ASANTE ASS

GESTÃO EMPRESARIAL INTEGRADA, RASTREÁVEL E PRONTA PARA ESCALAR

Asante ASS
Defesa Cibernética

Guia de Formação — Central de Defesa, Sinais, Bloqueios e Simulações

Asante ASS
asante.mainsolenergy.com | Agosto de 2026

Índice

Introdução à Central de Defesa Cibernética

A **Central de Defesa Cibernética** (Fase 133 — v1.9.64+) é o sistema de deteção e resposta automática a ameaças aplicacionais integrado no Asante ASS. Opera em segundo plano, em cada pedido ao sistema, observando sinais de comportamento anómalo e reagindo automaticamente quando deteta padrões de ataque — sem interromper utilizadores legítimos.

> **Nota — O que é e o que não é:** a Defesa Cibernética do Asante ASS protege a **camada aplicacional** — as páginas e APIs do sistema. Não substitui uma firewall de rede, um antivírus ou um sistema de deteção de intrusão de infraestrutura. É uma camada adicional de segurança dentro da própria aplicação.

> **Nota — Acesso restrito:** a Central de Defesa Cibernética é exclusiva para os perfis **TI** (departamento de Tecnologia da Informação), **Admin** e **CEO**. Outros perfis não têm acesso a esta área.

> **Nota — Migração obrigatória:** antes de usar a Central de Defesa, o Super Admin deve aplicar a migração `migration_defesa_cibernetica_fase133.sql` em `Super Admin → Migrações`. Sem ela, o módulo mostra um aviso e não opera.

---

1. Como a Defesa Cibernética Funciona

1.1 Observação Passiva Contínua

A cada pedido feito ao sistema (página carregada, formulário submetido, chamada à API), a função `cyberDefenseObserveRequest()` corre automaticamente em segundo plano. Ela analisa:

- A **origem** do pedido (identificada por um hash anónimo do IP — o IP real é minimizado para proteger privacidade, mas o padrão de origem é rastreável);
- A **rota** acedida (que página ou endpoint foi chamado);
- O **método HTTP** (GET, POST, PUT, DELETE);
- O **conteúdo** do pedido — sinais de padrões de ataque conhecidos.

Este processo é completamente transparente para o utilizador legítimo — não existe tempo de espera adicional perceptível.

1.2 Tipos de Ameaça Detetados Automaticamente

Tipo de Ameaça	O que deteta	Resposta automática
`credenciais`	Múltiplas tentativas de login falhadas da mesma origem (□5 em 15 min)	Bloqueio temporário da origem + notificação a Admin/CEO
`injecao`	Padrões de SQL Injection ou command injection em campos de entrada	Pedido isolado + origem limitada

Tipo de Ameaça	O que deteta	Resposta automática
`travessia_caminho`	Tentativas de aceder a ficheiros fora do diretório permitido (`../`, `%2e%2e`)	Pedido isolado + origem limitada
`abuso_api`	Volume anormal de pedidos da mesma origem num curto período	Origem limitada temporariamente
`upload_suspeito`	Tentativa de upload com extensão ou conteúdo proibido	Upload recusado + origem observada
`sondagem_privilegios`	Tentativas de aceder a áreas restritas além do perfil atual	Acesso negado + evento registado para análise

> **Nota — Hash de origem:** o sistema não regista o IP completo em texto claro. Usa um hash HMAC-SHA256 do IP com a chave da aplicação — o que permite detetar reincidências da mesma origem sem guardar dados pessoais diretamente. O IP real só é visível em eventos recentes para fins de análise imediata.

1.3 Bloqueio Temporário Automático

Quando uma origem acumula sinais suficientes (ex.: 5 falhas de autenticação em 15 minutos), o sistema:

1. Cria um **bloqueio ativo** (`seguranca_bloqueios_origem` com estado `ativo`);
2. Define o **tempo de expiração** (padrão: 60 minutos, máximo: 1440 min/24h);
3. Atualiza o evento que desencadeou o bloqueio para estado `bloqueada`;
4. **Notifica** automaticamente todos os utilizadores Admin e CEO da empresa com uma notificação de tipo `danger`;
5. A origem bloqueada recebe uma resposta de acesso negado em pedidos subsequentes.

