Rating CSIRT FCT

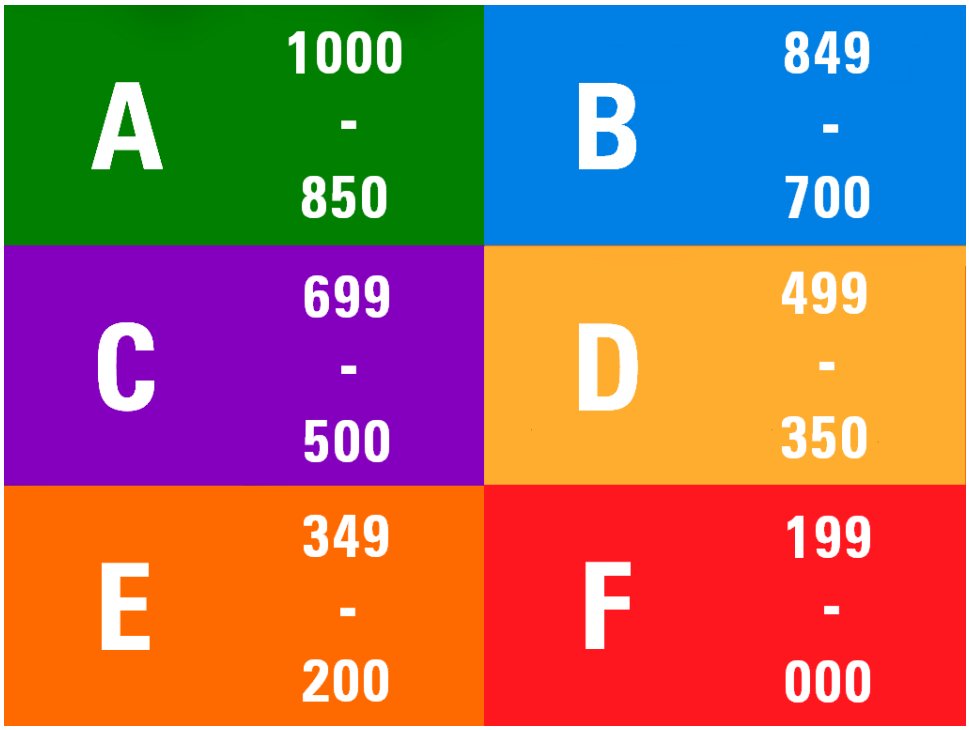
O Rating CSIRT FCT é um score mensal composto por 25 diferentes parâmetros divididos por oito categorias.

Alguns parâmetros dependem de eventos, que podem variar de mês para mês, consoante dados recolhidos de diversas fontes. Outros parâmetros dependem de configurações que podem assumir a forma considerada correcta ou segura, ou regredir para configurações inseguras (por exemplo no caso de substituição de um sistema).

Sobre estes 25 parâmetros é construído um «score» que pode variar entre 0 e 1000.

Nenhum dos componentes tem um peso inferior a 2,5% e nenhum tem um peso superior a 12,5%.

O «score» em cada mês dá origem a uma categoria, que varia de A (melhor) a F (pior), de acordo com os intervalos da figura abaixo:



As páginas seguintes deste documento detalham a lógica de cada parâmetro.

Qualquer dúvida sobre o rating ou sobre qualquer um dos parêmetros deve ser dirigida a info@csirt.fct.pt

versão 3.3 - Julho/2025

Categoria «CSIRT»

1) Formalização de um CSIRT

A existência de um CSIRT contribui para a segurança global de uma organização. A principal função de um CSIRT é responder a incidentes de segurança informática, pelo que cada organização só terá vantagens em estabelecer qual é a equipa, ou o conjunto de pessoas que estão mandatadas para essa função. É importante que a resposta a incidentes não seja realizada numa base ad-hoc, sem qualquer preparação prévia. É também muito relevante que a comunidade servida saiba qual é a equipa que tem esta função, assim como qualquer outra equipa externa na eventualidade de ser necessário trocar informação de forma segura.

Fórmula de cálculo

Esta componente tem um peso de 2,5% no total do rating. As leituras desta componente são realizadas no próprio sistema de rating, onde é registado se cada organização tem ou não uma equipa CSIRT formalizada.

