LusNIC Associação de ccTLDs de língua portuguesa

Coalition for Digital Africa

ICANN

Formação LusNIC:
Sessão Prática de Cibersegurança

Ricardo Pires, .PT
Coordenador de Cibersegurança

27.03.2026

Agenda

- **9:00 - 10:30** - Boas práticas e requisitos de segurança na gestão e operação de um ccTLD
- **10:30 – 10:45** – Pausa
- **10:45 - 12:30** - Exercício prático: Anatomia de uma fuga de informação (CTF)

Quem somos

- Registry do .pt, domínio de topo de Portugal
- Dinamizar e promover a utilização da internet a nível nacional
- Player nacional na capacitação e inclusão digital de pessoas e organizações
- Segurança e confiança no .pt

Contexto

O que é um ccTLDs?

Um ccTLD é um tipo de domínio de topo que representa um país específico. É como um "sobrenome" online que indica a origem geográfica de um site

Os TLDs são classificados geralmente por:

- gTLD: Tais como .com; .org ou .amazon.
- ccTLD: Country Code Top Level Domain como é o .pt.

Ecossistema DNS

Registo de domínio

Registrants

Quer registar domínio

Registrars

Verificação de disponibilidade e registo

TLD Registry

Base de dados do Registry

Resolução de domínio

Utilizador visita o domínio

Servidores de resolução de nomes

Servidores de nomes

Centro de Operações de Segurança

O Centro de Operações de Segurança do .PT – **PTSOC** – encerra dois grandes objetivos na sua atuação:

Acelerar e aprofundar internamente as capacidades de **deteção**, **resposta** e **prevenção** de incidentes de segurança e ameaças cibernéticas, dotando o .PT dos meios tecnológicos, processuais e humanos necessários à proteção da sua infraestrutura e serviços críticos

Densificar os níveis de **cooperação** com os nossos parceiros, nomeadamente no contexto do ecossistema da gestão dos nomes de domínio

RJC: entidade essencial do setor das infraestruturas digitais

- Registries são classificados **entidades essenciais**
- Obrigações para uma entidade essencial (art.27.º):

  - Políticas de gestão do risco
  - Gestão dos incidentes
  - Continuidade de negócio
  - Segurança da cadeia de fornecimento
  - Segurança na aquisição e desenvolvimento
  - Formação e sensibilização de práticas básicas de ciberhigiene
  - Políticas relativas a criptografia
  - Segurança dos recursos humanos (controlos de acesso)
  - Uso de tecnologias de multi fator de autenticação

Gestão dos riscos

- **Passo 1:** Identificar os ativos
- **Passo 2:** Identificar as ameaças
- **Passo 3:** Avaliar os riscos
- **Passo 4:** Implementar controlos
- **Passo 5:** Monitorizar

Identificar os ativos

- Um **ativo** é algo que **tem valor para a organização** e que, portanto, requer **proteção** na ótica da mesma

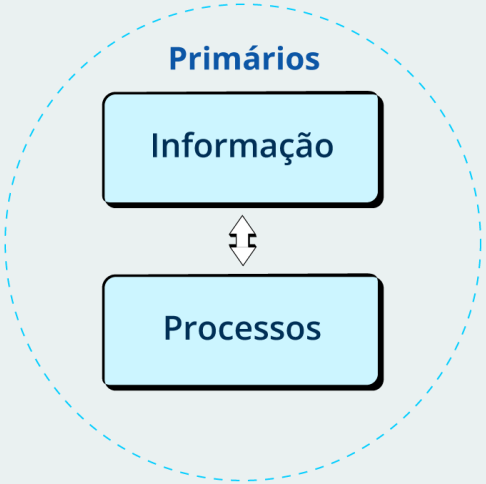
- No âmbito do Regime Jurídico da Segurança do Ciberespaço, classifica-se como ativo:

"todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos (aplicações e plataformas de software) considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços"

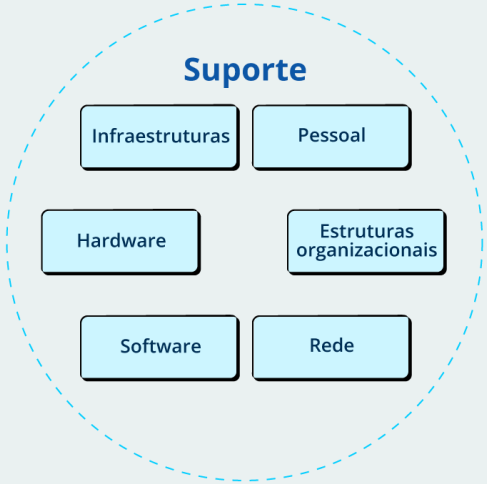
Identificar os ativos

Podemos dividir os ativos em:

Ativos primários:



Ativos de suporte:



Catálogo de ameaças

Donos dos ativos

Colaboradores

Áreas corporativas
(RH, legal, infraestruturas, ...)

