CFT	NEP NAT 02.03.04	Exemplar n.º Pág 1 de 58 Pág 14JAN14
Assunto:	**ESTRUTURA DE SEGURANÇA DA INFORMAÇÃO DO EXÉRCITO. NORMAS TÉCNICAS E PROCEDIMENTOS DO ADMINISTRADOR DA REDE LOCAL DAS U/E/O**	
Ref	a. Despacho 04/VCEME/11, de 26MAI2011 b. Despacho S. Exª GEN CEME de 02ABR2012 c. Diretiva nº 156/CEME/2009 d. SEGMIL-1 e. RAD 280-1, JAN04 f. RAD 280-2, MAI05 g. Lei 32/2008, 17Jul h. Lei 41/2004, 18Ago com as alterações introduzidas pela Lei 46/2012, 29Ago i. Despacho nº 204/CEME/10, de 15NOV10	
NEP Relacionadas	NEP NAT 02.03.03; NEP NAT 02.03.05	

1. FINALIDADE

A administração e gestão de topo das diferentes redes que constituem o Sistema de Informação e Comunicações Operacional (SIC-Op), nomeadamente a Rede de Transmissão do Exercito (RTE), a Rede de Dados do Exército (RDE) e a Rede de Comutação de Voz do Exército (RCVE), encontra-se na responsabilidade da Direção de Comunicações e Sistemas de Informação (DCSI) através do Centro de Transmissões do Exército (CTE), herdeiro das missões e tarefas do Regimento de Transmissões - Lisboa. Por forma a disponibilizar apoio técnico ao utilizador, tornando célere o solucionamento de problemas mais comuns e de menor complexidade, algumas das tarefas de administração dos recursos tecnológicos existentes nas Unidades/Estabelecimentos/Orgãos (U/E/O) foram descentralizadas, sendo executadas pelos Administradores Locais segundo determinadas regras e de acordo com a atribuição de responsabilidades.

Assim, este documento tem como finalidade primária estabelecer normas e procedimentos a cumprir pelos gestores/administradores locais dos meios de Comunicações e Sistemas de Informação da RDE no âmbito da realização das suas tarefas.

2. ÂMBITO

A presente norma destina-se a ser do conhecimento de todos os Administradores de Rede Local e outros elementos que, por força da necessidade ou por nomeação superior, tenham necessidade de executar tarefas e aceder, quer de forma física quer lógica, às redes e sistemas do SIC-Op, presentes na sua U/E/O.

3. SITUAÇÃO

a. O alto nível de informatização dos serviços e a consequente dependência das Tecnologias de Informação e Comunicação (TIC) apresentam riscos e vulnerabilidades de segurança que obrigam à definição de políticas, atribuição de responsabilidades, identificação de procedimentos e tarefas conducentes à Segurança da Informação e da Privacidade;

b. Neste sentido, avaliados os riscos de segurança informática na RDE, torna-se necessário identificar normas técnicas de gestão e de suporte para garantir a segurança dos sistemas de informação e comunicação, que se encontram sob a responsabilidade do Exército Português, em termos de integridade, confidencialidade, disponibilidade, autenticidade, não repúdio, auditabilidade e privacidade da informação;

c. Surge assim uma sistematização para identificar e atribuir responsabilidades em termos de gestão da informação, clarificação do papel e função dos diversos intervenientes na implementação de medidas e ações de monitorização, de controlo e avaliação das políticas de Segurança dos Computadores (COMPUSEC);

d. Neste âmbito, os Administradores da Rede Local das U/E/O, assumem um papel fundamental na:

(1) Implementação da Política de Segurança definida superiormente pela DCSI;

(2) Fazer a correta gestão de Ativos;

(3) Garantir a Segurança dos Recursos Humanos;

(4) Garantir a Segurança Física e Ambiental;

(5) Contribuir para a Gestão de Comunicações;

(6) Assegurar um conveniente Controlo de Acessos;

(7) Fazer, dentro das suas capacidades de intervenção, a Manutenção de Sistemas de Informação;

(8) Contribuir para a Gestão de Incidentes de Segurança da Informação.

4. EXECUÇÃO

a. Conceitos gerais

Ao abordarmos as Normas Técnicas e Procedimentos dos Administradores das Redes Locais das diferentes U/E/O, torna-se essencial referir que:

(1) Importa articular, de forma consistente e segundo um conjunto de metodologias de triagem e procedimentos de resolução e acompanhamento, todas as entidades internas e externas envolvidas na resolução dos problemas gerados pela utilização dos diversos SIC em exploração no Exército, contribuindo para o aumento da qualidade do serviço prestado e na projeção de uma imagem de eficiência, dinamismo e modernidade do Exército;

(2) Deve ser garantido que todos os problemas reportados sejam convenientemente registados, encaminhados e acompanhados, para quem tenha capacidade para os solucionar, desejavelmente ao nível mais especializado possível;

(3) O acesso pelo Administrador da Rede Local a qualquer sistema CSI existente na sua U/E/O, cumprindo com o estipulado nas refª g) e h), deve ser autorizado pelo CTE, que previamente obteve autorização da DCSI;

(4) O acesso físico às instalações dos equipamentos, tais como servidores, centrais telefónicas, rádios e outros sistemas de transmissão, deve ser condicionado, sendo apenas permitido o acesso a estas instalações a pessoal superiormente autorizado;

(5) Todos os apoios solicitados e informações desejadas devem ser redigidos e enviados para o correio eletrónico, ou telefonicamente, do *help-desk* do CTE, por forma a ser possível manter um registo único e atualizado de todos os pedidos e contactos efetuados;

(6) O acesso aos recursos de rede é feito mediante uma identificação e autenticação constituída por um nome de utilizador (NIM/função/organismo) e por uma palavra – passe ("*password*") individual e intransmissível. Desde a entrada em sessão ("*Login*") até ao seu encerramento ("*Logout*") o indivíduo ligado a esse nome de utilizador e palavra-passe é responsável pelas ações que executar.

b. Nomeação do Administrador de Rede Local

(1) É da responsabilidade do Comandante/Diretor/Chefe da U/E/O a nomeação do Administrador de Rede Local e, eventualmente, um adjunto;

(2) A nomeação deverá recair sobre graduados, sempre que possível do QP, habilitados com conhecimentos técnicos de administração e segurança de redes, por forma a

colaborar com o CTE na realização das tarefas inerentes à implementação, exploração, manutenção, segurança e resposta a incidentes nos meios CSI existentes e em produção na U/E/O;

(3) A nomeação deverá ser comunicada à DCSI.

c. <u>Deveres e responsabilidades do Administrador de Rede Local</u>

(1) É dever do Administrador de Rede Local cumprir e divulgar as normas técnicas bem como sensibilizar de forma permanente os utilizadores para os aspetos de segurança da informação e de operação dos meios e sistemas de informação: cuidados com o equipamento, manuseamento de matérias classificadas, políticas de segurança, sistema de relato de incidentes, etc;

(2) No âmbito da infraestrutura da RDE, é da responsabilidade do Administrador da Rede Local:

(a) Acompanhar o planeamento e a execução de trabalhos de expansão/melhoramento da Rede Local, responsabilidade da DCSI;

(b) Manter um cadastro atualizado das ligações físicas e lógicas de todos os equipamentos de rede existentes na U/E/O e fornece-lo ao CTE, sempre que solicitado ou em caso de alterações;

(c) No processo de implementação de pontos de acesso *wireless*, regulamentados em Norma Técnica própria (NEP/NAT 02.03.06), é responsabilidade do Administrador Local:

1. Solicitar autorização e parecer técnico à DCSI;

2. Se autorizada, garantir que se cumprem as normas de implementação e exploração de pontos de acesso *wireless*,

(3) No âmbito da configuração de equipamentos ligados ao domínio *exercito.local*, é da responsabilidade do Administrador de Rede Local:

(a) Garantir que os equipamentos conectados à RDE cumprem os requisitos mínimos de *software* e *hardware* necessários à implementação das políticas de segurança da Rede;

(b) A instalação do sistema operativo em qualquer computador da sua U/E/O, tendo por base as versões disponibilizadas pelo CTE, e de acordo com as diretivas superiores emanadas pela DCSI. Qualquer computador que apresente sinais de infeção grave ou que tenha sido alvo de uma severa recuperação dos dispositivos de armazenamento nomeadamente discos rígidos, deve ser

formatado e em último caso, esses dispositivos substituídos por outros e os antigos destruídos, em conformidade com o expresso na refª f);

(c) Garantir que todos os computadores respeitam as politicas de instalação e operação em vigor e determinadas pela DCSI;

(d) Garantir que não é instalado qualquer tipo de *software* (aplicações, base de dados, jogos, etc.), sem a devida autorização do CTE;

(e) A manifestação de necessidades específicas de *software* e *hardware* devem ser efetuadas pela U/E/O à DCSI através do seu Administrador de Rede Local, indicando as especificações técnicas do pretendido e a finalidade a que se destina;

(f) Não permitir alterar ou apagar as configurações estabelecidas pelo Administrador de Rede do Exército segundo as orientações e indicações da DCSI, como por exemplo: proteção de ecrãs, caracterização do correio eletrónico e antivírus, etc;

(g) Garantir que o manuseamento/configuração extraordinária de *hardware* tais como computadores, digitalizadoras, impressoras, gravadores de CD e DVD, fax e sistemas de vídeo e áudio, incluindo terminais telefónicos, só poderá ser efetuado por pessoal formalmente autorizado. O manuseamento reporta-se a ligar/desligar cabos, transportar e/ou mudar de lugar, substituir componentes e/ou consumíveis;

(h) Solicitar autorização ao CTE/DCSI para a ligação excecional de equipamentos particulares à RDE;

(4) No âmbito da exploração dos recursos da RDE, o Administrador de Rede Local:

(a) Deve restringir a utilização de recursos de rede (transferência e partilha de ficheiros, etc.) ao racionalmente indispensável, evitando congestionamento da rede e demoras na operação;

(b) É responsável por verificar, controlar e apoiar a operação e manutenção da rede local e a interligação a outras U/E/O do domínio Exército, ou domínios de Forças Nacionais Destacadas (FND);

(c) Sendo expressamente proibido a colocação de conteúdos impróprios (tais como música, vídeos não institucionais, imagens de caráter não profissional e organizacional) em pastas pessoais ou partilhadas, em dispositivos de armazenamento local, ou em portais colaborativos, é responsável por notificar

imediatamente o(s) utilizador(es) proprietário(s) dessa(s) pasta(s) ou ficheiro(s) dessa ocorrência e eliminar os referidos conteúdos de forma permanente;

(d) Na eventualidade de existirem acessos à rede pública de *Internet* não controlados por IXBOX e devidamente autorizados pela DCSI (em locais onde não se encontra implementada RDE), a U/E/O que contratou o serviço de internet detém a responsabilidade sobre todos os incidentes que possam ocorrer com origem no ponto de acesso contratado. Desta forma, qualquer infração ocorrida apesar de não colocar em causa a segurança da Informação que circula na RDE, poderá constituir ameaça à imagem da instituição Exército, pelo que é responsabilidade do Administrador da rede Local:

1. Garantir a implementação de um servidor *proxy* que intercete os pedidos para a *Internet*, garantindo o controlo de acessos por utilizador e filtragem de conteúdos considerados maliciosos (*Warez, Hacking, Drogue, Child*, etc) de forma a impedir ou dissuadir a tentativa de qualquer acesso considerado como Cibercrime;

2. Elaborar NEP da U/E/O e sensibilizar os utilizadores para o facto de os acessos não serem controlados e existirem preocupações reforçadas no âmbito da segurança informática, nomeadamente a proibição de acesso a *sítios* de conteúdo malicioso, a proibição de métodos que contornem as implementações técnicas de segurança em vigor, precauções na utilização das redes sociais, precauções na utilização da internet em geral, etc.

