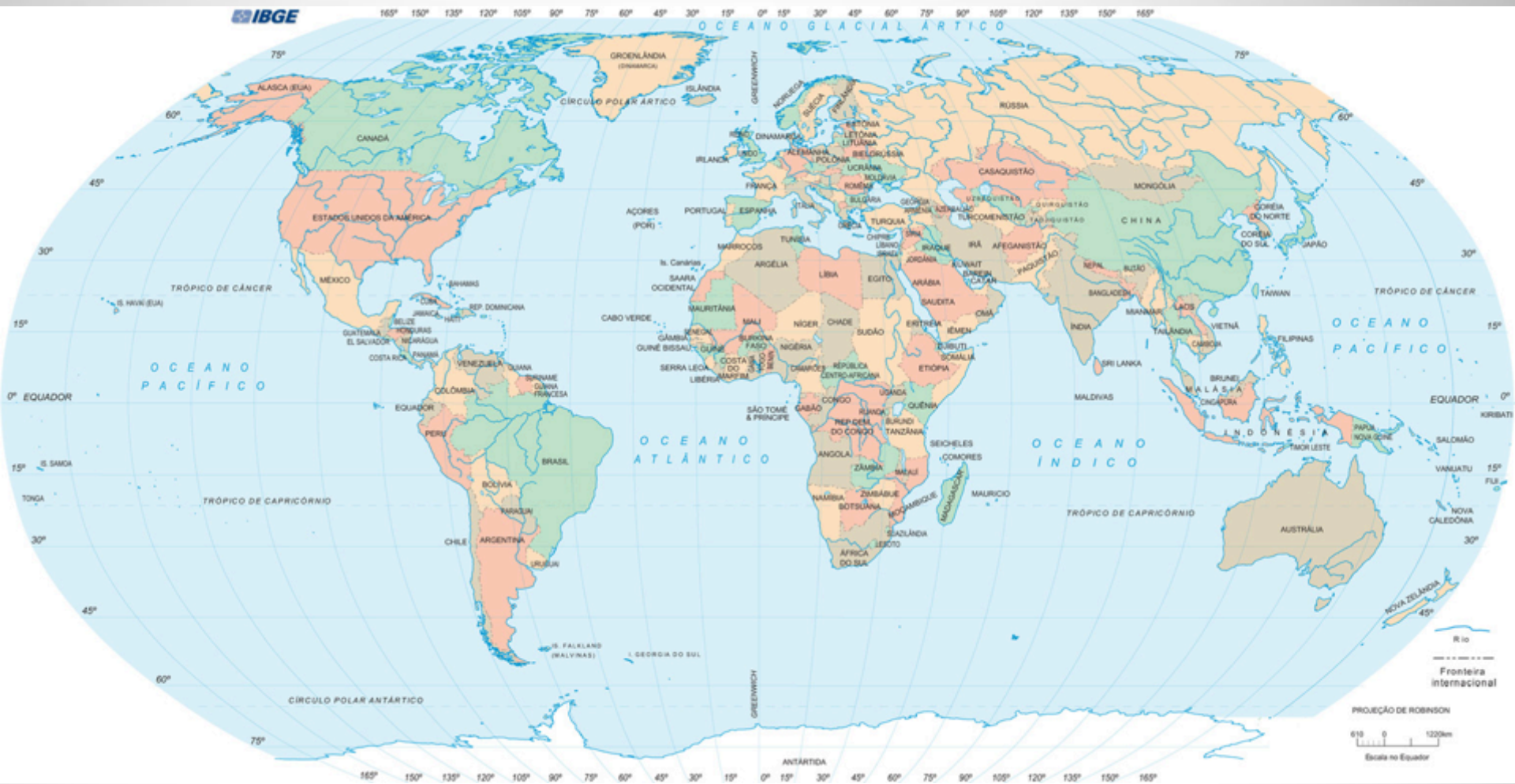
Além dos **17 países** da América Latina, está presente nos **Estados Unidos e Espanha**



# ATUAÇÃO – SECURITY & COMPLIANCE



terra



Equipe **GLOBAL** com sede em SP, responsável por Argentina, **Brasil**, Chile, Colômbia, **Estados Unidos**, **Espanha**, México e Peru

# ATIVIDADES – SECURITY & COMPLIANCE

- Requerimentos Legais**
- Controle de Acesso**
- Auditoria e Conformidade**
- Segurança Física**
- Gestão de Incidentes**
- Fraudes**
- Segurança Tecnológica**
- Políticas & Normas**
- Conscientização**
- Proteção da Marca**





# Segurança

Atenção a postura!