O que fazer?

Publicar um RFC2350, que é basicamente o bilhete de identidade de uma equipa CSIRT.

Referência: https://csirt.fct.pt/pt/rede-academica-de-csirts/

Categoria «DNS»

2) DNS do domínio principal – Transferência de Zona

A transferência de zona de um domínio DNS é algo que deve estar sempre limitada, uma vez que estando publicamente disponível representará um valioso contributo para qualquer acção de reconhecimento que mais tarde vise o ataque a uma instituição.

Fórmula de cálculo

Se a transferência de zona do domínio principal da instituição estiver inibida serão atribuídos 50 pontos (5% do valor do rating). Se a transferência de zona for permitida serão atribuídos 0 pontos.

O que fazer?

Na configuração de todos os servidores DNS autoritativos para o seu domínio deve estar inibida a transferência de zona. A transferência de zona só deve ser permitida no servidor primário (SOA – Start of Authority) para o servidores secundários (listados nos registos NS do próprio domínio).

3) DNS do domínio principal - DNSSEC

A configuração de DNSSEC permite aumentar o grau de segurança das zonas DNS. A existência de DNSSEC configurado inibe alguns tipos de ataques como *cache poisoning* e *answer forgery*.

Fórmula de cálculo

A existência de DNSSEC configurado no principal domínio da instituição vale 50 pontos (ou seja 5% do valor total do rating).

O que fazer?

A plataforma webcheck.pt pode ser usada para verificar se o DNSSEC está configurado num determinado domínio.

Em https://www.pt.pt/pt/seguranca/dnssec/ estão várias referências que serão úteis para configurar DNSSEC no seu domínio.

Categoria «E-Mail»

4) E-MAIL - SPF

SPF é um registo DNS (do tipo TXT) que lista todos os servidores autorizados a enviar emails a partir de um certo domínio. Um servidor ao receber um email vai verificar os registos SPF desse domínio e verifica se o IP do servidor que enviou o email se encontra nessas lista de IPs autorizados.

Fórmula de cálculo

A existência de registo Sender Policy Framework (SPF) vale 50 pontos. Esta componente tem um peso de 5% no total do rating.

O que fazer?

É necessário criar um registo SPF adicionado à zona DNS de cada domínio. Aqui devem estar especificados que endereços IP ou hostnames é que estão autorizados a enviar emails deste domínio.

https://support.google.com/a/answer/10685031?hl=en

5) E-MAIL - DKIM

DKIM é um tecnica de autenticação de email que ajuda a prevenir que agentes maliciosos se façam passar por domínios legítimos.

Tem dois aspetos principais, o registo DKIM guardado no DNS e o header DKIM adicionado a todos os emails do domínio.

DKIM usa criptografia de chave pública para autenticar de onde vem o email e qual o agente que o envia. A chave privada é utilizada para assinar as mensagens e a chave pública, guardada no registo DKIM, é usada para verificar a assinatura.

Fórmula de cálculo

Esta componente vale 50 pontos se o DKIM estiver configurado no principal domínio da instituição. Representa 5% do valor global do rating.

O que fazer?

Em primeiro lugar é necessário gerar um par de chaves.

De seguida temos de colocar a chave pública gerada como um registo TXT nos settings do DNS. Cada DNS provider pode ter uma forma diferente de configurar isto, pelo que é recomendada uma investigação para cada caso.

Por fim é preciso um milter (email filter) que permita adicionar um header ao email com a chave privada gerada anteriormente.

Mais informações de configuração em:

https://www.mailjet.com/blog/deliverability/setting-up-dkim-step-by-step/

6) E-MAIL - DMARC

DMARC é um protocolo para autenticação de emails. Permite verificar se o email é legitimamente de quem o enviou, e o que fazer se não for.

DMARC permite indicar que as mensagens enviadas estão protegidas com SPF e DKIM, e indica como processar o email caso essas verificações falhem.

Fórmula de cálculo

Esta componente vale 50 pontos se existir um registo DMARC associado ao domínio principal da instituição, o que tem um peso de 5% no total do rating.