1.4 Expiração e Libertação de Bloqueios

- **Expiração automática:** ao atingir a data/hora de expiração, o bloqueio passa para estado `expirado` — a origem volta a ter acesso normal;
- **Libertação manual:** o Admin/TI/CEO pode libertar um bloqueio antes do tempo, com registo de quem libertou e quando;
- **Renovação:** se a origem reincide durante um bloqueio ativo, o sistema renova o prazo de expiração.

---

2. Painel da Central de Defesa Cibernética

Caminho: `TI / Admin / CEO` → `Defesa Cibernética` (`tecnico/defesa-cibernetica.php`)

O painel apresenta a situação de segurança em tempo real com 4 métricas principais das **últimas 24 horas**:

Métrica	O que conta
Sinais nas últimas 24h	Total de eventos de ameaça registados (reais + simulações)
Alta prioridade	Eventos com gravidade `alta` ou `critica` — requerem análise imediata
Respostas aplicadas	Eventos com estado `mitigada` ou `bloqueada` — situação tratada
Bloqueios ativos	Origens atualmente bloqueadas (expiram automaticamente conforme a política)

2.1 Últimos 60 Eventos

Tabela dos 60 eventos mais recentes da empresa com: - **Data/hora** de deteção; - **Tipo de ameaça** (credenciais, injecao, abuso_api, etc.); - **Gravidade** (baixa, media, alta, critica); - **Estado** (detetada, em_analise, mitigada, bloqueada, falso_positivo); - **Rota** onde o sinal foi detetado; - **Método HTTP** (GET, POST, etc.); - **Indicador** se é uma simulação ou evento real; - **Mecanismo de resposta** aplicado.

> **Nota — "Nenhum sinal registado":** a mensagem "A monitorização está pronta" significa que o sistema está operacional mas não detetou nenhum sinal nas últimas 24h — o que é positivo.

2.2 Bloqueios Ativos

Lista das origens atualmente bloqueadas com: - **Hash da origem** (identificador anónimo); - **IP** (quando disponível para análise imediata); - **Categoria** do bloqueio (ex.: `credenciais`, `injecao`); - **Motivo** detalhado (ex.: "Origem bloqueada após 7 falhas de autenticação em 15 minutos"); - **Expira em** — data e hora de expiração automática; - Botão **"Libertar"** — para remoção manual antes do prazo.

---

3. Estados dos Eventos de Ameaça

Estado	Significado	Ação do utilizador
`detetada`	Sinal registado, ainda não classificado	Analisar e reclassificar
`em_analise`	Em avaliação pelo TI	Aguardar conclusão da análise
`mitigada`	Ameaça tratada sem bloqueio	Registar ação tomada
`bloqueada`	Origem bloqueada automaticamente	Monitorizar ou libertar
`falso_positivo`	Evento detetado incorretamente	Marcar como falso positivo para refinar deteção

3.1 Gravidade dos Eventos

Gravidade	Critério	O que fazer
`baixa`	Sinal único sem reincidência	Registar e monitorizar
`media`	Padrão repetido ou sondagem	Analisar origem e rota afetada
`alta`	Ataque ativo detetado	Ação imediata — verificar origem e rota
`critica`	Ataque com bloqueio ativo ou comprometimento potencial	Escalonamento para Admin/CEO + análise forense

---

4. Simulações de Cenários

Caminho: botão **"Simulação"** no painel da Central de Defesa.

As simulações permitem à equipa de TI **testar o funcionamento da Defesa Cibernética** sem executar ataques reais e sem afetar utilizadores reais.