Esta área deve ser  
**consultiva!**



# AGENDA

- **Desafios**
- **Ambiente**
- **Metodologia**
  - **Análise de Vulnerabilidades**
  - **Aplicações**
  - **Classificação Criticidade**
- **Projeto → Processo**
- **Gestão de Riscos**
- **Resultados**
- **Monitoramento**



# CHALLENGES



terra

# TRANSMISSÕES AO VIVO



infernal broadcast

LONDON 2012  
de 27 de julho a 12 de agosto

Agenda | Top Atletas no Twitter | Esportes | Games | Mapa de Medalhas | Momentos Inesquecíveis

notícias | fotos | vídeos

## VÍDEOS

### Estádio Olímpico

02 de maio de 2012 - 19h13

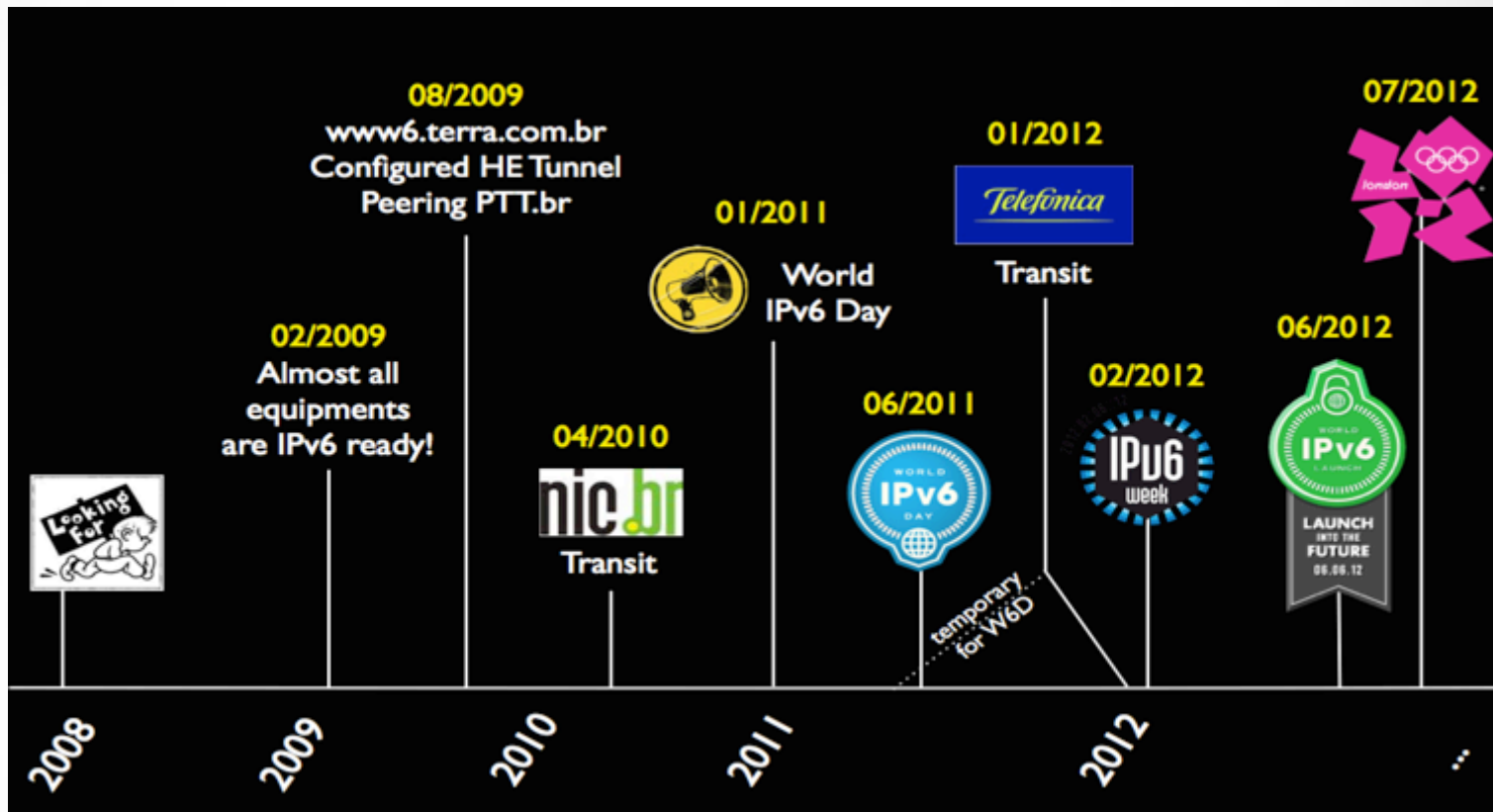
Viaje pelas arenas dos Jogos Olímpicos de Londres

#### próximos vídeos

- Atletas olímpicos treinam em novo ginásio: veja
- Parque Olímpico é aberto ao público para evento teste
- Vídeo com mascotes olímpicos tem animação de atleta amputado
- Assistindo: Viaje pelas arenas dos Jogos Olímpicos de Londres
- Proprietários colocam inquilinos na rua por lucro em Olimpíada
- Após ter vaga



# IMPLEMENTAÇÃO IPV6



**For better security, think like a bad guy**



terra

# superfície ataques



Contas de E-mails (*spammers*)