O que fazer?

É necessário existir um registo SPF adicionado à zona DNS do domínio. Estes validam a origem dos emails através da comparação do IP do endereço de email, contra o IP do dono do domínio que o envia.

Exemplo de um registo DMARC TXT da Microsoft:

_dmarc.microsoft.com. 3600 IN TXT "v=DMARC1; p=none; pct=100; rua=mailto:d@rua.contoso.com; ruf=mailto:d@ruf.contoso.com; fo=1"

Mais informações de configuração em:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email?view=o365-worldwide

https://mxtoolbox.com/dmarc/dmarc-setup?lm=NAV-PD

Categoria «Incidentes»

7) Incidentes

Este parâmetro incide sobre a actividade principal do CSIRT FCT, que é a disponibilização de um ponto de contacto para que qualquer pessoa possa reportar um incidente que diga respeito à RCTS. O valor atribuído neste parâmetro depende do número de incidentes reportados (depois de efectuada a triagem pelo CSIRT FCT) e dos dias em que as organizações demoram a fornecer feedback sobre a situação, que permita fechar os casos em aberto. Todos os incidentes são categorizados com base na Taxonomia da Rede Nacional CSIRT (https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf)

Fórmula de cálculo

Cada incidente desconta 1 ponto por cada dia em que permanecer aberto no sistema de registo de incidentes do CSIRT FCT. Esta componente tem um peso de 12,5% no total do rating.

O que fazer?

Adquirir o máximo de conhecimento sobre a própria infraestrutura da organização e dispor de contactos agilizados com pessoas das diversas unidades orgânicas que gerem partes da infraestrutura e que possam intervir de forma efectiva em caso de incidente de segurança informática.

Categoria «RPKI»

8) DNS

Este parâmetro é relativo à avaliação da existência de um certificado (ROA – autorização de objeto de rota) para o espaço de endereçamento IP que cobre o endereço IP dos servidores DNS do domínio principal da instituição. No caso de os servidores DNS estarem alojados na RCTS, à partida essa circunstância é garantida pela própria FCCN. A existência deste certificado ajuda a identificar situações onde alguém tenta fazer spoofing dos endereços IP dos servidores DNS.

Fórmula de cálculo

Se numa leitura for detetada a inexistência de certificado (ROA) relativo a algum dos servidores DNS (registos NS do domínio principal), o valor dessa leitura será zero. São realizadas leituras semanalmente e o resultado será a média. Esta componente tem um peso de 2,5% no total do rating.

O que fazer?

Solicitar a existência do certificado (ROA) caso ele não exista, ou em último caso, migrar o(s) endereço(s) IP dos servidores DNS para um segmento de rede relativamente ao qual este certificado já exista. Mais informação em: https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/

9) Blocos

Este parâmetro é relativo à avaliação da existência de um certificado (ROA – autorização de objeto de rota) para o espaço de endereçamento IP que a instituição usa. No caso de o endereçamento fazer parte da RCTS, à partida essa circunstância é garantida pela própria FCCN. A existência deste certificado ajuda a identificar situações onde alguém tenta fazer spoofing dos endereços IP atribuídos à instituição.

Fórmula de cálculo

Se numa leitura for detetada a inexistência de certificado (ROA) relativo a algum espaço de endereçamento IP em uso pela instituição, o valor dessa leitura será zero. São realizadas leituras semanalmente e o resultado será a média. Esta componente tem um peso de 2,5% no total do rating.

O que fazer?

Solicitar a existência do certificado (ROA) caso ele não exista. Mais informação em: https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/

Categoria «Utilização»

10) Malware

O CSIRT FCT recebe eventos de malware de diversas fontes que consolida no seu SIEM. Apesar de as várias fontes não terem todas o mesmo grau de confiança, todos os eventos de malware são considerados da mesma forma.

Fórmula de cálculo

Cada evento de malware desconta 1 ponto. Esta componente tem um peso de 5% no total do rating.

O que fazer?

Os eventos de malware surgirão em maior quantidade em função do menor grau de protecção dos dispositivos que usam as infraestruturas de rede de uma organização. Realizar as actualizações de sistema operativo e de aplicações contribui para manter um bom estado dos dispositivos. Também é aconselhável descontinuar todos os sistemas que deixem de ser necessários ou que fiquem sem um responsável pela sua gestão.