(5) No âmbito da manutenção da operacionalidade da RDE, o Administrador de Rede Local:

(a) É responsável por verificar periodicamente o estado de climatização e alimentação elétrica das instalações onde existem equipamentos e sistemas pertencentes ao SIC-Op, nomeadamente rádios, *multiplexers*, *modems*, retificadores DC, equipamentos de rede (tais como *Switches* e *Routers*, UPS, Servidores, Consolas, SAN, NAS, Unidades de Backup), etc. Nesta situação estão autorizados os contactos diretos com o CTE;

(b) É responsável por diagnosticar problemas de primeira linha relacionados com o bom funcionamento dos equipamentos de rede, incluindo sistemas *VoIP* e Videoconferência. Para tal deve manter uma listagem atualizada de todos os IP e endereços de MAC desses equipamentos e sempre que mandatado para tal, efetuar a alteração de IP de gestão ou de produção, de acordo com as indicações recebidas;

(c) Sempre que houver alteração de IP que influenciem o normal funcionamento dos serviços da U/E/O, o Administrador de Rede Local deve informar as entidades internas dessa alteração por forma a minimizar a disrupção de serviços;

(d) Deve receber os primeiros "*input*" por parte dos utilizadores locais no que respeita ao mau, ou deficiente funcionamento, quer da rede local, quer dos próprios sistemas terminais, tais como computadores e telefones;

(6) No âmbito da implementação de resposta a incidentes informáticos, mitigando possíveis danos na rede ou comprometimento de informação nela armazenada, como resultado da concretização de ataque à RDE, é responsabilidade partilhada por todos os utilizadores a comunicação célere da identificação de qualquer ocorrência anormal no funcionamento dos serviços disponibilizados pela RDE. O Administrador da Rede Local é responsável por:

(a) Sempre que for detetada uma anomalia e irregularidade no bom funcionamento da rede e serviços da U/E/O, deve:

1. Comunicar de imediato ao CTE a ocorrência;

2. Analisar o problema, efetuando testes de diagnóstico e, dentro das suas capacidades e responsabilidades, tentar resolver o mesmo;

3. Quando a resolução do incidente ultrapassar as suas competências, deve coordenar com o CTE, o encaminhamento do mesmo com vista à sua mitigação;

4. Após contacto com o CTE, tomar todas as medidas necessárias conforme as indicações recebidas, por forma a mitigar e eliminar o problema, nem que para tal seja necessário desligar fisicamente equipamentos da rede e mesmo em último caso, alguns segmentos da própria rede, permitindo a intervenção de equipas CIRC em ambiente controlado para uma análise mais profunda da situação detetada;

(b) Deve operar os meios de acordo com as instruções técnicas difundidas e comunicar de imediato ao CTE qualquer anomalia verificada, colaborando nas operações de gestão e manutenção dos equipamentos;

(c) Integrar e colaborar no processo de mitigação de incidentes de segurança na RDE conforme estabelecido nas NEP/NAT relativas à "Estrutura de Segurança da Informação do Exército";

(d) Anexo A – Procedimentos para Gestão de Incidentes

(7) No âmbito da criação e gestão de utilizadores da RDE:

(a) A criação de utilizadores e grupos de utilizadores é da responsabilidade do CTE. O pedido de criação e manutenção de grupos e utilizadores é da responsabilidade única dos administradores, os quais podem propor superiormente o cancelamento temporário de acesso de um utilizador em caso de suspeita de violação da segurança ou não cumprimento das normas técnicas da "Estrutura de Segurança da Informação do Exército";

(b) É da responsabilidade do Administrador de Rede Local, gerir as contas de utilizador da sua U/E/O, mantendo de forma dinâmica e atualizada a listagem de todos os objetos existentes na *Active Directory* referentes à sua(s) Unidade Organizacional. Para tal, deve solicitar, através do portal de Gestão de Contas as alterações necessárias, incluindo novas contas e remoção de outras, sendo que é da sua responsabilidade, sempre que existem militares ou civis aumentados ou transferidos da U/E/O, a sua atualização na estrutura de diretório dos SI do Exército;

(8) No âmbito do apoio ao utilizador, relativo à exploração do sistema de correio eletrónico do Exército, é dever do Administrador de Rede Local:

(a) Divulgar as normas técnicas relativas à "Estrutura de Segurança da Informação do Exército" e garantir que os utilizadores cumprem as diretivas emanadas superiormente relativas à utilização do sistema de correio eletrónico;

(b) Prestar assistência na configuração do correio eletrónico, incluindo a criação de pastas pessoais, e otimizar a utilização do mesmo, sensibilizando os utilizadores para a questão do "*SPAM*" e das mensagens não solicitadas;

(c) Reportar ao CTE qualquer anomalia especifica na configuração/utilização do sistema de correio eletrónico, incluindo a utilização de chaves eletrónicas e certificados digitais, permitindo a Assinatura Digital e Encriptação das mensagens de correio eletrónico com vista ao aumentado da confiança no sistema;

(d) Sensibilizar os utilizadores para que o sistema de correio eletrónico não deve ser utilizado na transmissão de mensagens classificadas acima de RESERVADO, mesmo com a utilização dos Certificados Digitais. Para a transmissão de mensagens com classificação de segurança superiores a RESERVADO, devem ser utilizadas as redes seguras existentes no Exército;

(9) No âmbito da Segurança Física, o Administrador de Rede Local é responsável por garantir que todos os equipamentos principais são mantidos em locais fechados,

nomeadamente bastidores e salas adequadas à sua Classificação de Segurança, e mantida uma coleção de chaves devidamente identificadas e guardadas com uma relação das mesmas;

(10) No âmbito da Segurança da Informação:

(a) É da responsabilidade do Administrador de Rede Local garantir uma correta ligação dos equipamentos à rede, nomeadamente com cabos certificados segundo as categorias em vigor e aprovadas pela DCSI. Todos os equipamentos devem ser autorizados e colocados no domínio *exercito.local*, e todos os parâmetros de rede, quando não obtidos de forma automática (DHCP), devem ser solicitados ao CTE, principalmente IP e DNS;

(b) O Administrador de Rede Local deve garantir que não se encontram ligados à RDE computadores/equipamentos terminais não adicionados ao domínio, institucionais ou particulares. Em situações excecionais e onde o desempenho das funções assim o obrigue, o Administrador Local após solicitar autorização ao CTE/DCSI pode permitir a utilização de equipamentos particulares na RDE;

(c) Sempre que for detetado algum equipamento não autorizado/certificado ligado na RDE deve o Administrador de Rede Local informar imediatamente do CTE desta anomalia, através de mensagem de correio eletrónico ou contacto telefónico, indicando o tipo de equipamento e o local onde foi detetada a infração. Cabe ao CTE efetuar o bloqueio de acesso aos recursos da RDE do equipamento identificado como não cumprindo com as especificações/políticas de segurança estabelecidas para o domínio;

(d) É-lhe expressamente proibido ligar computadores da rede do Exército a outras redes públicas ou privadas, sem autorização expressa do CTE;

(e) O Administrador de Rede Local tem o direito e a obrigação de inspecionar qualquer recurso da rede. Para isso, pode monitorizar toda a atividade dos recursos da rede (inclusive computadores) através de aplicações próprias, tendo presente os limites legais impostos pelas refª g) e h), de forma a prevenir e controlar possíveis violações de segurança e prestar assistência remotamente. O "*software*" a usar na assistência remota carece de autorização do CTE;

(f) Em coordenação com a DCSI, promover ações periódicas, no mínimo semestrais, de informação e sensibilização dos utilizadores para as políticas de segurança e normas técnicas de utilização dos meios CSI;

(11) Relativamente aos planos de restauro e salvaguarda da informação, é da responsabilidade do Administrador de Rede Local:

(a) Sensibilizar os utilizadores da sua U/E/O para a necessidade de planos de "*backup*" (cópia de segurança), diários e semanais, utilizando para tal o repositório de "*backup*" central no Servidor Local, em pasta partilhada criada especificamente para o efeito. O "*backup*" semanal será efetuado preferencialmente no último dia da semana e contemplará todos os ficheiros permanentes referentes a, pelo menos, uma semana. Devem ser desencorajados os procedimentos que passem por utilizar diretamente os ficheiros no servidor, mantendo estes abertos para edição, sem existir o documento original no próprio computador de trabalho;

(b) Sempre que existir informação crítica a ser guardada no Servidor Local, deve o Administrador informar formalmente o CTE, de qual ou quais as pastas, e/ou ficheiros, devem ser sujeitas a cópia de segurança para um outro dispositivo de armazenamento, nomeadamente os existentes nos Centros de Dados Regionais;

(c) Para a reposição dos ficheiros/informação corrompida acidentalmente, ou eliminada, deverá, se necessário, ser solicitado apoio ao CTE;

(d) Por razões de eficácia de gestão e de segurança, deve sensibilizar os utilizadores para a guarda dos ficheiros de trabalho ou pessoais em diretorias próprias, tanto nos computadores de trabalho, como no servidor local. Por norma, cada uma dessas diretorias deve estar acessível apenas aos utilizadores desse grupo de trabalho/secção que detêm igualmente a responsabilidade do seu conteúdo, organização, segurança e cópia de segurança. O Administrador local deve ter acesso a toda a estrutura de pastas existentes no servidor referente aos utilizadores da sua U/E/O;

(e) No caso de informação sensível, ou toda aquela que se corrompida ou indisponível devido a causa acidental/intencional cause graves constrangimentos à atividade do Exército, deverá ser incluída em Planos de Recuperação (de acordo com a sua Classificação de Segurança), sendo utilizados dispositivos de armazenamento físicos e com possibilidade de serem guardados desconectados da RDE;

(12) Em coordenação com o Gestor de Informação da U/E/O, é responsável pela atualização de conteúdos nos portais autorizados, da *Intranet* e *Internet* do Exército, referente à sua U/E/O, desde que devidamente mandatado para tal e tendo presente as limitações e pré-formatação impostas pelo Gabinete de Sua Ex.a o General Chefe de Estado-Maior do Exército, considerando o documento em refª i).

Sempre que existirem dúvidas referentes à tecnologia "*Sharepoint*" e necessidades de alteração do próprio "*Layout*", deve ser contactado o CTE.

5. INSTRUÇÕES DE COORDENAÇÃO

a. As UU/EE/OO têm a responsabilidade de adotar internamente as medidas necessárias para a implementação da presente NAT;

b. A presente NAT será revista sempre que necessário, através de proposta da DCSI e, após aprovação, terá assinalada a alteração através da numeração da versão e da data.

6. ENTRADA EM VIGOR

A presente NAT entra em vigor na data da sua assinatura.

Comando das Forças Terrestres, 28 de Janeiro de 2014

O Comandante das Forças Terrestres

Carlos António C.H. Jerónimo
TGen

CARLOS ANTÓNIO CORBAL HERNANDEZ JERÓNIMO
TGen

AUTENTICAÇÃO
O Diretor de Comunicações e Sistemas de Informação

JOSÉ FILIPE DA SILVA ARNAUT MOREIRA
MGen

ANEXOS:

Anexo A: PROCEDIMENTOS PARA GESTÃO DE INCIDENTES

DISTRIBUIÇÃO: De acordo com Lista A da NEP NAT 00.01

Anexo A (PROCEDIMENTOS PARA GESTÃO DE INCIDENTES) às NORMAS TÉCNICAS E PROCEDIMENTOS DO ADMINISTRADOR DA REDE LOCAL DAS U/E/O

1. FINALIDADE

Este anexo com procedimentos de ciberdefesa, tem por finalidade facilitar a sincronização de ações das diferentes Entidades do Exército que se enquadram na área de resposta a incidentes em redes informáticas, nomeadamente Administradores da Rede Local das U/E/O, Centro de Ciberdefesa e DCSI. Inclui eventos de ciberdefesa, cronogramas de relato e resposta, tabelas de verificação «*checklists*», Técnicas, Táticas e Procedimentos (TTP) e material de referência, necessário à implementação de uma capacidade mínima de Garantia de Informação («*Information Assurance*» - IA) e ciberdefesa.