*E-commerce* (cartões de créditos)



Base de Clientes (informações cadastrais)



Visibilidade e Abrangência (volume de acesso)



Hospedagem (*fake pages*)



# AMBIENTE

- ❑ 268.000 endereços IPs válidos (Internet)
- ❑ 101.000 endereços internos (backnet e ambiente corporativo)
- ❑ 280 aplicações web (próprias e de parceiros de conteúdo)
- ❑ 3 datacenters/ 10 escritórios (Global)





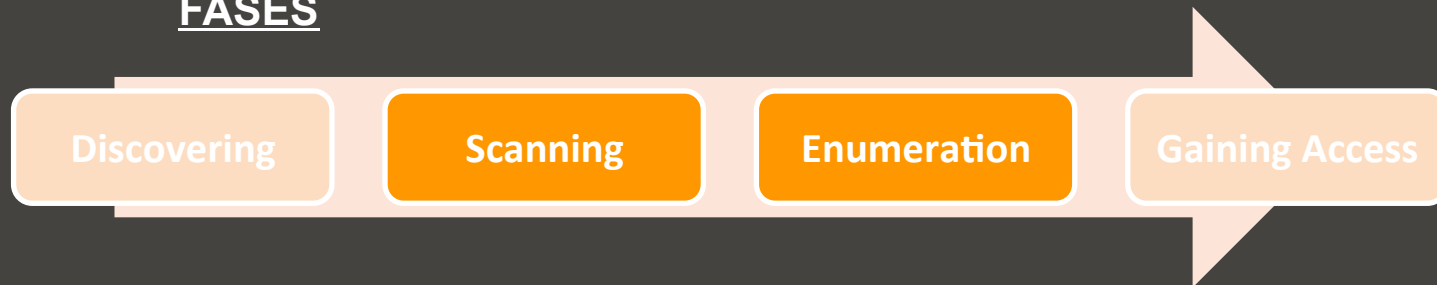


# METODOLOGIA – Análise de Vulnerabilidades

## GreyBox

Utilização de credenciais legítimas, visando a validação das permissões de acesso e autorização estão em conformidade com as necessidades de negócio.

### FASES



- Destaque para as fases de Scanning e Enumeration;
- No geral, a fase de Gaining Access, é realizada em aplicações onde há a necessidade de comprovar o impacto de vulnerabilidades críticas.

# METODOLOGIA - Aplicações

## ❑ Testes realizados com base nos 66 controles apresentados pelo OWASP TESTING GUIDE (v3.0):

- Information Gathering
- Configuration Management Testing
- Business Logic Testing
- Authentication Testing
- Authorization testing
- Session Management Testing
- Data Validation Testing
- Denial of Service Testing
- Web Services Testing
- Ajax Testing

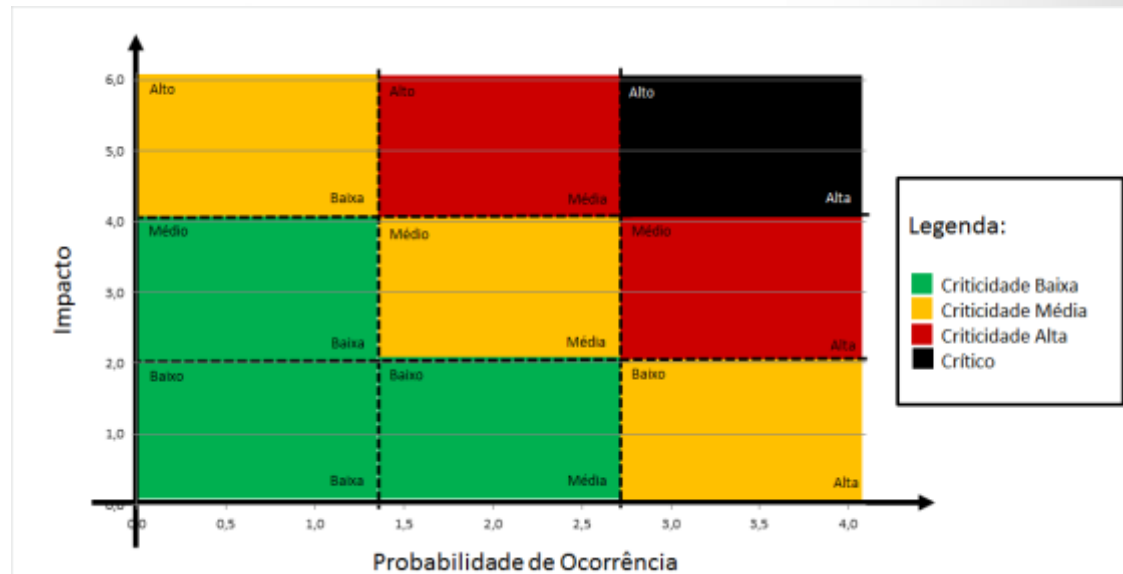


# METODOLOGIA – Classificação Criticidade

## Calculadora CVSS2

Probabilidade de Ocorrência	Vetor de Acesso	Remoto	4,0
	Complexidade de Acesso	Baixa	
	Autenticação	Nenhuma	
Impacto	Confidencialidade	Completa	6,0
	Integridade	Completa	
	Disponibilidade	Completa	
BASE SCORE		10,0	