11) IDS (Intrusion Detection System)

Esta componente está ligada à manutenção dos sistemas e dispositivos livres de malware. No caso de algum sistema comprometido atacar as redes da FCCN, os sistemas de detecção de intrusões existentes identificarão a proveniência desses ataques. De referir que a aplicação desta componente é extremamente limitada, pois só leva em conta casos onde a infraestrutura da FCCN é atacada/abusada.

Fórmula de cálculo

Cada detecção desconta 10 pontos. Esta componente tem um peso de 2,5% no total do rating.

O que fazer?

Minimizar as intrusões e os sistemas internos comprometidos que possam vir a atacar a infraestrutura da FCCN ou outras. No caso de serem detectados sistemas comprometidos deve-se bloquear o seu acesso à internet, em primeira instância, analisá-los se o dispositivo for da organização e por último reinstalá-los ou recomendar a sua reinstalação se se tratarem de dispositivos que são propriedade de terceiros.

12) Blacklists

Este parâmetro mede os pedidos realizados pelas instituições sobre domínios incluídos na «blacklist» que suporta o funcionamento do serviço DNS FIREWALL. Estes pedidos indiciam uma possível infecção de um dispositivo que está a usar as redes de uma instituição.

Fórmula de cálculo

Cada domínio inquirido desconta 1 ponto até um máximo de 40 pontos. As instituições que não subscrevem o serviço DNS FIREWALL terão estaticamente 10 pontos, de um máximo de 50. As instituições que subscrevem o serviço não poderão ter menos de 10 pontos. Esta componente tem um peso de 5% no total do rating.

O que fazer?

A subscrição do serviço DNS FIREWALL aumenta o potencial máximo de pontos deste parâmetro de 10 para 50. Do ponto de vista operacional é importante zelar para que os dispositivos não fiquem infectados.

13) Reputação

Este parâmetro tem por objetivo a verificação da reputação de endereços IP da instituição envolvidos no envio massivo de mensagens de correio electrónico.

Fórmula de cálculo

Se nenhum IP da instituição for detetado em «blacklists» relativas ao envio massivo de mensagens, o valor da leitura diária será zero. Esta componente tem um peso de 5% no total do rating.

O que fazer?

Controlar o envio de mensagens para o exterior, e em caso de algum IP ser classificado em alguma lista, intervir rapidamente para que ele seja removido.

Referência: multirbl.valli.org

14) Direitos de Autor (Queixas sobre)

Com alguma frequência o CSIRT FCT recebe queixas relativas a violações de direitos de autor (copyright). Essas queixas identificam sempre um endereço IP associável a uma organização. Estes eventos indiciam que existem utilizadores (voluntariamente) ou sistemas infectados a usar recursos da organização que estão a violar a lei.

Fórmula de cálculo

Cada queixa recebida desconta 5 pontos. Esta componente tem um peso de 2,5% no total do rating.

O que fazer?

Implantar mecanismos de detecção de utilização de protocolos peer-to-peer, que são habitualmente usados neste tipo de violação da lei.

Sensibilizar internamente os utilizadores das infraestruturas da organização de que os recursos disponibilizados não podem servir para violar a lei.

Categoria «Vulnerabilidades»

15) Acesso a ficheiros

O acesso a ficheiros, nomeadamente com capacidade de escrita pode ajudar a comprometer sistemas que os alberguem. É portanto importante garantir que o acesso externo de escrita está desabilitado, como comportamento padrão.

Fórmula de cálculo

Diariamente é realizada uma verificação no servidor web principal da instituição sobre a possibilidade de escrita no sistema do servidor. Esta componente tem um peso de 2,5% no total do rating.

O que fazer?

Configurar o servidor web de forma a que seja vedada a criação de ficheiros por um qualquer utilizador externo. No caso de ser necessária a criação de ficheiros, configurar acessos por VPN.

16) Vulnerabilidades

As vulnerabilidades estão normalmente associadas a serviços expostos na Internet que podem ser abusados, e dar origem a incidentes.