Especialistas
(cibersegurança, segurança física,...)

Autoridades governamentais e/ou legais

Parceiros

Autoridades meteorológicas

Catálogos de ameaças

Histórico de avaliações de ameaças

Histórico de incidentes

Ameaças de segurança a um ccTLD

#1

Acesso não autorizado a informações

#2

Obtenção de credenciais

#3

Ransomware

#4

Registo de nomes de domínio fraudulentos

#5

Phishing/Smishing

Ameaças cibernéticas a um ccTLD

Acesso não autorizado a informações:

Os cibercriminosos têm como objetivo exfiltrar informação pessoal dos titulares de domínios presentes nos sistemas de gestão de um ccTLD. Isto pode incluir:

- Nomes
- Endereços de morada
- Endereços de e-mail
- Detalhes dos cartões de crédito
- Dados de Negócio

Ameaças cibernéticas a um ccTLD

Obtenção de Credenciais:

Os cibercriminosos tentam adquirir credenciais de utilizadores internos de forma a obterem acesso ao sistema de gestão do ccTLD. As principais ameaças são:

- **Spear Phishing:** Ataques direcionados a funcionários através de emails falsos
- **Ataques de brute-force:** Tentativas sistemáticas de adivinhar passwords
- **Reutilização de passwords:** Aumenta o risco de comprometimento de contas

Ameaças cibernéticas a um ccTLD

Ransomware:

Os cibercriminosos podem encriptar a infraestrutura do registo de ccTLDs, exigindo um resgate para fornecer chaves de desencriptação. Isto pode causar interrupções significativas nos serviços prestados pelo registo de nomes de domínio dos ccTLDs

Ameaças cibernéticas a um ccTLD

Registo de nomes de domínio fraudulentos:

Os cibercriminosos criam versões falsas ou semelhantes de domínios existentes para se fazerem passar pelos domínios legítimos. Isso pode incluir a criação de websites maliciosos que imitam sites legítimos, frequentemente utilizados em ataques de phishing onde enganam os utilizadores a revelar informações sensíveis. Podem também vender estes domínios a terceiros que pretendem usá-los para atividades maliciosas

Ameaças cibernéticas a um ccTLD

Phishing/Smishing:

O Phishing é uma técnica comummente utilizada por cibercriminosos para obtenção de informações confidenciais sobre as pessoas (como nomes de utilizador e passwords)

Email

Chamada telefónica

SMS/Whatsapp

Analisar e avaliar os riscos

Exemplo de avaliação de risco:

Risco	Probabilidade	Impacto	Nível
Acesso não autorizado a informações	médio	alto	alto
Obtenção de Credenciais	médio	alto	alto
Ransomware	baixo	alto	médio
Registo de nomes de domínio fraudulentos	baixo	alto	médio

Tipos de Controlos

- **Prevenção** - Os controlos de prevenção têm como objetivo evitar a ocorrência de incidentes de segurança e proteger proactivamente os ativos
- **Deteção** - Os controlos de deteção concentram-se na identificação precoce de atividades ou eventos de segurança suspeitos ou maliciosos que possam ameaçar a integridade, confidencialidade e disponibilidade dos dados e sistemas de uma organização
- **Correção** - Os controlos de correção desempenham um papel fundamental na gestão de riscos de segurança da informação. O seu principal objetivo é abordar e resolver os problemas identificados, bem como evitar que esses problemas se repitam

Gestão dos incidentes

Identificação:

Compreender o contexto da organização, os processos que suportam as atividades críticas, conhecer os riscos de cibersegurança que a podem impactar e desenvolver estratégias para os prevenir e/ou mitigar

Governação & Controlo

- Missão e Objetivos
- Framework
- Papéis e Responsabilidades

Gestão do Risco & Compliance

- Análise e tratamento dos riscos
- Requisitos mínimos de segurança
- Normativos e legislação aplicável

Auditoria

- Auditorias de segurança aos sistemas e redes
- Auditorias de compliance

Gestão dos incidentes

Proteção:

Desenvolver e implementar controlos apropriados para garantir a segurança das atividades críticas, ou seja, neste contexto, são implementados mecanismos que limitem ou contenham o impacto de um potencial incidente de cibersegurança, através de ações de sensibilização realizadas aos colaboradores, partilha de informação de inteligência dentro da comunidade CSIRT

Awareness

- Ações de sensibilização
- Partilha de informação RNCSIRT

Protective Technologies

- Controlo de Perímetro (Firewalls)
- Segurança Endpoint (Antivírus)
- Filtro de e-mails anti-spam
- Controlo de Acessos e Backups

Cyber Intelligence

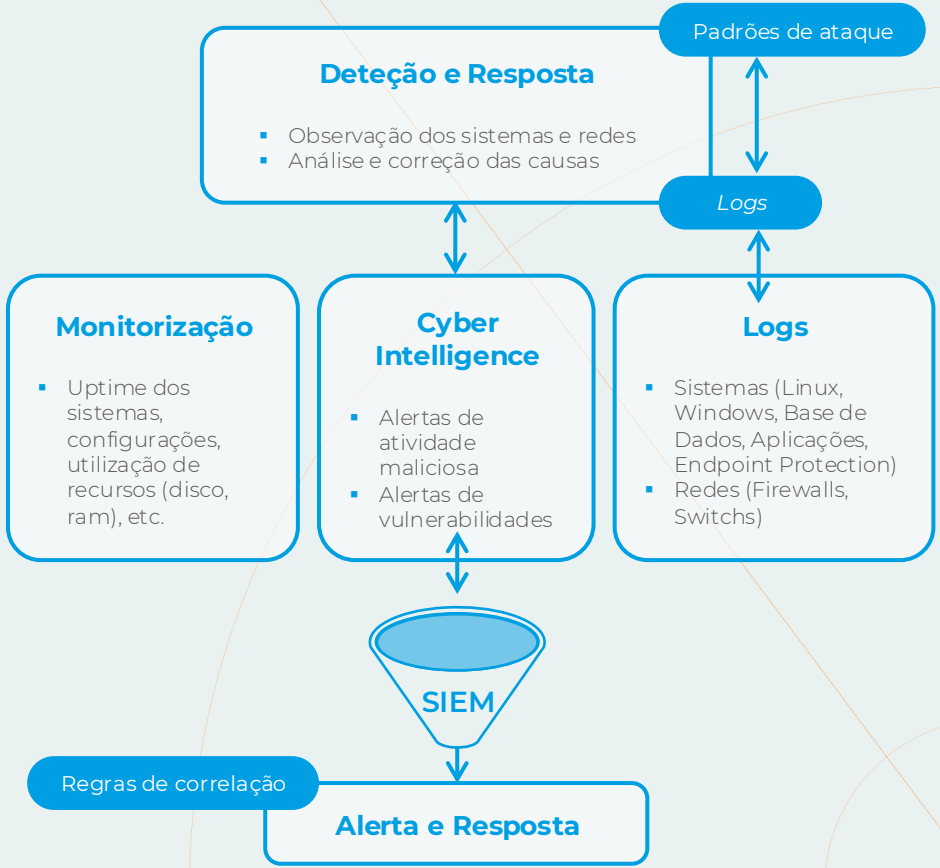
- Análise de relatórios de threat intelligence, threat actors e de incidentes de segurança

Gestão dos incidentes

Deteção:

Desenvolver e implementar de medidas apropriadas para detetar eventos ou incidentes de segurança da informação. Atividades de monitorização de logs e alertas através do sistema SIEM são um exemplo.