4.1 Como as Simulações Funcionam

- **IPs reservados:** as simulações usam exclusivamente os intervalos de IP reservados para documentação (`192.0.2.x`, `198.51.100.x`, `203.0.113.x`) — nunca IPs reais;
- **Campo `simulado = 1`:** os eventos gerados por simulação ficam marcados como simulados na base de dados — são claramente distinguíveis dos eventos reais no painel;
- **Sem impacto real:** nenhum utilizador real é bloqueado, nenhuma rota é limitada — a simulação é completamente isolada;
- **Auditável:** cada simulação fica registada no log de auditoria de segurança com o utilizador que a iniciou.

4.2 Para que Serve Simular

Objetivo	O que valida
Verificar deteção	O sistema regista o tipo de evento correto?
Verificar bloqueio	O bloqueio é criado com a categoria certa?
Verificar notificação	Admin e CEO recebem a notificação de alerta?
Verificar o painel	Os contadores e a tabela atualizam corretamente?
Testar após migração	Após aplicar `fase133.sql`, confirmar que o módulo está operacional

---

5. Incidentes Cibernéticos (registo manual)

Caminho: `TI` → `Incidentes Cibernéticos` (`tecnico/incidentes-ciberneticos.php`)

Além da deteção automática, a equipa de TI pode registar **incidentes cibernéticos manualmente** — para situações reportadas por utilizadores, detetadas por ferramentas externas ou identificadas

durante auditoria.

Caminho de criação: `tecnico/adicionar-incidente-cibernetico.php`

5.1 Campos do Incidente Manual

Campo	O que preencher
Título	Descrição breve do incidente
Quantidade de eventos	Número de eventos relacionados com este incidente
Gravidade	Baixa / Média / Alta / Crítica
Status	Estado atual do incidente
Origem	De onde veio o ataque/incidente
Canal	Que canal ou sistema foi afetado
Descrição	Detalhe completo do que aconteceu
Impacto	Que sistemas, dados ou utilizadores foram afetados
Ações tomadas	O que foi feito para mitigar ou resolver

5.2 Estados do Incidente Manual

Estado	Significado
`registado`	Incidente registado, aguarda análise
`em_analise`	Equipa de TI a investigar
`em_resolucao`	Solução a ser implementada
`resolvido`	Incidente fechado com solução documentada
`escalado`	Subiu para Admin/CEO/entidades externas
`arquivado`	Encerrado e arquivado para histórico

5.3 Ver e Editar um Incidente

Caminho: `tecnico/ver-incidente-cibernetico.php` / `tecnico/editar-incidente-cibernetico.php`

O detalhe do incidente mostra toda a informação registada, o histórico de alterações e permite adicionar atualizações de estado e ações. Cada atualização fica com data, hora e utilizador responsável.

---

6. Integração com Outros Módulos

6.1 Notificações Automáticas

Quando a Defesa Cibernética aciona um bloqueio automático, **Admin e CEO** da empresa recebem imediatamente uma notificação de tipo `danger` no sistema com: - Título: "Defesa cibernética acionada"; - Mensagem: descrição do tipo de ameaça e da ação tomada; - Link direto para a Central de Defesa para análise.

6.2 Log de Auditoria de Segurança

Todas as ações na Central de Defesa — deteção de sinais, bloqueios, libertações e simulações — são registadas no **log de auditoria de segurança** da empresa (`securityAuditEvent`), com: - Tipo de evento e utilizador responsável; - Data e hora exata; - Dados relevantes (tipo de cenário, ID do bloquio, etc.);

Este log é consultável em `TI` → `Logs` e `Admin` → `Logs`.