Fator de Risco/Criticidade	
0.0	Nenhum
0.1 - 3.9	Baixo
4.0 - 6.9	Médio
7.0 - 9.9	Alto
10.0	Crítico



# ameaças vulnerabilidades

conhecidas



desconhecidas



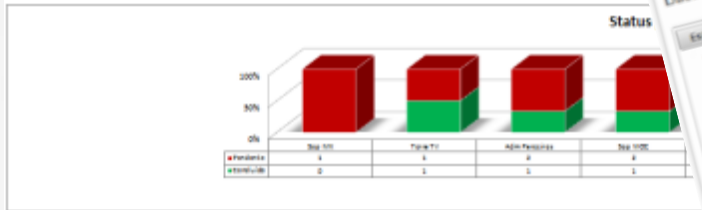
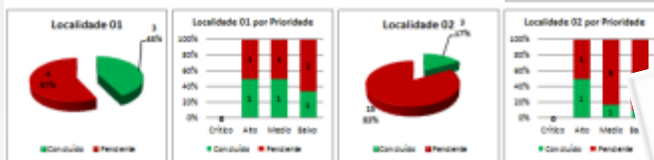
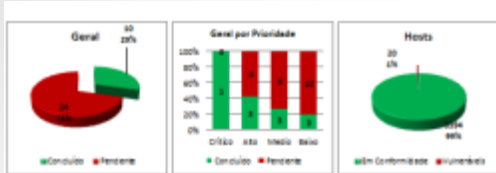
terra

# PROJETO → PROCESSO

- ❑ Projeto em fases  
(Externo, Interno e Aplicações)
- ❑ Cronograma e Comunicação
- ❑ Reporte executivos com informações relevantes
- ❑ Plataforma Web, em real time



# PROJETO → PROCESSO



Parâmetro	ID	Prioridade	Vulnerabilidade	Data	EE	Localização	Empres	Status
Resposta	4437cp	0	O servidor está disponibilizando acesso a console administrativa.	2011-01-01	E	Porto Alegre		Concluído
Acesso	4437cp	0	O servidor está disponibilizando acesso a console administrativa.	2011-01-01	E	Porto Alegre		Concluído
Ignorada	4437cp	0	O servidor está disponibilizando acesso a console administrativa.	2011-01-01	E	Porto Alegre		Concluído
Outros	4437cp	0	O servidor está disponibilizando acesso a console administrativa.	2011-01-01	E	Porto Alegre		Concluído
4	200 streamund0	4437cp	O servidor está disponibilizando acesso a console administrativa.	2011-01-01	C	Porto Alegre		Concluído
6	200 streamund0	4437cp	O servidor está disponibilizando acesso a console administrativa.	2011-01-01	C	Porto Alegre		Concluído
6	200 streamund1	4437cp	O servidor está disponibilizando acesso a console administrativa.	2011-01-01	C	Porto Alegre		Concluído
7	200 streamund0	4437cp	O servidor está disponibilizando acesso a console administrativa.	2011-01-01	C	Porto Alegre		Concluído
8	200 streamund0	80cp	Resolução de pacotes de atualização para o PHP	2011-01-01	E	Porto Alegre		Concluído
9	200 streamund0	80cp	Resolução de pacotes de atualização para o Apache	2011-01-01	E	Porto Alegre		Concluído
10	200 streamund0	35cp	O servidor de e-mail (MTA) está com a funcionalidade de relaying de e-mail habilitada	2011-01-01	E	Porto Alegre		Concluído
11	200 streamund0	74cp	O servidor de e-mail (MTA) está com a funcionalidade de relaying de e-mail habilitada	2011-01-01	E	Porto Alegre		Concluído

# PROJETO → PROCESSO

Ponto 03	Os servidores web estão suscetíveis a uma vulnerabilidade no cabeçalho Range e Request-Range devido à utilização de uma versão desatualizada do Apache.		
Criticidade Alta			
IP da Máquina/ Nome da Máquina			
Impacto	Alto	Probabilidade	Alta
Recomendação	Atualizar o Apache para a versão 2.2.21 ou superior. Adicionalmente, é possível realizar algumas configurações alternativas, até que o servidor seja atualizado, conforme referência abaixo:  <a href="http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3C20110826103531.998348F82@minotaur.apache.org%3E">http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3C20110826103531.998348F82@minotaur.apache.org%3E</a>		
Referências	CVE: CVE-2011-3192		
<p>Os servidores web estão utilizando versões do Apache anterior à 2.2.20, as quais estão suscetíveis a ataques de DoS (Denial of Service) devido uma vulnerabilidade na forma como o Apache manipula o cabeçalho HTTP.</p> <p>Esta vulnerabilidade permite que um atacante realize uma série de requisições com sobreposição de intervalos no cabeçalho HTTP (mais especificamente no cabeçalho Range ou Request-Range) resultando em uma sobrecarga no consumo de CPU e de memória, causando assim a paralisação do serviço. Já há um exploit publicado, além de terem sido notificados ataques, ao redor do mundo, que exploram esta vulnerabilidade.</p>			