Pretende-se assim uniformizar procedimentos e táticas relacionadas com os esforços de ciberdefesa, melhorar as relações de Comando e Controlo, de forma a garantir e manter a confidencialidade, disponibilidade e integridade dos Sistemas de Informação (SI) e da Informação neles residente e processada, bem como responder de forma coordenada a eventos de ciberdefesa, disponibilizando ao comando toda a informação relativa à situação («*situational awareness*»), necessária ao processo de tomada de decisão.

2. SITUAÇÃO

As redes militares de todos os países, incluindo a Rede de Dados do Exército (RDE), têm vulnerabilidades e enfrentam um vasto leque de ameaças aos seus SI e à informação que nela circula.

As ameaças podem apresentar uma grande variedade de fontes externas ou internas (incluindo um atacante isolado, organizações criminosas ou terroristas, atores não estatais ou elementos financiados por estados), podendo afetar de forma mais ou menos disruptiva a capacidade atual e futura de combate e de Comando e Controlo.

Vulnerabilidades das redes partilhadas e dos sistemas requerem uma coordenação operacional de proximidade e uma regular troca de informação de ciberdefesa e de IA. Tendo presente que no atual contexto de interdependência de redes de computadores, as nossas vulnerabilidades poderão ser as mesmas de outros países e que as ameaças nunca poderão ser completamente eliminadas, é crucial partilhar informação de forma proactiva, continuada, coordenada e em tempo útil, de forma a diminuir o risco global e mitigar eventuais consequências resultantes de incidentes, melhorando a capacidade de ciberdefesa e a forma como protegemos as nossas redes.

A criação de rotinas, através da execução de exercícios de ciberdefesa, contribui para melhorar e agilizar procedimentos, identificar boas práticas e melhorar a coordenação, colaboração, consciencialização e trabalho em equipa, necessários para contrariar, de forma eficaz, todos aqueles que ameacem as nossas redes.

3. EXECUÇÃO

a. Glossário

Termo	Significado em Inglês (se aplicável)	Significado em Português
ACL	Access Control List	Lista de Controlo de Acessos
ActiveX	Code that runs on Internet Explorer browser, and is included in some web sites	Código incluído em sítios web, executado pelo navegador *Internet Explorer*
AD	Active Directory	Serviço de Diretório da Microsoft
Blackhole	Blackholes (discard received data)	Buraco Negro (descartam dados recebidos)
Botmaster	Master of a Robot (computer) Network	Quem controla uma ou mais *botnets*.
Botnet	Robot (computer) Network	Rede composta por diversos computadores, normalmente milhares ou milhões, infetados e controlados por uma ou mais pessoas (*botmasters*)
CERT	Computer Emergency Response Team	Equipa de Resposta a Emergências Informáticas
CIRC	Computer Incident Response Capability	Capacidade de Resposta a Incidentes Informáticos
CSIRT	Computer Security Incident Response Team	Equipa de Resposta a Incidentes de Segurança Informática
CVE	Common Vulnerabilities and Exposures	Formato padrão de referência a vulnerabilidades
DDoS	Distributed Denial of Service	Negação de Serviços de forma distribuída
DNS	Domain Name Service	Serviço de resolução de nomes de domínio
DoS	Denial of Service	Negação de Serviços
E-mail	Electronic mail	Correio eletrónico
Exploit	Code that explores security flaw	Código que explora falha de segurança
GDH		Grupo DATA-HORA
Hacktivism	Hackers supporting causes	Atividade de Hackers em suporte a causas
IA	Information Assurance	Garantia de Informação
IDS	Intrusion Detection System	Sistema de Deteção de Intrusões
IP	Internet Protocol	Protocolo de Internet

IPS	Intrusion Prevention System	Sistema de Prevenção de Intrusões
IRC	Internet Relay Chat	Protocolo de conversação em tempo real através de mensagens de texto. Forma popular de controlo de *botnets*.
ISP	Internet Service Provider	Prestador de serviço de acesso á internet.
Javascript	Web Programming Language	Linguagem de programação web
Log	Event List	Registo de eventos
Malware	Malicious Software	Código Malicioso
Phishing	Electronic Fraud	Fraude informática
RDE		Rede de Dados do Exército
RSE		Rede Segura do Exército (Domínio Classificado do SIC-Op)
Spyware		Código malicioso que recolhe informação diversa sobre o utilizador como: hábitos de navegação na Internet, recolha de listas de contatos, certificados digitais, «*passwords*», etc.
TCP	Transmission Control Protocol	Protocolo de Controlo de Transmissão
Trojan		Programa malicioso que aparenta ter uma utilidade, disfarçando-se de algo apelativo, de forma a levar o utilizador a instala-lo (Cavalo de Troia)
TTP	Techniques, Tactics and Procedures	Técnicas, Táticas e Procedimentos
UDP	User Datagram Protocol	Protocolo de envio de pacotes personalizável pelas aplicações
U/E/O		Unidade/Estabelecimento/Orgão
URL	Uniform Resource Locator	Localizador Padrão de Recursos
Web	Global Network, Internet	A rede Global, Internet
Worm	Malicious code that spreads without human intervention	Código malicioso que se replica e infeta outras máquinas, sem intervenção humana
www	World Wide Web	Rede à escala Global
Zero-Day	Code that explorers a vulnerability, not known publically, but known by specialists / hackers	Código que explora vulnerabilidade, não divulgada publicamente, mas conhecida por especialistas / «*hackers*»

b. **Requisitos para o Relato de Incidentes**

Requisito	Exemplo
Perda de capacidade de ciberdefesa	Perda ou degradação da capacidade de ciberdefesa da RDE • Perda de «*firewalls*», Listas de Controlo de Acesso (ACL) de routers, Sistemas de Deteção de Intrusões. • Interrupção não autorizada nos serviços da RDE
Fuga de informação / Incidentes com mensagens classificadas	• Dispositivo não autorizado ligado a sistema classificado • Dispositivo não classificado ligado a sistema classificado • Dispositivo classificado ligado a um sistema não classificado
Alteração do estado de segurança de ciberdefesa	Alteração do estado de segurança de ciberdefesa devido a: • Negação Distribuída de Serviços (DDoS) • Incidente informático
Descoberta de vulnerabilidade critica não mitigada e anteriormente desconhecida	Novo «*exploit*» a «*software*», sem mitigação (Zero-Day)
Código malicioso (*Worm*, Vírus, *Trojan*)	Descoberta de código malicioso na rede
Negação de Serviço / Negação à disponibilidade	Ataque cibernético que resulta na perda de serviços de sistema ou da rede.
Intrusão / Confidencialidade	• Atividade que resulta em acesso com privilégios de administração não autorizado, comprometimento da «*Active Directory*» (AD) • Acesso físico não autorizado a sistema de informação ou à infraestrutura das redes
Garantia de Informação (IA) ou evento de rede a ser referido pela comunicação social	• «Wikileaks» • Desastre ou condições meteorológicas com impacto severo • Fóruns de «*hackers*» a descrever ações tomadas contra o Exército
Integridade	Tentativa de colocação de informação falsa em sistemas de informação do exército
Capacidades baseadas na Internet	• Ataques que utilizem Redes Sociais, sítios comerciais • Aumento da largura de banda usada (aumento > 30%) Aumento visível na exfiltração de dados

c. **Cronograma para o Relato de Incidentes**

		IMPACTO					
		Alto		**Médio**		**Baixo**	
		Backbone, *Router*, Gestão de rede, Dispositivos de Segurança (IDS, IPS, *Firewall*), Servidor Seguro.		Servidor de Rede Interna, Terminal Classificado		Servidor Publico, Terminal não Classificado	
EVENTO	**Acesso não autorizado, Ataque à Disponibilidade (DoS) ou *Malware***	**Notificação Inicial[1]**	**Enviar Relatório[2]**	**Notificação Inicial[1]**	**Enviar Relatório[2]**	**Notificação Inicial[1]**	**Enviar Relatório[2]**
➢ Atividade de rede não autorizada (Ex. *peer-to-peer*, acesso remoto, partilha de ficheiros, etc); ➢ Fraude informática, Embustes, Esquemas (*Phishing*); ➢ Interceção de informação transmitida eletronicamente; ➢ Perda ou roubo de computador ou dispositivo; ➢ Reconhecimento da Rede (Sondas Maliciosas ou *Scans*); ➢ Tentativas de Acesso falhadas (*password* errada, conteúdo bloqueado); ➢ Desconhecido.	SIM	30min	4h	1h	6h	2h	8h
	NÃO	1h	4h	2h	8h		
➢ Acesso ou modificação não autorizados a ficheiros ou sistema; ➢ Código Malicioso (Vírus, *Worms*, *Trojans*, *Spyware*, etc.); ➢ Desfiguração de Portal (incluindo Sítios Sociais); ➢ Negação de Serviços (DoS ou DDoS).	SIM	30min	4h	1h	6h		

[1] Apêndice 1 – (Formulário de Relato de Incidente)
[2] Apêndice 2 – (Formulário de Relato Técnico de Incidente)

d. **Resposta a Incidentes: Técnicas, Táticas, Procedimentos (TTP)**

PERDA OU ROUBO DE COMPUTADOR OU DISPOSITIVO DE ARMAZENAMENTO CLASSIFICADO		
Propósito: Relato e resposta a incidentes relativos a «perda ou roubo de computador ou dispositivo de armazenamento classificado»		
Ponto de Contato:		
Estado	Ação	GDH de início
Identificar	Determinar se o computador / dispositivo de armazenamento foi roubado ou perdido	
	Determinar se o item foi roubado ou perdido num local público, privado ou num local controlado pelo Exército ou por uma entidade nacional	
	Determinar quando o equipamento foi perdido ou roubado	
	Determinar se o item era classificado ou continha informação classificada	
	Obter uma curta descrição do item e evento	
	Registar pessoas/autoridades civis que foram notificadas	
	Determinar o nível de classificação mais elevado de acesso	
	Determinar o grau de comprometimento da segurança do sistema: Integridade de informação, disponibilidade do sistema, confidencialidade de informação ou do sistema, ou desconhecido	
Informar	Fornecer a notificação inicial ao escalão superior, dependendo do risco de acesso não autorizado, nos prazos de: 30min/1h – Impacto alto, 1h/2h - impacto médio, 2h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8, para conhecimento de situação (quem, o quê, quando, onde e como), com informação básica necessária para conhecimento da situação, incluindo a classificação de segurança do sistema, sistema operativo, certificados digitais, entre outros detalhes.	
Investigar	Efetuar avaliação de impacto nos recursos (sem impacto, impacto baixo, impacto moderado, impacto elevado)	
	Fornecer estimativa de impacto • Impacto nas operações ou exercícios do Exército; • Danos à reputação; • Ameaças de ação legal por afetar terceiros; • Perda de ligação ao ISP devido a violação da política de utilização responsável (contrato com o ISP); • Disrupção/comprometimento com uma ou mais redes de terceiros*; (* No caso do nosso sistema ser comprometido e utilizado para atacar outros sítios)	

	Fornecer uma suspeita do motivo principal, como por exemplo: • Ganho financeiro ilícito • Utilização de recursos do sistema para uso pessoal • Vantagem de instituições/governos estrangeiros (espionagem ou sabotagem) • Protesto político, causas populares («*hacktivism*») • Dano malicioso • Demonstração de capacidades ofensivas • Utilização de recursos do sistema para efetuar novos ataques • Indiscriminado (o ataque foi resultado de uma escolha aleatória, através da conetividade à internet) • Desconhecido	
	Submeter ao escalão superior, dependendo do risco de acesso não autorizado, nos prazos de: 4h – Impacto alto, 6h/8h - impacto médio, 8h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8, após deteção do roubo/perda.	
	Continuar a relatar nas 24 horas seguintes até ao encerramento	
	Fornecer o relatório final dentro de 7 dias, após encerramento e incluir análise de impacto na missão	
	Recomendar treino corretivo para os utilizadores	