6.3 Relação com o Módulo TI

A Central de Defesa Cibernética complementa o módulo TI — especificamente a secção de **Incidentes Cibernéticos** (`tecnico/incidentes-ciberneticos.php`). A diferença é:

Central de Defesa Cibernética	Incidentes Cibernéticos (TI)
Deteção **automática** em tempo real	Registo **manual** de incidentes
Sinais da camada aplicacional	Qualquer tipo de incidente de segurança
Bloqueios automáticos e reversíveis	Gestão de resposta e resolução
Eventos gerados pelo sistema	Eventos reportados pela equipa ou utilizadores

---

7. Boas Práticas de Operação

7.1 Rotina Diária Recomendada

- Abrir a Central de Defesa e verificar os **4 indicadores de 24h**;
- Rever eventos com gravidade `alta` ou `critica` que ainda estejam em `detetada` ou `em_analise`;
- Verificar se existem **bloqueios ativos** que mereçam revisão (ex.: origem que pode ser um utilizador legítimo com problema de conectividade);
- Confirmar que não existem **falsos positivos** recorrentes — se sim, ajustar políticas.

7.2 Libertar um Bloqueio — Quando e Como

Quando libertar: - A origem identificada é um utilizador legítimo com problema técnico confirmado (ex.: tentativas de login por esquecimento de senha); - O bloqueio foi gerado por uma simulação que ficou ativa indevidamente; - A análise confirma que os sinais eram de um utilizador interno em teste.

Como libertar: painel da Central de Defesa → secção “Bloqueios ativos” → botão “Libertar” → o sistema pede confirmação e regista o utilizador que libertou.

> **Atenção:** libertar um bloqueio de uma origem ativa em ataque permite que o ataque continue. Confirmar sempre a legitimidade da origem antes de libertar.

7.3 Interpretar Falsos Positivos

Marcar um evento como `falso_positivo` não altera o comportamento futuro do sistema automaticamente — mas documenta para auditoria. Se uma rota ou tipo de ação estiver a gerar

muitos falsos positivos, o TI deve reportar ao Super Admin para afinação das políticas de deteção.

---

8. Perguntas Frequentes

"A deteção afeta a performance do sistema?" Não de forma perceptível. A função de observação corre de forma assíncrona e está otimizada para zero impacto em pedidos normais.

"O sistema bloqueia utilizadores legítimos?" Raramente. O limiar de bloqueio (ex.: 5 falhas em 15 minutos) é suficientemente alto para não afetar utilizadores que erram a senha uma ou duas vezes. Em caso de bloqueio indevido, o Admin liberta a origem manualmente.

"Os dados de IP dos utilizadores ficam armazenados?" O sistema guarda um hash anónimo (HMAC-SHA256) do IP, não o IP em texto claro. O IP real aparece temporariamente em eventos recentes para análise imediata, minimizando a retenção de dados pessoais.

"A Defesa Cibernética opera em todas as páginas?" Sim — a função `cyberDefenseObserveRequest()` é chamada automaticamente em cada pedido, em todas as páginas do sistema, sem configuração adicional.

Glossário Defesa Cibernética

Termo	Significado
Ameaça aplicacional	Ataque dirigido à camada de software (páginas, formulários, APIs) — não à rede ou infraestrutura
Hash de origem	Identificador anónimo da origem de um pedido (HMAC-SHA256 do IP)
Bloqueio temporário	Restrição automática de acesso de uma origem por um período definido
Injeção	Ataque que insere código malicioso (ex.: SQL) em campos de entrada
Travessia de caminho	Ataque que tenta aceder a ficheiros fora do diretório autorizado
Abuso de API	Volume anormal de pedidos que sobrecarrega ou sonda o sistema
Sondagem de privilégios	Tentativa de aceder a funcionalidades além do perfil atual
Falso positivo	Evento detetado como ameaça que na realidade é comportamento legítimo
Simulação	Teste controlado do sistema usando IPs reservados, sem impacto real
HMAC-SHA256	Algoritmo de hash com chave — garante que o hash não pode ser revertido sem a chave
Mitigação	Ação tomada para neutralizar ou conter uma ameaça

Termo	Significado
Escalamento	Elevação de um incidente para um nível de autoridade superior
Log de auditoria	Registo cronológico de todas as ações relevantes com data, hora e responsável