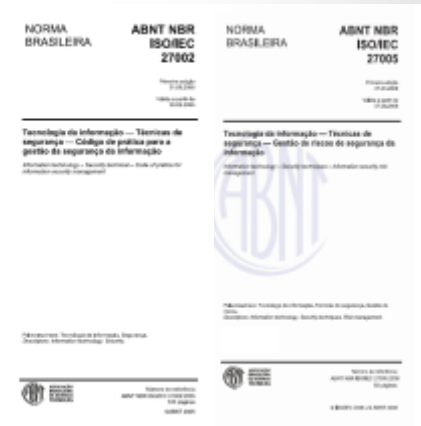
Ponto 01	As aplicações encontram-se vulneráveis a <i>Blind SQL Injection</i> .		
Crítico			
Site/ URL			
Impacto	Alto	Probabilidade	Alta
Recomendação	Evitar o uso de interpretadores externos sempre que possível, aproveitando que diversos <i>shell commands</i> e alguns <i>system calls</i> existam em bibliotecas específicas de linguagem que executam as mesmas funções sem envolver o interpretador de Shell do sistema operacional, e consequentemente, evita os riscos relacionados com o uso deste processo. Quando não for possível evitar o uso de interpretadores (ex. chamadas para <i>backend databases</i> ), é fundamental validar os dados para garantir que não existe nenhum argumento malicioso que possa ser processado. Outra opção recomendada é a estruturação de requisições de forma a garantir que os parâmetros fornecidos são tratados como dados, ao invés de conteúdo executável, o que não elimina, mas reduz significativamente a possibilidade de ocorrência destas vulnerabilidades.		
Referência	<a href="http://www.owasp.org/index.php/Blind_SQL_Injection">http://www.owasp.org/index.php/Blind_SQL_Injection</a> <a href="http://www.owasp.org/index.php/Guide_to_SQL_Injection">http://www.owasp.org/index.php/Guide_to_SQL_Injection</a> <a href="http://www.owasp.org/index.php/Reviewing_Code_for_SQL_Injection">http://www.owasp.org/index.php/Reviewing_Code_for_SQL_Injection</a>		
<p>A aplicação analisada está vulnerável a <i>Blind SQL Injection</i>. O SQL é a linguagem usada por bancos de dados para realizar consultas e alterar dados. Esta vulnerabilidade ocorre devido à possibilidade de um atacante inserir uma série de instruções SQL dentro de uma consulta (<i>query</i>) através da manipulação das entradas de dados de uma aplicação. Um usuário mal-intencionado pode explorar esta vulnerabilidade de <i>SQL Injection</i> para alterar de forma maliciosa os comandos que são passados ao banco de dados, com isso, é possível ler ou alterar dados que normalmente não poderiam ser lidos e alterados.</p> <p>Abaixo listamos os formulários vulneráveis a <i>Injection</i>:</p> <p><a href="#">/novosite/categoriadades.cfm</a>  <a href="#">/novosite/detail.cfm</a>  <a href="#">/novosite/galerianova.cfm</a>  <a href="#">/novosite/postnew.cfm</a>  <a href="#">/novosite/reservas_p1.cfm</a></p> <p>Foram realizados ataques automatizados e manuais visando à extração de informações sensíveis do banco de dados que suporta a aplicação.</p> <p>O primeiro passo foi levantar os nomes das tabelas existentes e, em seguida, consultar os dados de algumas tabelas, conforme ilustramos a seguir:</p>			





# GESTÃO de RISCOS

- ❑ Transformar o “techniques” em linguagem de negócio
- ❑ Apoio do CEO, CTO, direção
- ❑ Maior envolvimento de áreas de Tecnologia
- ❑ Métricas, Indicadores do PLR
- ❑ Mapa de Riscos Tecnológicos (atualização Trimestral/ reunião Semestral)



# GESTÃO de RISCOS

[CONFIDENCIAL] - Relatório de Ar

[CONFIDENCIAL] - Relatório de Análise de Riscos



## 4. DETALHAMENTO DA ANÁLISE DE RISCO

### 1. Excessivo número de ativos disponíveis

#### Situação Atual

Durante as análises externas de vulnerabilidades de In ativos (hosts) com algum tipo de serviço de acesso remoto qualquer computador na Internet.

#### Riscos

O acesso remoto através da Internet pode permitir, por e autorizados, realizados via ataques de força bruta, expor outras situações.