Resposta

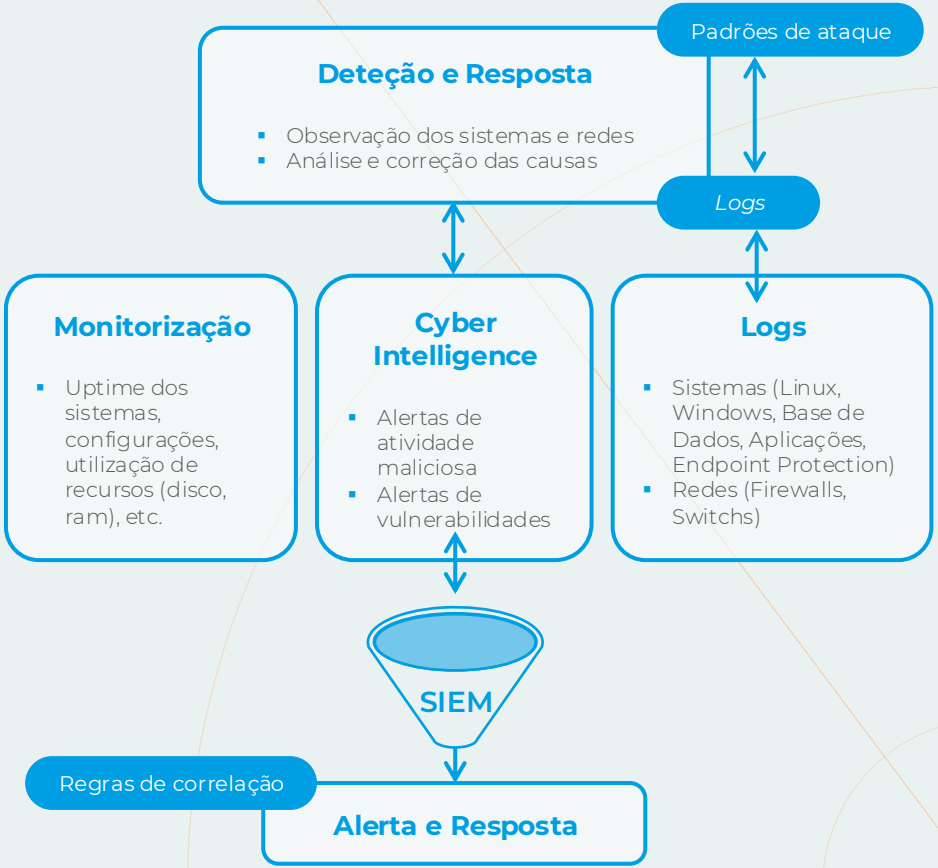


Gestão dos incidentes

Deteção

Resposta:

Desenvolver e implementar medidas apropriadas para agir quando detetado um incidente de cibersegurança. Neste contexto, são colocadas em prática as capacidades necessárias para conter como a definição de playbooks contra Ransomware



Gestão dos incidentes

Recuperação:

Desenvolver e implementar medidas apropriadas para manter planos de continuidade e de recuperação dos serviços críticos impactados por um incidente de cibersegurança, através do estabelecimento de um Plano de continuidade do negócio e de recuperação de desastre e de comunicação em crise

Continuidade de Negócio

- Plano de continuidade e recuperação de desastres

Análise Forense

- Análise de logs e investigação

Continuidade de Negócio

Análise de Impacto no Negócio

- Análise de Impacto nos Negócios é efetuada com recurso a questionários relativos à análise de impacto no negócio
- O processo é coordenado pelo Gestor da Continuidade de Negócio
- A análise de cada atividade é conduzida pela pessoa responsável em cada atividade
- A análise de Impacto no Negócios é realizada após a conclusão da Análise de Risco, de modo que as informações sobre os recursos necessários possam ser obtidas durante a análise de risco.

Análise de Impacto no Negócio

Questionario de Analise de Impacto de Negocio
Parte 1

1. Informação Geral acerca da actividade			
Nome da Organização		Nome da Pessoa Responsável	
Nome da atividade		E-mail:	
Morada		Data:	

2. Descrição da Actividade	
Descrição Breve da Actividade	Tarefas Chave e obrigações legais e contratuais: Data Limite para execução

3. Impacto Geral de um Incidente Disruptivo (1- impacto marginal , 2 - impacto aceitavel , 3 - impacto alto, 4 - impacto catastrófico)						
	Descrição (se necessário)	2 horas	4 horas	24 horas	48 horas	1 semana
Perda de reputação da Organização:						
Reação dos Clientes						
Impacto de outras actividades na organização:						
Impacto na equipa de Saude e Segurança no Trabalho; Impactos Ambientais:						
Quanto difícil é recuperar o backlog:						

4. Impacto financeiro do Incidente Disruptivo - Qual a perda Financeira causada pelo Incidente Disruptivo (em EUR)						
	Descrição se necessário	2 hours	4 hours	24 hours	48 hours	1 semana
Penalidades legais						
Penalidades Contratuais						
Perda de Receita de potênciais clientes:						
Perda de Receita de Clientes existentes:						
Despesas adicionais(reparações, manutenções, etc.)						