Fórmula de cálculo

Cada vulnerabilidade encontrada desconta 2 pontos. Esta componente tem um peso de 7,5% no total do rating.

O que fazer?

As vulnerabilidades são cada vez mais importantes, permitindo a actores maliciosos comprometer sistemas vulneráveis. É importante aplicar as actualizações que são publicadas, nomeadamente as que dizem respeito ao sistema operativo.

17) Bases de dados

A inclusão de um parâmetro «bases de dados» deve-se ao grau de criticidade que uma base de dados exposta publicamente pode assumir. A exposição pública pode dever-se a várias causas, como por exemplo regras de firewall inexistentes ou mal configuradas, mas o mais importante será o conteúdo de cada base de dados que poderá inclusivamente conter dados pessoais, e fazer a organização incorrer numa violação do RGPD.

Fórmula de cálculo

Cada incidente desconta 1 ponto, sendo realizadas leituras numa base semanal. Esta componente tem um peso de 2,5% no total do rating.

O que fazer?

O acesso a bases de dados tem que ser gerido criteriosamente, e a sua não exposição pública é uma regra de segurança básica. Uma medida preventiva consiste na realização de varrimentos (scan) à própria infraestrutura para detectar situações desta tipologia.

18) Acesso Remoto

Vulnerabilidades ligadas ao acesso remoto, seja por RDP ou outros protocolos têm sido fonte de muitas intrusões e posteriores exfiltrações de dados ou mesmo acções destrutivas. É pois importante garantir que o acesso remoto é apenas permitido através de acessos VPN (com dupla autenticação, desejavelmente) e nunca através de qualquer ponto da Internet.

Fórmula de cálculo

São realizadas leituras semanais sobre eventos relativos a este tipo de vulnerabilidade. Cada evento encontrado descontará 1 ponto. Esta componente tem um peso de 2,5% no total do rating.

O que fazer?

Uma medida de segurança preventiva consiste em efetuar varrimentos periódicos à própria infraestrutura no sentido de verificar se existe algum serviço acesso remoto atingível desde o exterior. Quando são detectados casos, o serviço deve ser restrito apenas a acessos via VPN.

Categoria «Web»

19) Defacements

«Defacement» é um tipo de ataque no qual um atacante consegue alterar o conteúdo e a aparência visual da homepage, de uma página particular, ou até mesmo de todo um domínio web, e assim substituir o conteúdo exibido no website com o seu próprio conteúdo. O defacement pode estar associado a outros tipos de ataques como SQL Injection, Cross-Site Scripting (XSS), DNS hijacking, infecções por malware, e acesso não autorizado. Através das diversas fontes que o CSIRT FCT usa, podemos receber também informação de que um domínio foi blacklisted por motivo de defacement.

Fórmula de cálculo

Cada «defacement» desconta 10 pontos. Esta componente tem um peso de 2,5% no total do rating.

O que fazer?

A não ocorrência de «defacements» depende essencialmente de os sistemas expostos à Internet estarem devidamente protegidos e actualizados. Websites não geridos são habitualmente um problema. As auditorias periódicas poderão contribuir para encontrar vulnerabilidades, que, ficando latentes representam um risco acrescido.

20) Robots.txt

A existência de um ficheiro robots.txt informa os motores de pesquisa sobre quais os URLs que podem ser acedidos. Isto é utilizado principalmente para evitar sobrecarregar o website com pedidos, podendo por isso ter um impacto positivo no eixo da disponibilidade.

Fórmula de cálculo

É realizada uma verificação diária sobre a existência do ficheiro robots.txt no website principal da instituição. O resultado será o valor da média das leituras realizadas. Esta componente tem um peso de 2,5% no total do rating.

O que fazer?

Crie um ficheiro robots.txt e coloque-o nos seus servidores web.

Referência: https://developers.google.com/search/docs/crawling-indexing/robots/create-robots-txt

21) Cabeçalhos (Headers)

A ideia principal para o uso de headers é melhorar a navegação e experiência do cliente. Melhora a cibersegurança pois permite-nos evitar o seu uso por atacantes em alguns vetores de ataque e deve por isso ser tido em consideração nas configurações do website principal da instituição.