Adicionalmente, é importante destacar que em alguns ca controle criptográfico, ou seja, todo o tráfego de informaç são transmitidas em texto puro, podendo ser capturadas há a interceptação dos dados trafegados.

#### Recomendações

Recomenda-se a restrição do acesso aos serviços de ac de acordo com as melhores práticas de Segurança.

Para os casos onde é necessário acessar remotamente e de acesso remoto (VPN).

#### Risco ISO/IEC 27001:2005

- 11.5 - Ineficiência na prevenção de acesso não z

#### Comentário da Diretoria

Plano de Ação:	
Responsáveis:	
Data Prevista de Correção:	
Complexidade de Implementação:	
Aquisição de Solução:	

### 6. Fragilidades no processo de manutenção e atualização de patch dos recursos de processamento de informação

#### Situação Atual

Foi identificado um alto número de vulnerabilidades relacionadas a desatualização e/ ou pendências de instalação de patches de atualização nos recursos de processamento de informação durante os trabalhos de análises externas de vulnerabilidades de infraestrutura.

#### Riscos

A falta de tempestividade na aplicação dos patches e/ ou na atualização de versão dos recursos de processamento de informação potencializa o risco de exploração de vulnerabilidades, podendo permitir, por exemplo, acesso aos recursos de maneira não autorizada, execução de comandos arbitrários, obtenção de informações sensíveis, entre outros.

Adicionalmente vale destacar que vulnerabilidades que apresentam como causa raiz a desatualização de patch, em sua grande maioria caso exploradas, apresentam um alto impacto a todo ambiente.

#### Recomendações

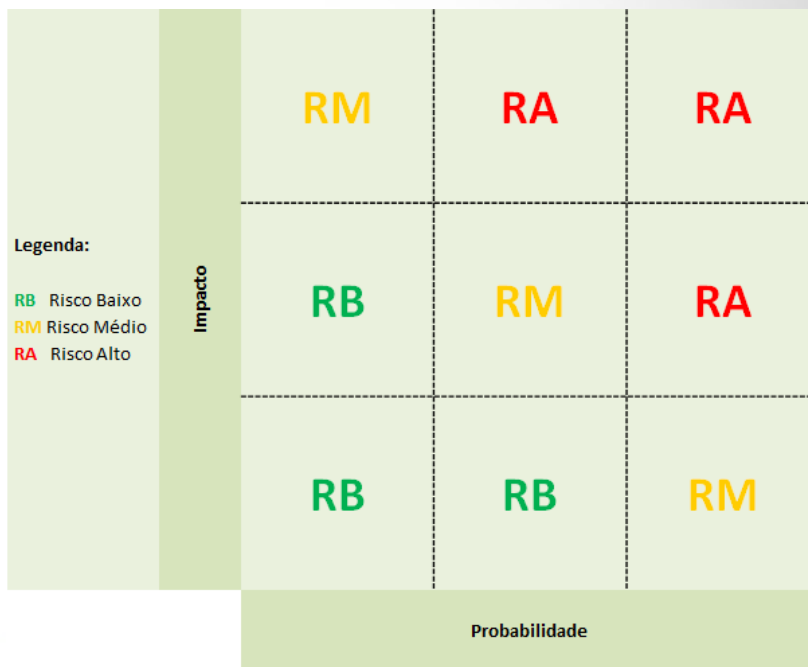
Implementar um processo para Gestão de Correções e Atualizações (Patches), visando realizar as correções e atualizações dos recursos de processamento de informação assim que houver a disponibilização do patch por parte do fornecedor ou quando uma vulnerabilidade no recurso for mapeada pela SI.

#### Risco ISO/IEC 27001:2005

- 12.6 - Ineficiência na redução dos riscos resultantes da exploração de vulnerabilidades técnicas que tenham sido publicadas.

#### Comentários da Diretoria

Plano de Ação:	
Responsáveis:	
Data Prevista de Correção:	
Complexidade de Implementação:	
Aquisição de Solução:	



