Região Autónoma da Madeira
Governo Regional

Secretaria Regional
de Educação, Ciência e Tecnologia
Direção Regional de Educação

# Plano de Ciber-Segurança

## Escola Básica dos 2.º e 3.º Ciclos da Torre

Ciber.EDU

Julho 2024

PRR Plano de Recuperação e Resiliência

REGIÃO AUTÓNOMA DA MADEIRA

REPÚBLICA PORTUGUESA

Financiado pela União Europeia
NextGenerationEU

# Conteúdos

# Introdução

Com a globalização da informação, estimulada pela evolução exponencial das tecnologias ao serviço dos internautas, passamos a ter acesso a uma panóplia de serviços e informação nunca dantes conseguido. Com esta disponibilidade de informação, surgem também, a um ritmo alucinante, os crimes virtuais e os ataques cibernéticos. Independentemente da quantidade e qualidade dos mecanismos de prevenção instalados, os incidentes de ciber-segurança têm-se mostrado mais frequentes e complexos. Neste cenário, interessa preparar as organizações, no sentido de elevarem o nível da sua ciber-segurança, tendo em conta as suas diversas vertentes.

Perante esta situação, delineou-se o presente documento, cujo teor constitui um plano de ciber-segurança, passível de responder prontamente a ameaças cibernéticas.

# Responsável da Equipa de Ciber-Segurança

O responsável de ciber-segurança é o ponto de contato da organização. Do ponto de vista técnico/operacional, deverá ser capaz de responder às solicitações da equipa *CiberEDU*, sendo esperada disponibilidade para contactos de emergência, fora do horário de expediente. Este elemento deverá conhecer bem a organização a nível de gestão. Do ponto de vista técnico, deverá ser capaz de reencaminhar internamente, as solicitações do *CiberEDU*.

Adicionalmente, deverá ser indicado um segundo (e/ou terceiro) elemento para a equipa. Este (s) deverá (ão) conhecer bem a organização do ponto de vista técnico.

**Responsável da Equipa de Ciber-Segurança:**

**Nome**: Hélder José Vieira Miranda

**eMail**: helder.miranda@edu.madeira.gov.pt

**Contato Telefónico**: 918 554 187



PRR Plano de Recuperação e Resiliência · Região Autónoma da Madeira · República Portuguesa · Financiado pela União Europeia NextGenerationEU

V 1.0

**Cargo**: Vice-Presidente do Conselho Executivo

**Segundo elemento da Equipa de Ciber-Segurança**

**Nome**: Luís Alexandre Conduto

**eMail**: luis.conduto@edu.madeira.gov.pt

**Contato Telefónico**: 919 438 034

**Cargo**: Técnico de Informática

**Terceiro elemento da Equipa de Ciber-Segurança**

**Nome**: Aureliano de Sousa Barreto

**eMail**: aureliano.6717@edu.madeira.gov.pt

**Contato Telefónico**: 962 696 625

**Cargo**: Coordenador TIC

## Identificação de funções ou atividades críticas

A identificação das funções ou atividades críticas requer a conjugação de uma visão alargada da instituição com uma visão alargada dos processos que a sustentam. Esta ação consiste em definir os serviços/aplicações mais importantes para a organização, ordená-los por criticidade, identificar potenciais ameaças e consequentes impactos, identificar dependências internas e externas entre sistemas, e, finalmente, construir o quadro global de ameaças da organização.

| Serviço /aplicação | Rede | Nível de prioridade | Dependências | Impacto | Alternativa |
|---|---|---|---|---|---|
| Servidor Windows com partilha de Ficheiros – aplicação TAB. | Administrativa | Alta | - Secretaria e SASE utiliza para consulta/venda/c arregamentos de cartão. | Alto | Registo em papel e pagamento em dinheiro. |

# Cadeia de Responsabilidade

Esta ação começa com a nomeação de um órgão/equipa/pessoa responsável pela deteção de incidentes de ciber-segurança dentro da organização. Esta responsabilidade, que pode ou não ser atribuída ao RESPONSÁVEL DE SEGURANÇA (Elemento de Contato Operacional com o Ciber.EDU), deve ser conhecida por toda a organização e ser o ponto de contacto para todos os assuntos relacionados com a deteção de incidentes de ciber-segurança. A cadeia de responsabilidade e a constituição da equipa de Ciber-Segurança está publicada na página inicial do site da organização, mais precisamente no módulo "CIBERSEGURANÇA": https://escolas.madeira-edu.pt/eb23torre/INÍCIO/tabid/8040/Default.aspx#LiveTabsContent5934713 .