5. Comentários/ outra informação importante:

6. Conclusão (a ser preenchido pelo Gestor de Continuidade de Negocio)	
Maximo Periodo Tolerável de disrupção (Tempo Maximo de corte aceitavel)	

Análise de Impacto no Negócio

Questionário de Análise de Impacto no Negócio
Parte 2

7. Quantidade de trabalho	
Período (s) de maior volume de trabalho:	
Quantidade de trabalho executado durante períodos de maior volume de trabalho:	
Máxima quantidade de trabalho aceitável para a atividade imediatamente a seguir ao desastre:	
Período a partir do qual a quantidade normal de trabalho/nível de funcionamento deverá regularizar:	

8. Recursos necessários para a recuperação

Nome do Recurso	Especificações	Quantidade	Ponto de Falha	Tempo a partir do qual o recurso é necessário: Imediato	2 horas	4 horas	24 horas	48 horas	1 semana	Outro (especificar)
Pessoas:										
Aplicações e Base de dados:										
Dados guardados em formato electrónico (não incluído em aplicações e base de dados)										
Dados guardados em papel										
Equipamentos de IT e Comunicações										
Canais de Comunicação										
Outros equipamentos										
Infraestrutura e Instalações										
Capital necessário para a operação										
Serviços externos										

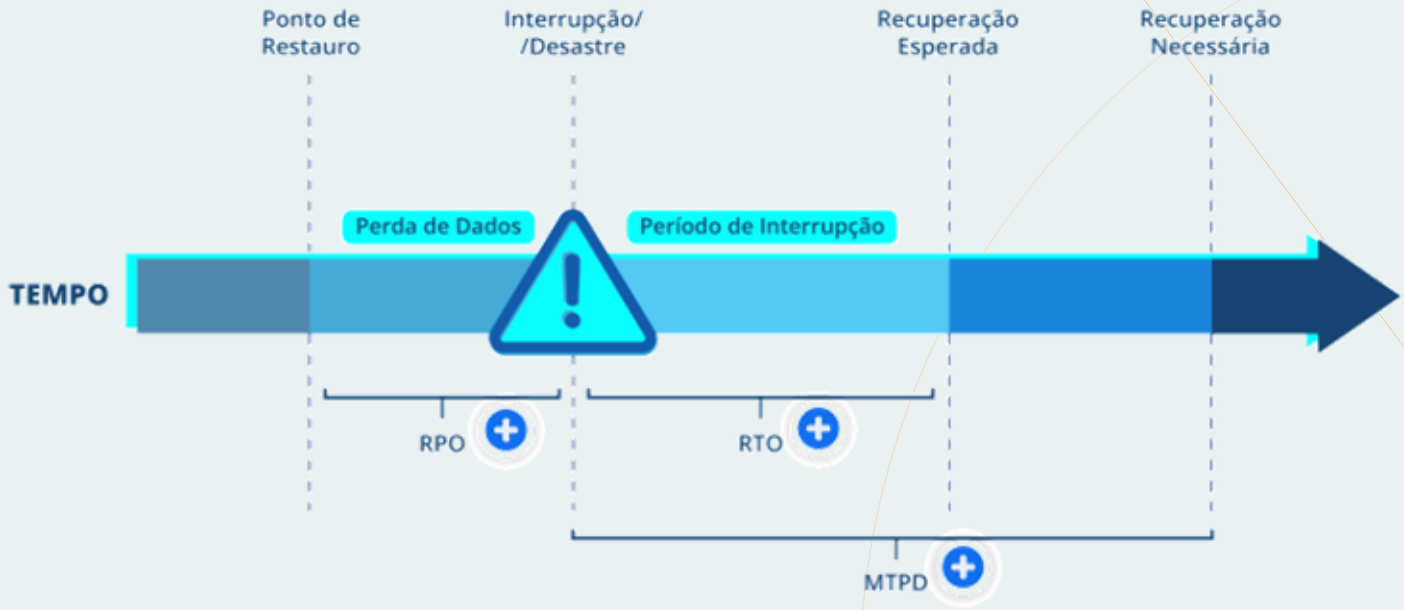
9. Dependência de outros (Quem é necessário para a recuperação desta atividade)			
Dependência de outras actividades da equipa		Quais os documentos ou procedimentos que definem como é que a continuidade de negócio é assegurada por produtos ou serviços providenciados por parceiros, outsourcers e fornecedores em caso de disrupção de serviços:	Avaliação das capacidades da continuidade de negócio. (1 - inadequadas, 2 - algumas capacidades existem mas necessitam de melhorias, 3 - adequadas):
Dependencia de Parceiros ou Outsourcers:			
Dependencia de fornecedores			