FRAUDE INFORMÁTICA, EMBUSTES, ESQUEMAS (PHISHING)		
Propósito: Fornecer procedimentos para a resposta a incidentes que envolvam *e-mails* suspeitos de incluir fraude, embustes ou esquemas.		
Ponto de Contato:		
Estado	Ação	GDH de início
Identificar	Receber notificação sobre receção de *e-mails* com conteúdo malicioso/fraudulento	
	Tentar perceber a intenção do conteúdo malicioso, por exemplo: • Números de cartões de crédito roubados ou ilicitamente gerados, credenciais de serviços bancários «*online*»; • Acesso fraudulento a serviços de transmissão de informação e de telecomunicações; • Transferências não autorizada de fundos; • Promoção «*online*» de investimentos fraudulentos; • Mensagens de correio eletrónico, portais de serviços de correio eletrónico ou de redes sociais falsos, para facilitarem acesso fraudulento a contas financeiras/fundos dos utilizadores ou a credenciais de início de sessão dos utilizadores nas redes do Exército; • Outros	
	Verificar se utilizador • Reencaminhou a mensagem de correio eletrónico; • Clicou em alguma hiperligação incluída na mensagem; • Partilhou informação pessoal; • Outros.	
	Investigar em base de dados nacionais por variantes no campo «assunto» e informação associada ao remetente	
Isolar	Mitigar imediatamente eventos de rede anormais ou adversos se for encontrado código malicioso ativo na rede • Isolar o sistema; • Bloquear a conta de utilizador; • Bloquear atividade maliciosa	
Informar	Fornecer a notificação inicial ao escalão superior, dependendo do risco de acesso não autorizado, nos prazos de: 30min/1h – Impacto alto, 1h/2h - impacto médio, 2h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8, para conhecimento de situação (quem, o quê, quando, onde e como). Fornecer os endereços de origem e destino, portos TCP/UDP comuns, outros protocolos, tipo de terminal/dispositivo, dimensão da rede afetada, classificação de segurança, sistema operativo, vulnerabilidade, referência CVE associada, detalhes sobre o «*exploit*». **Enviar o e-mail suspeito como <u>anexo</u> e com o assunto: "ATENÇÃO: e-mail suspeito"**	

	Esboçar mensagem de alerta para distribuição • Procura direta por conteúdo malicioso através do campo «assunto», «remetente» ou outro conteúdo único na mensagem eletrónica (hiperligação, anexo); • Remoção das mensagens maliciosas das caixas de correio, nos servidores; • Bloqueio da hiperligação de acesso direto ao servidor de tentativa de «*phishing*» (porta, IP/DNS, etc); • Bloqueio de futuras mensagens de *e-mail* do mesmo remetente ou com um assunto específico; • Procura de registos sobre transferência de ficheiros associados ao endereço IP e suas sub-redes ou sítios ou tempo; • Rever registos de eventos (*logs*) de grandes transferências de ficheiros, normalmente com duração coincidente com os incidentes de *e-mail*; • Relatar tentativas de ligação • Relatar todas as descobertas, incluindo respostas negativas	
	Informar os utilizadores da rede da gravidade da ameaça e das restrições adicionais impostas. Identificar claramente ações que serão necessárias para ajudar a reduzir o risco durante as atividades da missão. Quando possível, educá-los sobre as consequências do comprometimento da rede, para que compreendam a razão para as medidas de segurança adicionais e até que ponto poderá ter sido afetada a disponibilidade, confidencialidade ou integridade das suas atividades na missão.	
Investigar	Determinar quais os utilizadores que clicaram na hiperligação, obter informação da hiperligação, qualquer exfiltração/infiltração de ficheiros e número de estações de trabalho afetadas	
Mitigar	Analisar e avaliar os danos causados • Assegurar que os Antivírus e «*anti-spyware*» estão instalados, a funcionar e atualizados; • Procurar por código malicioso; • Monitorizar entradas consideradas críticas, no registo do Sistema Operativo; • Considerar a possibilidade de utilização de políticas de grupo para bloquear opções do navegador de *Internet*, desativar «*Javascript*», controlos ActiveX e capacidades similares (permitir *scripts* apenas se funções criticas para a missão não puderem ser feitas de outra forma); • Procurar informação de segurança relacionada, em fóruns especializados e fidedignos; • Efetuar/solicitar análise ao «*malware*».	
	Determinar grau de comprometimento da segurança do sistema: integridade de informação, disponibilidade de sistema, confidencialidade de informação e sistema, ou desconhecido	

	Efetuar avaliação de impacto nos recursos (sem impacto, impacto baixo, impacto moderado ou impacto elevado)	
	Fornecer estimativa de impacto • Impacto nas operações ou exercícios do Exército; • Danos à reputação; • Ameaças de ação legal por afetar terceiros; • Perda de ligação ao ISP devido a violação da política de utilização responsável (contrato com o ISP); • Disrupção/comprometimento com uma ou mais redes de terceiros*; (* No caso do nosso sistema ser comprometido e utilizado para atacar outros sítios)	
	Fornecer uma suspeita do motivo principal, como por exemplo: • Ganho financeiro ilícito • Utilização de recursos do sistema para uso pessoal • Vantagem de instituições/governos estrangeiros (espionagem ou sabotagem) • Protesto político, causas populares (*hacktivism*) • Dano malicioso • Demonstração de capacidades ofensivas • Utilização de recursos do sistema para efetuar novos ataques • Indiscriminado (o ataque foi resultado de uma escolha aleatória, através da conetividade à internet) • Desconhecido	
	Submeter ao escalão superior, dependendo do risco de acesso não autorizado, nos prazos de: 4h – Impacto alto, 6h/8h - impacto médio, 8h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8.	
	Continuar a relatar nas 24 horas seguintes até ao encerramento	
	Fornecer o relatório de atividade	
	Fornecer o relatório final dentro de 7 dias, após encerramento e incluir análise de impacto na missão	
	Recomendar treino corretivo para os utilizadores	

ACESSO OU MODIFICAÇÃO NÃO AUTORIZADOS A FICHEIROS OU SISTEMA		
Propósito: Fornecer procedimentos para resposta a incidentes do tipo: acesso não autorizado ou modificação do sistema ou ficheiros (intrusões tanto com privilégios administrativos como de utilizador)		
Ponto de Contato:		
Estado	Ação	GDH de início
Identificar	Potencial reconhecimento de evento de segurança significativo, que constitua uma ameaça às redes do Exército, através de atividade suspeita e identificada através de relatórios da rede ou relatórios de sensores da rede, etc. • Determinar a localização do sistema afetado • Efetuar uma avaliação inicial para determinar a natureza e a validade ou relatar como incidente de segurança real.	
Isolar	Mitigar imediatamente eventos anormais ou adversos • Isolar o sistema • Bloquear a conta de utilizador • Bloquear atividade maliciosa • Rever registo de chaves críticas, procurando por alterações • Assegurar que o Antivírus / «*anti-spyware*» está instalado, atualizado e a funcionar.	
Informar	Fornecer a notificação inicial ao escalão superior, nos prazos de: 30min – Impacto alto, 1h - impacto médio, 2h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8, para conhecimento de situação (quem, o quê, quando, onde e como), endereços de origem e de destino, portos TCP/UDP comuns, outros protocolos, tipo de dispositivo anfitrião, dimensão da rede afetada, classificação de segurança, sistema operativo, vulnerabilidade, CVE associado, detalhes do «*exploit*».	
	Informar os utilizadores de rede da gravidade da ameaça e as restrições sob as quais eles operam, limitar a informação nas redes se ainda houver suspeitas de adversários a operar na rede. Identificar claramente ações que serão necessárias para ajudar a reduzir o risco durante as atividades da missão. Quando possível, educá-los sobre a extensão do comprometimento da rede, para que compreendam a razão para as medidas de segurança adicionais e até que ponto a disponibilidade, a confidencialidade ou integridade das suas atividades de missão podem ser afetadas.	
Investigar	• Entrevistar utilizadores afetados; • Rever relatórios de auditoria; • Validar evento/incidente; • Avaliar a extensão da intrusão; • Rever o impacto na operacionalidade; • Verificar com a rede nacional de CSIRT e/ou NATO NCIRC se existe mais informação sobre a atividade em curso; • Efetuar cópia do disco rígido para análise forense.	

	Descrever o acesso ou alteração não autorizados • Leitura/cópia de ficheiros classificados do Exército/Nacionais (nível de classificação); • Leitura/cópia de ficheiros não classificados do Exército/Nacionais; • Modificação/exclusão de ficheiros do Sistema Operativo; • Modificação/exclusão de ficheiros de informação; • Ferramentas de ataque instaladas, ex. *Rootkit*, ferramentas DDoS; • Material ilegal instalado, licenças pirateadas ou violação de direitos de autor/propriedade intelectual; • *Software* instalado para facilitar maior controlo de sistemas, ex. IRC bot; • Ficheiros desconhecidos instalados; • Desconhecido	
	Descrever a sensibilidade dos ficheiros que foram comprometidos • Atacante acedeu a algum ficheiro/informação em toda a rede; • Atacante acedeu a ficheiros do sistema; • Atacante acedeu a informação sensível (ex: *passwords*); • Atacante acedeu a ficheiros de utilizadores; • Atacante acedeu a documentação classificada; • Atacante acedeu a outro material confidencial; • Desconhecido	
Mitigar	Recuperar e instalar novo disco a partir de cópia de segurança • Implementar o bloqueio de endereços IP ou efetuar alterações ao DNS de forma a parar o tráfego («*blackhole*»); • A operação de recuperação numa rede comprometida deve ser cuidadosa e sempre com autorização e indicações técnicas do Centro de Ciberdefesa; • Revalidar contas de utilizadores/administradores. Desativar as contas que não sejam válidas; • Forçar a mudança de palavras passe nas contas, base de dados e início de sessão remotos. Assegurar que alterações a contas, como as de base de dados, que são muitas vezes acessíveis através de aplicações, são alteradas de forma coordenada com os utilizadores e/ou equipas de desenvolvimento de aplicações; • Procurar equipamento/redes sem fios, não autorizados. • Documentar lições aprendidas; • Documentar atividades de treino associadas ao incidente.	
	Determinar o grau de comprometimento da segurança do sistema: integridade de informação, disponibilidade de sistema, confidencialidade de informação e sistema, ou desconhecido	
	Efetuar avaliação de impacto nos recursos (sem impacto, impacto baixo, impacto moderado ou impacto elevado)	

	Fornecer estimativa de impacto • Impacto nas operações ou exercícios do Exército; • Danos à reputação; • Ameaças de ação legal por afetar terceiros; • Perda de ligação ao ISP devido a violação da política de utilização responsável (contrato com o ISP); • Disrupção/comprometimento com uma ou mais redes de terceiros*; (* No caso do nosso sistema ser comprometido e utilizado para atacar outros sítios)	
	Fornecer uma suspeita do motivo principal, como por exemplo: • Ganho financeiro ilícito • Utilização de recursos do sistema para uso pessoal • Vantagem de instituições/governos estrangeiros (espionagem ou sabotagem) • Protesto político, causas populares (*hacktivism*) • Dano malicioso • Demonstração de capacidades ofensivas • Utilização de recursos do sistema para efetuar novos ataques • Indiscriminado (o ataque foi resultado de uma escolha aleatória, através da conetividade à internet) • Desconhecido	
	Submeter ao escalão superior, nos prazos de: 4h – Impacto alto, 6h - impacto médio, 8h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8.	
	Continuar a relatar nas 24 horas seguintes até ao encerramento	
	Fornecer o relatório de atividade	
	Fornecer o relatório final dentro de 7 dias, após encerramento e incluir análise de impacto na missão	
	Recomendar treino corretivo para os utilizadores	