Telefônica

seguranca.informacao@telefonica

seguranca.informacao@corp.terra.com.br

terra



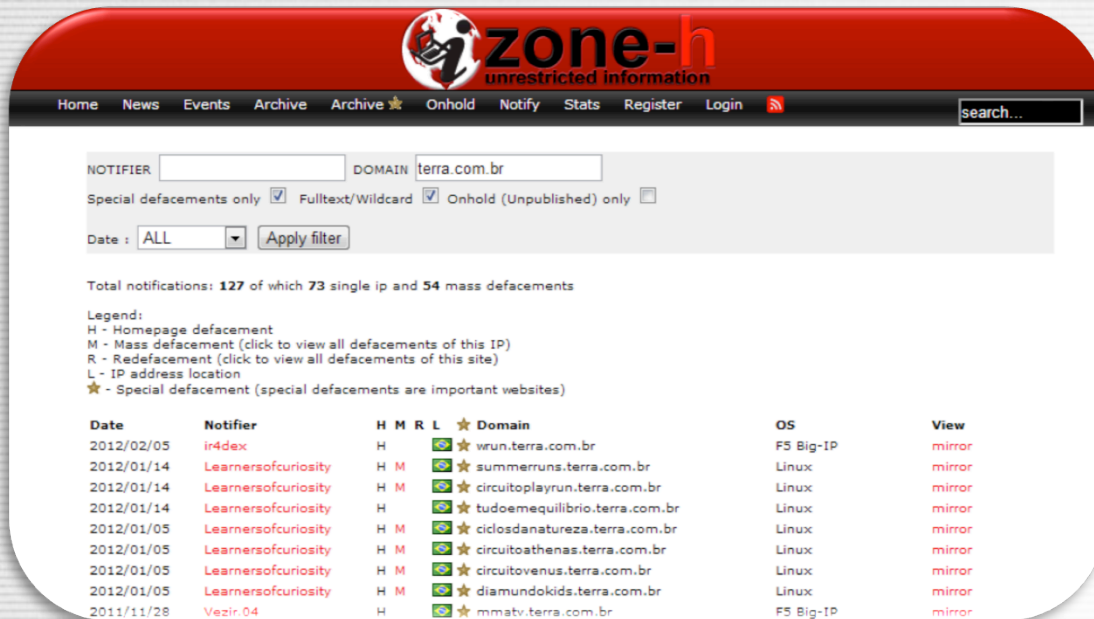
# RESULTADOS

- ✓ +11.000 vulnerabilidades tratadas
- ✓ Melhor nível de proteção
- ✓ Não há *defacement* desde mar/12
- ✓ Percepção dos executivos da importância de SI e Governança
- ✓ Aumento da maturidade e cultura da Segurança da Informação



# MONITORAMENTO

## Defacements



zone-h  
unrestricted information

Home News Events Archive Archive ★ Onhold Notify Stats Register Login

NOTIFIER  DOMAIN

Special defacements only  Fulltext/Wildcard  Onhold (Unpublished) only

Date :

Total notifications: **127** of which **73** single ip and **54** mass defacements

Legend:  
H - Homepage defacement  
M - Mass defacement (click to view all defacements of this IP)  
R - Redefacement (click to view all defacements of this site)  
L - IP address location  
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★ Domain	OS	View
2012/02/05	ir4dex	H				★ wrun.terra.com.br	F5 Big-IP	mirror
2012/01/14	Learnersofcuriosity	H	M			★ summerruns.terra.com.br	Linux	mirror
2012/01/14	Learnersofcuriosity	H	M			★ circuitoplayrun.terra.com.br	Linux	mirror
2012/01/14	Learnersofcuriosity	H				★ tudoemequilibrio.terra.com.br	Linux	mirror
2012/01/05	Learnersofcuriosity	H	M			★ ciclosdanatureza.terra.com.br	Linux	mirror
2012/01/05	Learnersofcuriosity	H	M			★ circuitoathenas.terra.com.br	Linux	mirror
2012/01/05	Learnersofcuriosity	H	M			★ circuitovenus.terra.com.br	Linux	mirror
2012/01/05	Learnersofcuriosity	H	M			★ diamundokids.terra.com.br	Linux	mirror
2011/11/28	Veziir.04	H				★ mmstv.terra.com.br	F5 Big-IP	mirror

Acompanhar notificação  
de domínios  
vítimas de Defacement

Atenção especial aos Parceiros de Conteúdo,  
foco na autopromoção de grupos *hackers*



# MONITORAMENTO

## Malwares

**stop badware**

### Search Badware Website Clearinghouse

To locate a website, enter the site's URL (for example: "your-website.com") into the box below and click "Search Clearinghouse." For best results, do not include prefixes such as "http://www."

Results will be displayed below. Clicking on the search result will not take you to the displayed link, but will take you to a dynamically-generated page that will show you information about the site.

If you are the administrator of a website on this list, you can ask StopBadware to review the inclusion of your site in the Badware Website Clearinghouse through our Request for Review process. For more information, please see our FAQ.

Website URL:

You searched for items containing the term "www.terra.es" there are 54 results.

Status	Report
<input type="radio"/>	www.terra.es/personal/guassimof
<input type="radio"/>	www.terra.es/personal/yahor
<input type="radio"/>	www.terra.es/personal/5imgogipe/
<input type="radio"/>	www.terra.es/personal/0tp2000/
<input type="radio"/>	www.terra.es/personal/0faccosr/
<input type="radio"/>	www.terra.es/personal/0fbrctsr/
<input type="radio"/>	www.terra.es/personal/0famonosr/
<input type="radio"/>	www.terra.es/personal/0focasdr/
<input type="radio"/>	www.terra.es/personal/0fmafo.castane/
<input type="radio"/>	www.terra.es/personal/0fduccsr/
<input type="radio"/>	www.terra.es/personal/0fmonjcs/
<input type="radio"/>	www.terra.es/personal/0f5enpmr/
<input type="radio"/>	www.terra.es/personal/0fcamagpr/
<input type="radio"/>	terra.es/

Acompanhar notificação

domínios do Terra

relacionados a *Malwares*

Grande desafio no mapeamento e identificação, nos casos onde o *malware* ou problema está na Publicidade.