10.Maximo de dados perdidos - quantidade de dados que podem ser perdidos (1 - impacto marginal, 2 - impacto aceitável, 3 - alto impacto, 4 - impacto catastrófico)

	2 horas	4 horas	24 horas	48 horas	1 semana	São feitas cópias de backup (sim/Não). Com que periodicidade
Aplicações e Base de dados:						
Dados guardados em formato electrónico						
Dados guardados em papel						

11. Alternativas em caso de desastre	
Podem outras actividades sobreporem-se às operações desta actividade? Se sim, quais?	
Podem algumas das actividades ser desempenhadas manualmente, sem IT ou outro equipamento standard?	
12. Experiencia anterior	
Com que periodicidade incidentes disruptivos têm ocorrido até agora, e quanto tempo duraram?	
Como enfrentaram estas situações?	
13. Comentários/ outra informação importante	

Continuidade de Negócio



Continuidade de Negócio

Cadeia de fornecimento

Avaliação dos riscos associados a fornecedores

Requisitos mínimos de segurança para os fornecedores

Monitorização contínua da cadeia

Gestão de dependências críticas

Formação e Sensibilização

Todos os colaboradores recebam **formação adequada** em cibersegurança

Possuem **competências alinhadas** com as suas funções

Existe uma **cultura organizacional** de segurança.

Formação e Sensibilização

AnáliseFormação técnica a equipas responsáveis pela tecnologia e cibersegurança:

- Conhecer DNSSEC
- Conhecer processos de resposta a incidentes

Sensibilização geral a todos os colaboradores:

- Phishing e engenharia social
- Gestão segura de credenciais
- Boas práticas de acesso privilegiado

Treino operacional:

- Exercícios de incident response
- Tabletop exercises
- Simulações de ataques

Formação e Sensibilização

Formação disponibilizada de forma gratuita:

- Gestão dos Riscos nas Organizações
- Gestão da Continuidade de Negócio
- Segurança na Cloud
- Cidadão Ciberseguro
- Fundamentos da segurança de IA

Fonte:
https://lusnic.org/pt/cursos-de-ciberseguranca/

Formação e Sensibilização

- Garantir proteção da informação através de **mecanismos criptográficos adequados**
- Assegurar **confidencialidade, integridade e autenticidade** dos dados

Criptografia: Requisitos

Os requisitos principais pedidos pela norma são:

- Definir uma política de criptografia
- Determinar quando usar criptografia
- Usar algoritmos e protocolos seguros
- Implementar gestão de chaves criptográficas
- Proteger dados em trânsito e em repouso
- Cumprir requisitos legais e regulatórios

Recursos Humanos

- **Gestão de acessos baseada em funções (RBAC):**
  - Atribuição de permissões conforme responsabilidades, aka. principio do privilégio mínimo
- **Processos no ciclo de vida do colaborador:**
  - Onboarding, mobilidade interna e offboarding seguros
- **Formação e sensibilização contínua:**
  - Redução de erro humano e phishing
- **Verificação e confiança no pessoal:**
  - Na seleção e recrutamento realizar verificações e cruzamento de referências

Controlos de Acesso

Autenticação forte:

- MFA para sistemas críticos

Gestão de identidades e acessos (IAM):

- Controlo centralizado de utilizadores, utilização de Single Sign-On (SSO) sempre que possível
- Gestão de contas privilegiadas, garantindo que são auditáveis e restringido o uso das mesmas ao essencial

Monitorização e registo de acessos:

- Deteção de acessos indevidos
- Bloqueio automático após tentativas falhadas

LusNIC
Associação de ccTLDs de língua portuguesa

Coalition for Digital Africa

ICANN

PAUSA

EXERCÍCIO TABLE TOP

INSTRUÇÕES INICIAIS:

Fazer o registo na plataforma **https://ctf.ptsoc.pt**,
token de convite: **15a801909e984f65**

https://ctf.ptsoc.pt/login?invite=15a801909e984f65

Aceder ao tab “Table Top” e entrar no exercicio
“Possível incidente de cibersegurança num ccTLD”

LusNIC
Associação de ccTLDs de língua portuguesa

Coalition for Digital Africa

ICANN

QUESTÕES?

Comentários?
Sugestões?

LusNIC
Associação de ccTLDs de língua portuguesa

Coalition for Digital Africa

ICANN

Obriagd@!

lusnic@lusnic.org