DESFIGURAÇÃO DE PORTAL (INCLUINDO SÍTIOS SOCIAIS)		
Propósito: Relato e procedimentos para resposta a incidentes do tipo «desfiguração de portal» (*web site defacement*)		
Pontos de Contato:		
Estado	Ação	GDH de início
Identificar	Potencial reconhecimento de evento de segurança significativo que constitua uma ameaça a portais do Exército, através de atividade suspeita, identificado através de relatórios da rede, relatórios de sensores de rede, alerta de utilizadores, etc. • Determinar a localização do sistema afetado • Efetuar uma avaliação inicial para determinar a natureza e a validade ou relatar como incidente de segurança real.	
Isolar	Mitigar imediatamente eventos anormais ou adversos • Isolar o sistema • Bloquear a atividade do administrador web • Bloquear atividade maliciosa • Notificação inicial do incidente ao escalão superior	
Informar	Fornecer a notificação inicial ao escalão superior, nos prazos de: 30min – Impacto alto, 1h - impacto médio, 2h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8, para conhecimento de situação (quem, o quê, quando, onde e como), endereços de origem e destino, portos TCP/UDP comuns, outros protocolos, tipo de dispositivo anfitrião, dimensão da rede afetada, classificação de segurança, sistema operativo, vulnerabilidade, detalhes CVE sobre este «*exploit*».	
	Informar os utilizadores de rede da gravidade da ameaça e as restrições sob as quais eles operam, limitar a informação nas redes se ainda houver suspeitas de adversários a operar na rede. Identificar claramente ações que serão necessárias para ajudar a reduzir o risco durante as atividades da missão. Quando possível, educá-los sobre a extensão do comprometimento da rede, para que compreendam a razão para as medidas de segurança adicionais e até que ponto a disponibilidade, a confidencialidade ou integridade das suas atividades de missão podem ser afetadas.	

Investigar	• Rever relatórios de auditoria; • Validar eventos/incidentes; • Avaliar a extensão da intrusão; • Rever o impacto operacional; • Verificar com a rede nacional de CSIRT e o NATO NCIRC se existe mais informação sobre a atividade em curso; • Requerer assistência com atividade forense, se necessário; • Identificar a rede onde está o servidor web desfigurado; • Fornecer a hiperligação completa do sítio desfigurado; • Fornecer a plataforma e a versão da aplicação servidor web; • Fornecer o propósito do portal; • Fornecer os detalhes do conteúdo da desfiguração; • Anexar "*print screens*" ou fotografias/imagens do portal desfigurado	
Mitigar	Recuperar e instalar novo disco a partir de cópia de segurança • Implementar o bloqueio de endereços IP ou efetuar alterações ao DNS de forma a parar o tráfego («*blackhole*»); • Assegurar que o Antivírus/«*anti-spyware*» está instalado, atualizado e a funcionar; • Utilizar início de sessão remoto com «*software*» fidedigno e com conta de utilizador segura e com autenticação; • Rever requisitos para acesso remoto. Assegurar que é utilizada uma «*password*» complexa e a sua alteração é efetuada de forma regular e sem repetir *passwords* anteriormente utilizadas; • Documentar lições aprendidas.	
	Determinar o grau de comprometimento da segurança do sistema: integridade de informação, disponibilidade de sistema, confidencialidade de informação e sistema, ou desconhecido	
	Efetuar avaliação de impacto nos recursos (sem impacto, impacto baixo, impacto moderado ou impacto elevado)	
	Fornecer estimativa de impacto • Impacto nas operações ou exercícios do Exército; • Danos à reputação; • Ameaças de ação legal por afetar terceiros; • Perda de ligação ao ISP devido a violação da política de utilização responsável (contrato com o ISP); • Disrupção/comprometimento com uma ou mais redes de terceiros*; (* No caso do nosso sistema ser comprometido e utilizado para atacar outros sítios)	

	Fornecer uma suspeita do motivo principal, como por exemplo: • Ganho financeiro ilícito • Utilização de recursos do sistema para uso pessoal • Vantagem de instituições/governos estrangeiros (espionagem ou sabotagem) • Protesto político, causas populares («*hacktivism*») • Dano malicioso • Demonstração de capacidades ofensivas • Utilização de recursos do sistema para efetuar novos ataques • Indiscriminado (o ataque foi resultado de uma escolha aleatória, através da conetividade à internet) • Desconhecido	
	Submeter ao escalão superior, nos prazos de: 4h – Impacto alto, 6h - impacto médio, 8h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8.	
	Continuar a relatar nas 24 horas seguintes até ao encerramento	
	Fornecer o relatório de atividade	
	Fornecer o relatório final dentro de 7 dias, após encerramento e incluir análise de impacto na missão	
	Recomendar treino corretivo para os administradores web	

NEGAÇÃO DE SERVIÇOS (DoS OU DDoS) INCLUINDO MEIOS ELETRÓNICOS DISRUPTIVOS /NEGAÇÃO À DISPONIBILIDADE		
Propósito: Relato e procedimentos para resposta a incidentes do tipo «*Denial of Service*» (DoS), ou «*Distributed Denial of Service*» (DDoS), disrupção de serviços através de meios eletrónicos.		
Ponto de Contato:		
Estado	Ação	GDH de início
Identificar	Potencial reconhecimento de evento de segurança significativo que constitua uma ameaça às redes da Exército através de atividade suspeita, identificado através de relatórios da rede, relatórios de sensores de rede, etc. • Determinar a localização do sistema afetado • Determinar a origem, Porto/Protocolo do «*exploit*» em questão	
Isolar	Mitigar imediatamente eventos anormais ou adversos • Implementar controlos de acesso (bloqueando os atacantes) no «*router*» e na «*firewall*» do local onde é feita a entrada do trafego dos atacantes	
Informar	Fornecer a notificação inicial ao escalão superior, nos prazos de: 30min – Impacto alto, 1h - impacto médio, 2h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8, para conhecimento de situação (quem, o quê, quando, onde e como), endereços de origem e destino, portos TCP/UDP comuns, outros protocolos, tipo de dispositivo anfitrião, dimensão da rede afetada, classificação de segurança, sistema operativo, vulnerabilidade, detalhes CVE sobre este «*exploit*».	
	Informar os utilizadores de rede da gravidade da ameaça e as restrições sob as quais eles operam, limitar a informação nas redes se ainda houver suspeitas de adversários a operar na rede. Identificar claramente ações que serão necessárias para ajudar a reduzir o risco durante as atividades da missão. Quando possível, educá-los sobre a extensão do comprometimento da rede, para que compreendam a razão para as medidas de segurança adicionais e até que ponto a disponibilidade, a confidencialidade ou integridade das suas atividades de missão podem ser afetadas.	
Investigar	• Rever relatórios de auditoria; • Validar eventos/incidentes; • Avaliar a extensão da intrusão; • Rever o impacto operacional; • Verificar com a rede nacional de CSIRT e o NATO NCIRC se existe mais informação sobre a atividade em curso; • Requerer assistência com atividade forense, se necessário;	

	Determinar o tipo de Negação de Serviços • Negação de Serviços (DoS) não distribuído, através do consumo de largura de banda; • Negação de Serviços Distribuída (DDoS) verificada através do consumo de largura de banda; • Ações para bloquear ou degradar o desempenho do servidor ou servidores; • Ações para negar o acesso a serviços, ativando medidas de segurança automáticas (ex. bloqueio de contas, bloqueio de portas, ativação de regras de IPS, etc.); Determinar qual o Serviço/Sistema que foi atacado. Fornecer informação no decorrer do ataque. Determinar o consumo de largura de banda do ataque.	
Mitigar	Verificar com a rede nacional de CSIRT se existem atividades relacionadas adicionais • Monitorizar a situação para assegurar a não reincidência de negações de serviço DoS/DDoS vindos de outros endereços IP; • Investigar atividades adicionais da gama de IP's envolvida; • Documentar lições aprendidas	
	Determinar o comprometimento de segurança do sistema: integridade de informação, disponibilidade de sistema, confidencialidade de informação e sistema, ou desconhecido	
	Efetuar avaliação de impacto nos recursos (sem impacto, impacto baixo, impacto moderado ou impacto elevado)	
	Fornecer estimativa de impacto • Impacto nas operações ou exercícios do Exército; • Danos à reputação; • Ameaças de ação legal por afetar terceiros; • Perda de ligação ao ISP devido a violação da política de utilização responsável (contrato com o ISP); • Disrupção/comprometimento com uma ou mais redes de terceiros*; (* No caso do nosso sistema ser comprometido e utilizado para atacar outros sítios)	
	Fornecer uma suspeita do motivo principal, como por exemplo: • Ganho financeiro ilícito • Utilização de recursos do sistema para uso pessoal • Vantagem de instituições/governos estrangeiros (espionagem ou sabotagem) • Protesto político, causas populares («*hacktivism*») • Dano malicioso • Demonstração de capacidades ofensivas • Utilização de recursos do sistema para efetuar novos ataques • Indiscriminado (o ataque foi resultado de uma escolha aleatória, através da conetividade à internet) • Desconhecido	

	Submeter ao escalão superior, nos prazos de: 4h – Impacto alto, 6h - impacto médio, 8h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8.	
	Continuar a relatar nas 24 horas seguintes até ao encerramento	
	Fornecer o relatório de atividade	
	Fornecer o relatório final dentro de 7 dias, após encerramento e incluir análise de impacto na missão	

INTERCEÇÃO DE INFORMAÇÃO TRANSMITIDA ELETRONICAMENTE		
Propósito: Relato e procedimentos para resposta a incidentes do tipo «interceção de informação transmitida eletronicamente»		
Ponto de Contato:		
Estado	Ação	GDH de início
Identificar	Potencial reconhecimento de evento de segurança significativo que constitua uma ameaça às redes do Exército através de atividade suspeita, identificado através de relatórios da rede, relatórios de sensores de rede, etc. • Determinar o método de interceção	
Isolar	Mitigar imediatamente eventos anormais ou adversos • Isolar o sistema; • Bloquear conta de utilizador; • Bloquear atividade maliciosa	
Informar	Fornecer a notificação inicial ao escalão superior, dependendo do risco de acesso não autorizado, nos prazos de: 30min/1h – Impacto alto, 1h/2h - impacto médio, 2h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8, para conhecimento de situação (quem, o quê, quando, onde e como), endereços de origem e destino, portos TCP/UDP comuns, outros protocolos, tipo de dispositivo anfitrião, dimensão da rede afetada, classificação de segurança, sistema operativo, vulnerabilidade	
Investigar	• Rever relatórios de auditoria; • Validar eventos/incidentes; • Avaliar a extensão da intrusão; • Rever o impacto operacional; • Verificar com a rede nacional de CSIRT e o NATO NCIRC se existe mais informação sobre a atividade em curso; • Requerer assistência com atividade forense, se necessário	
Mitigar	Verificar com a rede nacional de CSIRT e o NATO NCIRC se existe mais informação sobre a atividade em curso	
	Determinar o comprometimento de segurança do sistema: integridade de informação, disponibilidade de sistema, confidencialidade de informação e sistema, ou desconhecido	
	Efetuar avaliação de impacto nos recursos (sem impacto, impacto baixo, impacto moderado ou impacto elevado)	
	Fornecer estimativa de impacto • Impacto nas operações ou exercícios do Exército; • Danos à reputação; • Ameaças de ação legal por afetar terceiros; • Perda de ligação ao ISP devido a violação da política de utilização responsável (contrato com o ISP); • Disrupção/comprometimento com uma ou mais redes de terceiros*; (* No caso do nosso sistema ser comprometido e utilizado para atacar outros sítios)	