# MONITORAMENTO

**From:** "ctir@ctir.gov.br" <ctir@ctir.gov.br>  
**Subject:** [CTIR Gov BR #57256] SMTP Abuse [parc-smtp02-tna-mia.terra.com|208.84.247.225]  
**Date:** February 27, 2014 at 11:00:02 AM GMT-3  
**To:** "abuse@terra.com" <abuse@terra.com>, "Eng. Redes" <eng.redes@corp.terra.com.br>  
**Cc:** "soc@us-cert.gov" <soc@us-cert.gov>

Manager,

After analyzing incident (Phishing), we've detected that:

1. A machine with the IP address [208.84.247.225] probably hosts/relays a phishing message (see below).
2. We kindly request you to verify this occurrence since this machine could be compromised or abused.
3. This message was sent to the network's registered technical, administrative and contact, but if you are not

## Abuse

CTIR

CSIRT

Serviços

**Trojan Detected – Please Shut Down! – [ATS #11019] – IP: 177.53.152.51 Domain: n...**

RSA Anti-Fraud Command Center

Sent: quarta-feira, 3 de outubro de 2012 07:02

To: Terra – Abuse

Cc: Leandro Bennaton

[ATS ID - 11019]

PayPal 5146.2

Dear Team, Please be advised that it is likely an empty page will appear when accessing the URL below. The resource under this URL is used by machines infected with a Trojan. The content is designed to remain undetected, thus an empty page or a fake error message may appear. Please take the necessary steps in order to disable this fraudulent URL. We appreciate your cooperation. RSA Security – Anti Trojan Team

# CSIRT

## Cenários

---

### **Crimes eletrônicos**

Quando recebemos um requerimento de autoridade pública para investigar um assinante ou usuário do portal.

### **Alvo dos ataques**

Portal sofre tentativas de invasão, fraudes, roubo de informações, DDoS, port scan, etc.

---



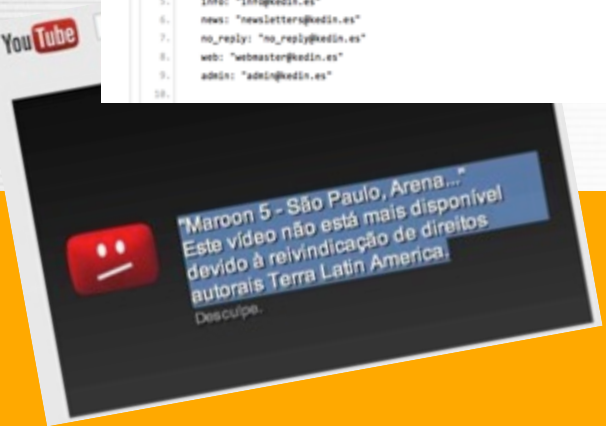
terra



# MONITORAMENTO

Marca

Brand Protection  
Acompanhar a marca  
(Pastebin, Youtube, etc)



# MONITORAMENTO

Marca

[nokterra.com](http://nokterra.com)

Ativo - 200 - OK

[positivterraceapartmentbarcelona.com](http://positivterraceapartmentbarcelona.com)

Inativo - 404 - Not Found

[puidukodafranceterrasses.com](http://puidukodafranceterrasses.com)

Inativo - 404 - Not Found

[rhterra.com](http://rhterra.com)

Inativo - Connection Error

[rousselet-terrassement.com](http://rousselet-terrassement.com)

Ativo - 301 - Moved Permanently

[sonorachemical.com](http://sonorachemical.com)

Ativo - 200 - OK

[sonorataxhelp.com](http://sonorataxhelp.com)

Ativo - 200 - OK

[superterradox.com](http://superterradox.com)

Ativo - 200 - OK

[terra-studios.com](http://terra-studios.com)

Ativo - 200 - OK

[terraptura.com](http://terraptura.com)

Ativo - 200 - OK

[terracecentralapartmentbarcelona.com](http://terracecentralapartmentbarcelona.com)

Inativo - 404 - Not Found

[terraxis.com](http://terraxis.com)

Ativo - 200 - OK

[terradiciclismo.com](http://terradiciclismo.com)

Ativo - 200 - OK

[terrdomis.com](http://terrdomis.com)

Inativo - Connection Error



terra

# STRATEGY PROCES



terra



terra

# segurança da informação



**Leandro Bennaton** 

✉ leandro.bennaton@corp.terra.com.br  
@bennaton

**Carlos Borella** 

✉ carlos.borella@corp.terra.com.br

# Obrigado!



terra