Fórmula de cálculo

A existência de todos os headers corresponde a 25 pontos, e representa 2,5% do valor total.
Entre 3 e 4 headers corresponde a 15 pontos.
2 ou menos headers encontrados corresponde a 0 pontos.

Neste momento a nossa verificação assenta sobre a existência de alguns headers, em particular verificamos se existem os seguintes cinco headers:

- Strict-Transport-Security
- X-Frame-Options
- X-XSS-Protection
- Content-Security-Policy
- X-Permitted-Cross-Domain-Policies

O que fazer?

Para obter a pontuação máxima nesta compontente todos os headers referidos acima devem existir. Estes headers, por regra, são activados ou inibidos na configuração do próprio servidor web.

22) Server Signature

Nesta verificação o que fazemos é garantir que nenhum dos headers usados tem versões que possam ser usadas para identificar vulnerabilidades, e posteriormente identificar alvos de possiveis ataques.

Fórmula de cálculo

Esta verificação representa 2,5% do valor total ou 25 pontos. Por cada header com possiveis indicadores de versões são descontados 12,5 pontos ao valor total da verificação.

No imediato estamos a testar 2 dos headers mais conhecidos por conterem essa informação:

- server
- x-powered-by

O que fazer?

Devem ser removidos da configuração do servidor web quaisquer headers que contenham versões específicas.

23) SSL

Actualmente é importantíssimo usar certificados SSL para garantir aos utilizadores dos websites que estão a visitar o website que pretendem, e que não estão a ser vítimas de algum processo fraudulento. Esta componente tem a especificidade de a qualidade do certificado SSL poder assumir diversos graus.

Fórmula de cálculo

Esta componente vale 50 pontos, representando 5% do valor global do rating. Se a qualidade do certificado for acima de "B" ou superior serão atribuídos os 50 pontos, se for entre "C" e "D" serão atribuídos 20 pontos. No caso de o certificado existir, mas por alguma razão não ser inteiramente confiável serão atribuídos apenas 5 pontos. O valor será de 0 pontos se o certificado SSL não existir.

O que fazer?

Caso ainda não tenha certificado SSL ou deseje melhorar a sua qualidade, deverá solicitar o seu certificado SSL ao serviço Certificados FCT (https://www.fccn.pt/areas-tecnologicas/seguranca/rcts-certificados/). Após a devida obtenção e instalação poderá testar a qualidade do certificado já instalado recorrendo ao teste da SSLLabs: https://www.ssllabs.com/ssltest.

24) TLS

TLS (*Transport Layer Security*) é um protocolo criptográfico projetado para fornecer segurança nas comunicações. A utilização de versões consideradas seguras do protocolo TLS, em combinação com a utilização de certificados digitais válidos, permite fornecer aos visitantes de um domínio de internet um maior grau de segurança na ligação estabelecida. A versão do TLS do servidor web principal da instituição é avaliada, uma vez que nem todas as versões do TLS são consideradas seguras atualmente.

Fórmula de cálculo

A versão TLS do servidor principal da instituição é verificada semanalmente. O resultado é o valor da média dessas leituras. Esta componente tem um peso de 2,5% no total do rating.

O que fazer?

Configurar as versões consideradas seguras: TLS v1.2 ou TLS v1.3.

Referência: https://webcheck.pt/pt/

25) Security.txt

O security.txt é um ficheiro de texto com informações de contacto que deve ser colocado em servidores web. Investigadores de segurança podem utilizar estas informações para contactar diretamente o departamento ou a pessoa certa da sua organização sobre vulnerabilidades encontradas no seu website ou sistemas de TI. Isto pode acelerar a correção de vulnerabilidades encontradas, reduzindo a oportunidade de exploração por partes mal-intencionadas.

Fórmula de cálculo

São realizadas verificações semanais sobre a existência do ficheiro security.txt no servidor web principal da instituição. O resultado será a média do valor das leituras realizadas. Esta componente tem um peso de 2,5% no total do rating.

O que fazer?

Gerar e colocar um ficheiro security.txt no servidor web principal da instituição.

Exemplo: https://example.nl/.well-known/security.txt