	Fornecer uma suspeita do motivo principal, como por exemplo: • Ganho financeiro ilícito • Utilização de recursos do sistema para uso pessoal • Vantagem de instituições/governos estrangeiros (espionagem ou sabotagem) • Protesto político, causas populares («*hacktivism*») • Dano malicioso • Demonstração de capacidades ofensivas • Utilização de recursos do sistema para efetuar novos ataques • Indiscriminado (o ataque foi resultado de uma escolha aleatória, através da conetividade à internet) • Desconhecido	
	Submeter ao escalão superior, dependendo do risco de acesso não autorizado, nos prazos de: 4h – Impacto alto, 6h/8h - impacto médio, 8h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8.	
	Continuar a relatar nas 24 horas seguintes até ao encerramento	
	Fornecer o relatório de atividade	
	Fornecer o relatório final dentro de 7 dias, após encerramento e incluir análise de impacto na missão	

CÓDIGO MALICIOSO (VÍRUS, *WORM*, *TROJAN*, ETC.)		
Propósito: Relato e resposta a incidentes do tipo «código malicioso» (ou lógica maliciosa) em redes e sistemas		
Ponto de Contato:		
Estado	Ação	GDH de início
Identificar	Potencial reconhecimento de evento de segurança significativo que constitua uma ameaça às redes do Exército através de atividade suspeita, identificado através de relatórios da rede, relatórios de sensores de rede, etc. • Determinar o local do sistema infetado; • Determinar o método de propagação; • Determinar se a intenção da lógica maliciosa é: o Obter informação de segurança nacional; o Obter acesso às redes do Exército; o Roubo de identidade pessoal; • Determinar a gravidade da infeção do sistema: o Severo: Exploração de vulnerabilidade não conhecida (*Zero Day exploit)*, novo processo não reconhecido ou escondido, código dissimulado com o código ou drivers do Sistema Operativo e vírus; o Moderado: Ferramenta de ataque distribuído a redes ou um serviço malicioso, ferramentas de acesso remoto não autorizadas, Cavalos de Troia ou ferramenta de acesso clandestino dissimulado (*backdoor*)	
Isolar	Mitigar imediatamente eventos anormais ou adversos • Isolar o sistema; • Bloquear a conta do utilizador; • Bloquear/parar atividade maliciosa;	
Informar	Fornecer a notificação inicial ao escalão superior, nos prazos de: 30min – Impacto alto, 1h - impacto médio, 2h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8, para conhecimento de situação (quem, o quê, quando, onde e como), endereços de origem e destino, portos TCP/UDP comuns, outros protocolos, tipo de dispositivo anfitrião, dimensão da rede afetada, classificação de segurança, sistema operativo e vulnerabilidade.	
	Informar os utilizadores de rede da gravidade da ameaça e as restrições sob as quais eles operam, limitar a informação nas redes se ainda houver suspeitas de adversários a operar na rede. Identificar claramente ações que serão necessárias para ajudar a reduzir o risco durante as atividades da missão. Quando possível, educá-los sobre a extensão do comprometimento da rede, para que compreendam a razão para as medidas de segurança adicionais e até que ponto a disponibilidade, a confidencialidade ou integridade das suas atividades de missão podem ser afetadas.	

Investigar	• Rever relatórios de auditoria; • Validar eventos/incidentes; • Avaliar a extensão da intrusão; • Rever o impacto operacional; • Verificar com a rede nacional de CSIRT e o NATO NCIRC se existe mais informação sobre a atividade em curso; • Requerer assistência de atividade forense, se necessário.	
	Desenvolver um alerta para a rede nacional de CSIRT • Referir a forma de detetar o código malicioso e solicitar cooperação de forma a conter mais rapidamente a ameaça; • Fornecer instruções de como remover o código malicioso de servidores e estações de trabalho; • Solicitar aos parceiros nacionais o bloqueio de ligações ao sítio malicioso (bloquear porto, bloquear IP/DNS, IP *blackhole*); • Solicitar aos parceiros nacionais informação sobre transferência de ficheiros com destino aos endereços IP, sub-redes ou sítios relacionados com o incidente; • Identificar e rever qualquer tentativa de ligação; • Identificar utilizadores que possam ter executado o código malicioso; Determinar o nome e o endereço de destino (DNS e endereço IP) que estejam evolvidos em incidentes anteriores ou atuais, que afetem operações em curso ou necessitem de ações de reativas relevantes.	
Recuperar	Recuperar e instalar novo disco a partir de cópia de segurança • Implementar o bloqueio de endereços IP ou efetuar alterações ao DNS de forma a parar o tráfego («*blackhole*»); • Assegurar que o Antivírus/«*anti-spyware*» está instalado, atualizado e a funcionar; • Rever registos de modificação das configurações para assegurar que apenas existem alterações autorizadas; • Documentar lições aprendidas; • Documentar atividades de treino associadas a este incidente	
	Determinar o grau de comprometimento da segurança do sistema: integridade de informação, disponibilidade de sistema, confidencialidade de informação e sistema ou desconhecido	
	Efetuar avaliação de impacto nos recursos (sem impacto, impacto baixo, impacto moderado ou impacto elevado)	

	Fornecer estimativa de impacto • Impacto nas operações ou exercícios do Exército; • Danos à reputação; • Ameaças de ação legal por afetar terceiros; • Perda de ligação ao ISP devido a violação da política de utilização responsável (contrato com o ISP); • Disrupção/comprometimento com uma ou mais redes de terceiros*; (* No caso do nosso sistema ser comprometido e utilizado para atacar outros sítios)	
	Fornecer uma suspeita do motivo principal, como por exemplo: • Ganho financeiro ilícito • Utilização de recursos do sistema para uso pessoal • Vantagem de instituições/governos estrangeiros (espionagem ou sabotagem) • Protesto político, causas populares («*hacktivism*») • Dano malicioso • Demonstração de capacidades ofensivas • Utilização de recursos do sistema para efetuar novos ataques • Indiscriminado (o ataque foi resultado de uma escolha aleatória, através da conetividade à internet) • Desconhecido	
	Submeter ao escalão superior, dependendo do risco de acesso não autorizado, nos prazos de: 4h – Impacto alto, 6h - impacto médio, 8h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8.	
	Continuar a relatar nas 24 horas seguintes até ao encerramento	
	Fornecer o relatório de atividade	
	Fornecer o relatório final dentro de 7 dias, após encerramento e incluir análise de impacto na missão	
	Recomendar treino corretivo para os utilizadores.	

RECONHECIMENTO DA REDE (SONDAS MALICIOSAS OU *SCANS*)		
Propósito: Relato e procedimentos para resposta a incidentes do tipo «reconhecimento da rede» onde se incluem sondas maliciosas e análise a serviços da rede.		
Estado	Ação	GDH de início
Identificar	Potencial reconhecimento de evento de segurança significativo que constitua uma ameaça às redes do Exército através de atividade suspeita, identificado através de relatórios da rede, relatórios de sensores de rede, etc. Indicadores limite para investigação: • Número elevado de sistemas alvo de pesquisas (contagem ao longo do tempo), toda a rede alvo de pesquisa; • Endereços IP correlacionado com incidente anterior; • Pesquisa relacionada a equipamentos com dependência funcional (todos os IDS, servidores de e-mail, routers, etc.)	
Isolar	Colaboração é a chave para definir medidas de proteção contra a ameaça • Identificar equipamentos da rede que foram alvo do sistema anfitrião; • Origem do ataque; • Implementar níveis de bloqueios (router ou firewall); • Identificar atividades anteriores semelhantes	
Informar	Fornecer a notificação inicial ao escalão superior, dependendo do risco de acesso não autorizado, nos prazos de: 30min/1h – Impacto alto, 1h/2h - impacto médio, 2h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8, para conhecimento de situação (quem, o quê, quando, onde e como), endereços de origem e destino, portos TCP/UDP comuns, outros protocolos, tipo de dispositivo anfitrião, dimensão da rede afetada, classificação de segurança, sistema operativo e vulnerabilidade.	
Investigar	• Rever relatórios de auditoria; • Validar eventos/incidentes; • Avaliar a extensão da intrusão; • Rever o impacto operacional; • Verificar com a rede nacional de CSIRT e o NATO NCIRC se existe mais informação sobre a atividade em curso; • Requerer assistência de atividade forense, se necessário;	
	Desenvolver um alerta para a rede Nacional CSIRT • Referir a forma de detetar o código malicioso e solicitar cooperação de forma a conter rapidamente a ameaça; • Identificar e rever quaisquer tentativas de ligações; • Determinar a natureza provável das sondas/pesquisas: atividade «*worm*», ferramenta automática de pesquisa; • Fornecer nome do «*worm*» ou ferramenta, se conhecido.	

Mitigar	• Implementar o bloqueio de endereços IP ou efetuar alterações ao DNS de forma a parar o tráfego («*blackhole*»); • Documentar lições aprendidas; • Documentar atividade adicional associada a este incidente.	
	Determinar o grau de comprometimento da segurança do sistema: integridade de informação, disponibilidade de sistema, confidencialidade de informação e sistema, ou desconhecido	
	Efetuar avaliação de impacto nos recursos (sem impacto, impacto baixo, impacto moderado ou impacto elevado)	
	Fornecer estimativa de impacto • Impacto nas operações ou exercícios do Exército; • Danos à reputação; • Ameaças de ação legal por afetar terceiros; • Perda de ligação ao ISP devido a violação da política de utilização responsável (contrato com o ISP); • Disrupção/comprometimento com uma ou mais redes de terceiros*; (* No caso do nosso sistema ser comprometido e utilizado para atacar outros sítios)	
	Fornecer uma suspeita do motivo principal, como por exemplo: • Ganho financeiro ilícito • Utilização de recursos do sistema para uso pessoal • Vantagem de instituições/governos estrangeiros (espionagem ou sabotagem) • Protesto político, causas populares («*hacktivism*») • Dano malicioso • Demonstração de capacidades ofensivas • Utilização de recursos do sistema para efetuar novos ataques • Indiscriminado (o ataque foi resultado de uma escolha aleatória, através da conetividade à Internet) • Desconhecido	
	Submeter ao escalão superior, dependendo do risco de acesso não autorizado, nos prazos de: 4h – Impacto alto, 6h/8h - impacto médio, 8h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8.	
	Continuar a relatar nas 24 horas seguintes até ao encerramento	
	Fornecer o relatório de atividade	
	Fornecer o relatório final dentro de 7 dias, após encerramento e incluir análise de impacto na missão	

DESCONHECIDO		
Propósito: Relato, análise e resposta a eventos desconhecidos, que possam estar relacionados com atividade anómala na rede		
Ponto de Contato:		
Estado	Ação	GDH de início
Identificar	Potencial reconhecimento de evento de segurança significativo que constitua uma ameaça às redes do Exército através de atividade suspeita, identificado através de relatórios da rede, relatórios de sensores de rede, etc. Indicadores para investigação: • *«Peer-to-peer»*, «*software*» de partilha de ficheiros, *software* não aprovado, etc.; • Determinar local/identificar sistema	
Isolar	• Determinar equipamento de rede alvo do sistema anfitrião; • Fonte do ataque; • Bloquear conta; • Identificar atividades anteriores similares	
Informar	Fornecer a notificação inicial ao escalão superior, dependendo do risco de acesso não autorizado/afetação de disponibilidade/existência de *malware*, nos prazos de: 30min/1h – Impacto alto, 1h/2h - impacto médio, 2h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8, para conhecimento de situação (quem, o quê, quando, onde e como), endereços de origem e destino, portos TCP/UDP comuns, outros protocolos, tipo de dispositivo anfitrião, dimensão da rede afetada, classificação de segurança, sistema operativo e vulnerabilidade.	
Investigar	• Rever relatórios de auditoria; • Validar eventos/incidentes; • Avaliar a extensão da intrusão; • Rever o impacto operacional; • Verificar com a rede nacional de CSIRT e o NATO NCIRC se existe mais informação sobre a atividade em curso; • Requerer assistência de atividade forense, se necessário;	
	Desenvolver Alerta • Troca de informação com a rede CSIRT nacional, sobre atividades similares em curso; • Identificar e rever qualquer tentativa de ligações; • Determinar a natureza provável das sondas/pesquisas: atividade «*worm*», ferramenta de pesquisa automática; • Fornecer nome de atividade anómala se conhecido.	

Mitigar	• Remover «*software*» não autorizado; • Documentar lições aprendidas	
	Determinar o grau de comprometimento da segurança do sistema: integridade de informação, disponibilidade de sistema, confidencialidade de informação e sistema, ou desconhecido	
	Efetuar avaliação de impacto nos recursos (sem impacto, impacto baixo, impacto moderado ou impacto elevado)	
	Fornecer estimativa de impacto • Impacto nas operações ou exercícios do Exército; • Danos à reputação; • Ameaças de ação legal por afetar terceiros; • Perda de ligação ao ISP devido a violação da política de utilização responsável (contrato com o ISP); • Disrupção/comprometimento com uma ou mais redes de terceiros*; (* No caso do nosso sistema ser comprometido e utilizado para atacar outros sítios)	
	Fornecer uma suspeita do motivo principal, como por exemplo: • Ganho financeiro ilícito • Utilização de recursos do sistema para uso pessoal • Vantagem de instituições/governos estrangeiros (espionagem ou sabotagem) • Protesto político, causas populares («*hacktivism*») • Dano malicioso • Demonstração de capacidades ofensivas • Utilização de recursos do sistema para efetuar novos ataques • Indiscriminado (o ataque foi resultado de uma escolha aleatória, através da conetividade à internet) • Desconhecido	
	Submeter ao escalão superior, dependendo do risco de acesso não autorizado/afetação de disponibilidade/existência de *malware*, nos prazos de: 4h – Impacto alto, 6h/8h - impacto médio, 8h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8.	
	Continuar a relatar nas 24 horas seguintes até ao encerramento	
	Fornecer o relatório de atividade	
	Fornecer o relatório final dentro de 7 dias, após encerramento e incluir análise de impacto na missão	
	Documentar atividades de treino associados a este incidente.	

TENTATIVAS DE ACESSO FALHADAS (EVENTO)		
Propósito: Relato e procedimentos para resposta a incidentes do tipo «tentativa de acesso falhada», por adversários, com intuito de ganhar acesso às redes/estações de trabalho do Exército		
Ponto de Contato:		
Estado	Ação	GDH de início
Identificar	Potencial reconhecimento de evento de segurança significativo que consista numa ameaça às redes do Exército através de atividade suspeita, identificada através de relatórios da rede, relatórios de sensores de rede, etc. Indicadores limite para investigação: • Atividade suspeita nos relatórios da rede (firewall, IDS ou notificações de utilizadores) • Engenharia Social, **Portal** ou pessoal técnico, «*Helpdesk*»	
Isolar	• Determinar local/identificar o sistema • Determinar equipamento de rede alvo do sistema anfitrião;	
Informar	Fornecer a notificação inicial ao escalão superior, dependendo do risco de acesso não autorizado/afetação de disponibilidade/existência de *malware*, nos prazos de: 30min/1h – Impacto alto, 1h/2h - impacto médio, 2h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8, para conhecimento de situação (quem, o quê, quando, onde e como), endereços de origem e destino, portos TCP/UDP comuns, outros protocolos, tipo de dispositivo anfitrião, dimensão da rede afetada, classificação de segurança, sistema operativo e vulnerabilidade.	
Investigar	• Rever relatórios de auditoria; • Validar eventos/incidentes; • Avaliar a extensão da possível intrusão; • Rever o impacto operacional; • Verificar com a rede nacional de CSIRT e o NATO NCIRC se existe mais informação sobre a atividade em curso; • Requerer assistência forense, se necessário.	
	Desenvolver Alerta • Referir a forma de detetar o código malicioso e solicitar cooperação de forma a conter mais rapidamente a ameaça; • Identificar e rever qualquer tentativa de ligações; • Determinar a natureza provável das sondas/pesquisas: atividade «*worm*», ferramenta automática de scan; • Fornecer nome de atividade anómala se conhecido.	

Mitigar	• Pesquisar a rede por potenciais intrusões; • Implementar bloqueios por ACL ou bloqueio de endereços IP (por «*blackhole*»), efetuar alterações ao DNS de forma a parar o tráfego («*blackhole*»); • Remover «*software*» não autorizado; • Documentar lições aprendidas.	
	Determinar o comprometimento de segurança do sistema: integridade de informação, disponibilidade de sistema, confidencialidade de informação e sistema, ou desconhecido	
	Efetuar avaliação de impacto nos recursos (sem impacto, impacto baixo, impacto moderado ou impacto elevado)	
	Fornecer estimativa de impacto • Impacto nas operações ou exercícios do Exército; • Danos à reputação; • Ameaças de ação legal por afetar terceiros; • Perda de ligação ao ISP devido a violação da política de utilização responsável (contrato com o ISP); • Disrupção/comprometimento com uma ou mais redes de terceiros*; (* No caso do nosso sistema ser comprometido e utilizado para atacar outros sítios)	
	Fornecer uma suspeita do motivo principal, como por exemplo: • Ganho financeiro ilícito • Utilização de recursos do sistema para uso pessoal • Vantagem de instituições/governos estrangeiros (espionagem ou sabotagem) • Protesto político, causas populares («*hacktivism*») • Dano malicioso • Demonstração de capacidades ofensivas • Utilização de recursos do sistema para efetuar novos ataques • Indiscriminado (o ataque foi resultado de uma escolha aleatória, através da conetividade à internet) • Desconhecido	
	Submeter ao escalão superior, dependendo do risco de acesso não autorizado/afetação de disponibilidade/existência de *malware*, nos prazos de: 4h – Impacto alto, 6h/8h - impacto médio, 8h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8.	
	Continuar a relatar nas 24 horas seguintes até ao encerramento	
	Fornecer o relatório de atividade	
	Fornecer o relatório final dentro de 7 dias, após encerramento e incluir análise de impacto na missão	
	Documentar atividades de treino associados a este incidente.	

ATIVIDADE DE REDE NÃO AUTORIZADA		
Propósito: Relato e procedimentos para resposta a incidentes do tipo «atividade de rede não autorizada»		
Ponto de Contato:		
Estado	Ação	GDH de início
Identificar	Potencial reconhecimento de evento de segurança significativo que constitua uma ameaça às redes do Exército através de atividade suspeita, identificado através de relatórios da rede, relatórios de sensores de rede, etc. Indicadores limite para investigação: • *Peer-to-peer*, *software* de partilha de ficheiros, *software* não aprovado, etc.; • Determinar local/identificar sistema	
Isolar	• Determinar equipamento de rede alvo do sistema anfitrião; • Bloquear conta;	
Informar	Fornecer a notificação inicial ao escalão superior, dependendo do risco de acesso não autorizado/afetação de disponibilidade/existência de *malware*, nos prazos de: 30min/1h – Impacto alto, 1h/2h - impacto médio, 2h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8, para conhecimento de situação (quem, o quê, quando, onde e como), endereços de origem e destino, portos TCP/UDP comuns, outros protocolos, tipo de dispositivo anfitrião, dimensão da rede afetada, classificação de segurança, sistema operativo e vulnerabilidade.	
Investigar	• Rever relatórios de auditoria; • Validar eventos/incidentes; • Avaliar a extensão da possível intrusão; • Rever o impacto operacional; • Verificar com a rede nacional de CSIRT e o NATO NCIRC se existe mais informação sobre a atividade em curso; • Requerer assistência de atividade forense, se necessário;	
	Desenvolver Alerta • Referir a forma de detetar o código malicioso e solicitar cooperação de forma a conter mais rapidamente a ameaça; • Identificar e rever qualquer tentativa de ligações; • Determinar a natureza provável das sondas/pesquisas: atividade «*worm*», ferramenta automática de scan; • Fornecer nome de atividade anómala se conhecido.	

Mitigar	• Remover «*software*» não autorizado; • Documentar lições aprendidas.	
	Determinar o grau de comprometimento da segurança do sistema: integridade de informação, disponibilidade de sistema, confidencialidade de informação e sistema, ou desconhecido	
	Efetuar avaliação de impacto nos recursos (sem impacto, impacto baixo, impacto moderado ou impacto elevado)	
	Fornecer estimativa de impacto • Impacto nas operações ou exercícios do Exército; • Danos à reputação; • Ameaças de ação legal por afetar terceiros; • Perda de ligação ao ISP devido a violação da política de utilização responsável (contrato com o ISP); • Disrupção/comprometimento com uma ou mais redes de terceiros*; (* No caso do nosso sistema ser comprometido e utilizado para atacar outros sítios)	
	Fornecer uma suspeita do motivo principal, como por exemplo: • Ganho financeiro ilícito • Utilização de recursos do sistema para uso pessoal • Vantagem de instituições/governos estrangeiros (espionagem ou sabotagem) • Protesto político, causas populares («*hacktivism*») • Dano malicioso • Demonstração de capacidades ofensivas • Utilização de recursos do sistema para efetuar novos ataques • Indiscriminado (o ataque foi resultado de uma escolha aleatória, através da conetividade à internet) • Desconhecido	
	Submeter ao escalão superior, dependendo do risco de acesso não autorizado/afetação de disponibilidade/existência de *malware*, nos prazos de: 4h – Impacto alto, 6h/8h - impacto médio, 8h - impacto baixo, conforme cronograma para relato de incidentes da pág. 8.	
	Continuar a relatar nas 24 horas seguintes até ao encerramento	
	Fornecer o relatório de atividade	
	Fornecer o relatório final dentro de 7 dias, após encerramento e incluir análise de impacto na missão	
	Documentar atividades de treino associados a este incidente.	

4. ALGUMAS PUBLICAÇÕES DE REFERÊNCIA

a. NATO International Cyber Defense Playbook, v1.0, de 18 de Abril de 2011

b. DoD 8500 series Information Assurance

c. CJCI 6510.01F, Information Assurance (IA) and Computer Network Defense (CND)

d. DODI 0-8530.02 Support to Computer Network Defense (CND)

e. Information Assurance Advisory, IAA-003-2010, de 3 Fevereiro 2010

APÊNDICES:

1: FORMULÁRIO DE RELATO DE INCIDENTE

2: FORMULÁRIO DE RELATO TÉCNICO DE INCIDENTE

DISTRIBUIÇÃO: Com a NEP NAT 02.03.04 "ESTRUTURA DE SEGURANÇA DA INFORMAÇÃO DO EXÉRCITO, NORMAS TÉCNICAS E PROCEDIMENTOS DO ADMINISTRADOR DA REDE LOCAL DAS U/E/O"

Apêndice 1 (FORMULÁRIO DE RELATO DE INCIDENTE) ao Anexo A (PROCEDIMENTOS PARA GESTÃO DE INCIDENTES) à NAT 02.03.04

RELATO DE INCIDENTE
Para:
U/E/O: 1. Nome da Unidade: 2. Número de telefone: **3.** Endereço de correio eletrónico:
***Responsável pelo relatório*:** 4. Nome: 5. Telefone: 6. Correio eletrónico: 7. Função:
Computadores afetados: 8. Número de computadores: 9. Nome(s) e IP(s) do(s) computador (es): 10. Função do computador: 11. Fuso horário: 12. Hardware: 13. Sistema operativo: 14. Software afetado: 15. Ficheiros afetados: 16. Antivírus do(s) Computador(es) *17.* Protocolo / porta:
Incidente: 18. Número de referência: 19. Tipo de incidente: 20. Início do incidente: 21. Trata-se de um incidente contínuo: 22. Hora e método de deteção: 23. Vulnerabilidades conhecidas: 24. Ficheiros suspeitos: 25. Contra -medidas: 26. Descrição detalhada:

Apêndice 2 (FORMULÁRIO DE RELATO TÉCNICO DE INCIDENTE) ao Anexo A (PROCEDIMENTOS PARA GESTÃO DE INCIDENTES) à NAT 02.03.04

CONTACTOS

Parte 1: Identificação do Administrador CSI da UEO

Contacto Primário:

Nome Completo:	Coloque aqui o seu nome completo
Título/Posto:	Coloque aqui o seu posto ou título
Função:	Coloque aqui a sua função

Contacto Alternativo:

Nome Completo:	Coloque aqui o nome completo do contacto alternativo
Título/Posto:	Coloque aqui o posto ou título do contacto alternativo
Função:	Coloque aqui a função do contacto alternativo

UEO:	Coloque aqui o nome da sua UEO
Endereço:	Coloque aqui o endereço da sua UEO

E-Mail:	Contacto Primário	Contacto Alternativo
Exército:	Coloque aqui o seu e-mail	Coloque aqui o endereço e-mail
Alternativo:	Coloque aqui o seu e-mail	Coloque aqui o endereço e-mail

Telefone:	Contacto Primário	Contacto Alternativo
Militar:	Coloque aqui o seu número de telefone	Coloque aqui o seu número de telefone
Tlm:	Coloque aqui o seu número	Coloque aqui o seu número
Fax (Seguro):	Coloque aqui o seu número	Coloque aqui o seu número
Fax(Não seguro):	Coloque aqui o seu número	Coloque aqui o seu número

Parte 2: Informação Comum de Eventos

A sua referência para este relatório: Coloque aqui a sua referência

GDH em que foi detetado o evento:

Dia: Coloque data	Mês: Out	Ano: 2013	Hora: Hora GMT

Endereços IP e especificações de serviços para este evento (se for o caso):

Endereços Fonte: Coloque aqui o endereço fonte

Endereços de destino: Coloque aqui o endereço de destino

Portos TCP Comuns: Escolha Porto TCP Outros portos TCP: Coloque aqui o número dos portos

Portos UDP Comuns: Escolha Porto UDP Outros portos UDP: Coloque aqui o número dos portos

Outros Protocolos: Coloque aqui outros protocolos

Informações sobre a plataforma/dispositivo associada ao evento

Tipo de dispositivo: Escolha tipo de dispositivo afetado Tamanho da rede afetada: Escolha o número de máquinas afetadas

Classificação de segurança do dispositivo: Escolha a classificação de segurança do dispositivo

Sistema Operativo: (Selecione todas que se apliquem)

- ☐ Desconhecido / Não específico
- ☐ Windows — Escolha o sistema operativo
- ☐ Unix — Escolha o sistema operativo
- ☐ Linux — Escolha o sistema operativo
- ☐ Aparelho de rede — Escolha dispositivo
- ☐ Outro — Especifique

Versão: Coloque aqui a versão

Informações sobre a vulnerabilidade explorada:

Natureza geral da vulnerabilidade: Especifique

Identificador(es) de Vulnerabilidade (e.g. CVE number(s)) Escreva o número de vulnerabilidade se conhecido

Detalhes da vulnerabilidade e/ou como foi explorada:

Escreva os detalhes

Tipo de Incidente a ser Reportado		
Descrição		**Secções adicionais a Completar**
Perda ou roubo de computador ou dispositivo de armazenamento classificado	☐	3, 11, 12
Fraude informático, Embustes, Esquemas (Phishing)	☐	4, 11, 12
Acesso ou modificação não autorizados a ficheiros e/ou sistema	☐	5, 11, 12
Desfiguração de Web Sites (incluindo Sítios Sociais)	☐	6, 11, 12
Negação de Serviços (DoS ou DDoS) incluindo meios eletrónicos disruptivos	☐	7, 11, 12
Interceção de informação transmitida eletronicamente	☐	8, 11, 12
Código Malicioso (Virus, Worm, Trojan,etc)	☐	9, 11, 12
Reconhecimento da Rede (Sondas Maliciosas ou Scans)	☐	10, 11, 12
Desconhecido	☐	11, 12

Parte 3: Perda ou roubo de computador ou dispositivo de armazenamento classificado

Detalhes da Perda:

O item foi perdido ou roubado: Perdido ☐ Roubado ☐

Onde foi roubado ou perdido o item em questão:

☐ Local Público — Indique uma breve descrição do local

☐ Local Privado/Casa — Indique uma breve descrição do local

☐ Um local controlado pelo Exército — Escolha a classificação de segurança da área

Quando é que o item foi roubado ou perdido: Indique data e hora

Qual era a classificação do item: Escolha a classificação de segurança do item

Descreva brevemente o item:

☐ Hardware ☐ Media/Dispositivo de Armazenamento

Escreva uma pequena descrição do evento e do item

Reportou o evento a alguma autoridade civil?

☐ Não ☐ Sim – Coloque os detalhes em baixo

Coloque as pessoas civis e/ou autoridades que foram notificadas

Parte 4: Fraude informática, Embustes, Esquemas (Phishing)

Método/tipo de fraude, embuste ou esquema:

- ☐ Número de cartões de crédito roubados ou ilicitamente gerados para pagamentos online
- ☐ Acesso fraudulento a informação classificada
- ☐ Transferências de fundos não autorizados
- ☐ Promoção online de investimentos fraudulentos
- ☐ Falsos websites ou e-mail falsos para facilitarem acesso fraudulento a contas financeiras/fundos/informação classificada/contas de acesso a sites internos ou contas de utilizador (também conhecido como phising)
- ☐ Outro

Por favor, forneça mais detalhes. Se possível, incluir cópias dos e-mails associados, print-screen, etc (se necessário anexar ao e-mail)

Coloque detalhes adicionais aqui

Part 5: Acesso ou modificação não autorizados a ficheiros e/ou sistema

Descreva que o tipo de informação que foi comprometida:
(Selecione todas as que se apliquem)

- ☐ Ficheiros classificados lidos/copiados Classificação: Escolha classificação de segurança
- ☐ Ficheiros não classificados lidos/copiados
- ☐ Modificação/exclusão de ficheiros do sistema operativo
- ☐ Ferramentas de ataque instaladas, ex. Rootkit, ferramentas DDos
- ☐ Material ilegal instalado, licenças ou propriedade intelectual pirateada
- ☐ Software instalado para facilitar maior controlo de sistemas, ex. IRC bot
- ☐ Ficheiros desconhecidos instalados
- ☐ Desconhecido

Se for o caso, liste os nomes das ferramentas / ficheiros instalados e / ou os ficheiros modificados pelo atacante:

Coloque detalhes aqui

Se aplicável, descrever a relevância do comprometimento:

- ☐ Atacante acedeu a algum ficheiro/informação em toda a rede
- ☐ Atacante acedeu a ficheiros do sistema
- ☐ Atacante acedeu a informação sensível – ex. ficheiros com passwords
- ☐ Atacante acedeu a ficheiros de utilizadores
- ☐ Atacante acedeu a ficheiros classificados NATO
- ☐ Atacante acedeu a outros materiais classificados
- ☐ Desconhecido ou não aplicável

Parte 6: Desfiguração de Web Sites (incluindo Sites Sociais)

IP do servidor web desfigurado: Coloque aqui o IP do servidor afetado

URL completo do web site desfigurado: Coloque o URL do site desfigurado

Qual é a plataforma do servidor Web: Escolha a aplicação Web Escreva aqui a versão

Qual o propósito do website: Escolha o propósito

Descreva o propósito:

Descreva o propósito do web site aqui

Detalhes do conteúdo da desfiguração:

Descreva os detalhes da desfiguração aqui

Se possível, anexar ao e-mail "print screens" ou fotografias/imagens do site desfigurado.

Parte 7: Negação de Serviços (DoS ou DDoS) incluindo meios eletrónicos disruptivos

Tipos de negação de serviços:

- ☐ DoS não distribuídos através de consumo de largura de banda
- ☐ DoS distribuídos através de consumo de largura de banda
- ☐ Ações para travar ou degradar o desempenho do servidor ou plataforma do servidor
- ☐ Ações automáticas de negação de acesso a serviço(s), por motivos de segurança (ex. bloqueio de contas de utilizadores, flexibilidade de resposta do IPS, etc.)

Serviço/sistema que foi atacado: Escolha a serviço/sistema

Se outro, por favor insira os detalhes: Coloque aqui os detalhes do serviço

Duração do ataque: Escolha a duração do ataque O ataque ainda está a decorrer? ☐ Sim ☐ Não

Largura de banda normalmente disponível: Escolha um se aplicável

Parte 8: Interceção de informação transmitida eletronicamente

Método de interceção: Escolha um item.

Se outro método, indique:

Coloque detalhes aqui

Parte 9: Código Malicioso (Vírus Worm, Trojan,etc)

Nome do vírus, worm ou trojan (se conhecido): Coloque detalhes aqui

Indique a fonte provável da infeção: Escolha um item

Se outro, indique a fonte de infeção: Coloque aqui a fonte

Se não conseguiu identificar o vírus, worms ou Trojan forneça quaisquer características que tenha identificado. No caso de infeções múltiplas relatar quaisquer características comuns que notou:

Coloque aqui as características

Parte 10: Reconhecimento da Rede (Sondas Maliciosas ou Scans)

Por favor, selecione a opção que descreve o tipo de atividade que está a ser relatada:

Se aplicável, escolha um item

Qual é a natureza provável do scan/sonda:

- ☐ Worm
- ☐ Ferramenta automática de scanning
- ☐ Desconhecido

Por favor, forneça o nome do worm ou da ferramenta, se for conhecida:

Coloque o nome do worm ou da ferramenta

Parte 11: Impacto e Motivo

Impacto:

Nível de acesso comprometido: Escolha o nível mais elevado de acesso ganho

Por favor, indique quais os aspetos do sistema de segurança que foram comprometidas como resultado do incidente:

☐ Integridade de Informação ☐ Disponibilidade de sistema

☐ Confidencialidade de sistema ou de ficheiros ☐ Desconhecido

Número de sistemas ou contas afetadas : Escolha da lista:

Impacto direto de recursos:

☐ Impacto menor – poucos recursos/tempo, necessários para normalizar a situação

☐ Impacto moderado - recursos/tempo moderados, necessários para normalizar a situação

☐ Impacto sério - recursos/tempo significativos, necessários para normalizar a situação

☐ Impacto grave – é necessário apoio para normalizar a situação

Impacto no Exército:

☐ Impacto em operações

☐ Impacto em exercícios

☐ Danos de reputação

☐ Ameaça de ação legal por afetar terceiros

☐ Perda de ligação do ISP devido a violação de uso aceitável

☐ Rompimento/Comprometimento com uma rede terceira*

☐ Rompimento/ Comprometimento com várias redes terceiras*

*O seu sistema comprometido foi usado para atacar outro site(s)

Suspeita de Motivo Primário

Escolha a suspeita de motivo(s) primário:	
Ganho financeiro ilícito	☐
Utilizar recursos do Exército para uso pessoal	☐
Vantagem de governos estrangeiros (espionagem estrangeira ou sabotagem)	☐
Protesto político (hacktivismo)	☐
Dano malicioso	☐
Para demonstrar capacidades de ataque	☐
Para utilizar recursos do sistema para novos ataques	☐
Indiscriminado (o ataque foi resultado de uma escolha aleatória através de conectividade com a internet)	☐
Desconhecido	☐

Parte 12: Informação Adicional

Por favor, forneça qualquer informação adicional não incluída nas perguntas anteriores que possam ser úteis na compreensão do evento relatado.

Coloque informação adicional aqui

Exemplos de logs:

Coloque aqui até 50 linhas ou anexe ao e-mail

Fuso horário dos logs: GMT

Você reportou este evento a qualquer outra entidade? ☐ Não ☐ Sim – Coloque os detalhes em baixo

Liste essas pessoas e/ou entidades notificadas