A equipa de ciber-segurança da Escola Básica dos 2.º e 3.º Ciclos da Torre foi nomeada a 18/04/2024 e apresentada no Conselho da Comunidade Educativa a 22 de julho do presente ano. Foi ainda publicitado na página eletrónica da escola essa informação, mais precisamente no endereço https://escolas.madeira-edu.pt/eb23torre/INÍCIO/tabid/8040/Default.aspx#LiveTabsContent5934713 .

Cabe ao orgão/equipa/pessoa responsável pela deteção de incidentes de ciber-segurança, definir e diligenciar pela aprovação dos processos de deteção de incidentes. Esta informação encontra-se presente no "Mapa de Emergência Ciber-Segurança".

# Definição de política de segurança de informação da organização

A criação de uma política de segurança de informação da organização é

um elemento estruturante da ciber-segurança. Enquanto elemento estratégico, é importante que tenha a aprovação e aceitação da gestão de topo e o envolvimento e **compromisso de todos os colaboradores**. A sua efetivação verificar-se-á mediante a respetiva tradução em processos e procedimentos específicos a serem posteriormente implementados por cada departamento.

É importante que aqui se definam as prioridades da organização, bem como os respetivos perfis de risco. As decisões devem ser tomadas, tanto quanto possível, partindo da análise da situação face a esse perfil, constituindo a política de segurança o principal garante das boas práticas e fator de redução de risco e exposição a ameaças nas atividades do dia-a-dia.

Com vista a facilitar o envolvimento e compromisso de todos os intervenientes sugere-se, a utilização dos materiais disponíveis em https://www.cncs.gov.pt/pt/recursos-para- sensibilizacao/ e a frequência por parte dos colaboradores dos cursos disponíveis em https://www.cncs.gov.pt/pt/cursos-e-learning/.

## Procedimentos de notificação de incidentes

Consiste em criar e fazer aprovar pela direção da organização, um procedimento de notificação de incidente de ciber-segurança com impacto nas funções ou atividades identificadas como críticas.

Neste processo deve estar definido quem, dentro da organização, deve ser informado além da equipa de ciber-segurança da escola (por exemplo Diretor, Coordenador TIC, Técnico de informática, etc.)

| Nível Incidente -Tipo | Elemento(s) | O que informar |
|---|---|---|
| Baixo. | Direção;<br>Técnico de informática. | Descrição do incidente;<br>Procedimentos a adotar. |

| | | |
|---|---|---|
| Médio – rede escolar. | Direção;<br>Técnico de informática;<br>Delegados dos grupos disciplinares. | Descrição do incidente;<br>Procedimentos a adotar. |
| Alto – rede escolar. | Direção;<br>Técnico de informática;<br>Delegados grupos disciplinares;<br>Docentes;<br>Alunos. | Descrição do incidente;<br>Procedimentos a adotar. |
| Médio – rede administrativa. | Direção;<br>Técnico de informática;<br>Responsáveis sectores. | Descrição do incidente;<br>Procedimentos a adotar. |
| Alto – rede administrativa. | Direção;<br>Técnico de informática;<br>Responsáveis sectores;<br>Assistentes operacionais. | Descrição do incidente;<br>Procedimentos a adotar. |

# Inventariação de ativos / produção de um mapa de rede

Interessa particularmente registar a lista dos principais ativos informáticos de suporte às funções críticas, anteriormente identificadas. Para cada um destes ativos deverá, no mínimo, ser armazenada a informação do endereçamento IP, versões de sistema operativo, versões de aplicações que comunicam com o exterior e dependências funcionais com outros serviços vitais.

No diagrama de rede deverão constar, no mínimo, todos os segmentos de rede da organização, endereçamento IP usado em cada um deles, endereços IP de interligação, equipamentos de interligação entre os vários segmentos e a

indicação das políticas de acesso entres estes.

Em baixo, é apresentado o diagrama geral de rede, assim como, o diagrama de rede do bastidor principal (Bastidor 1).

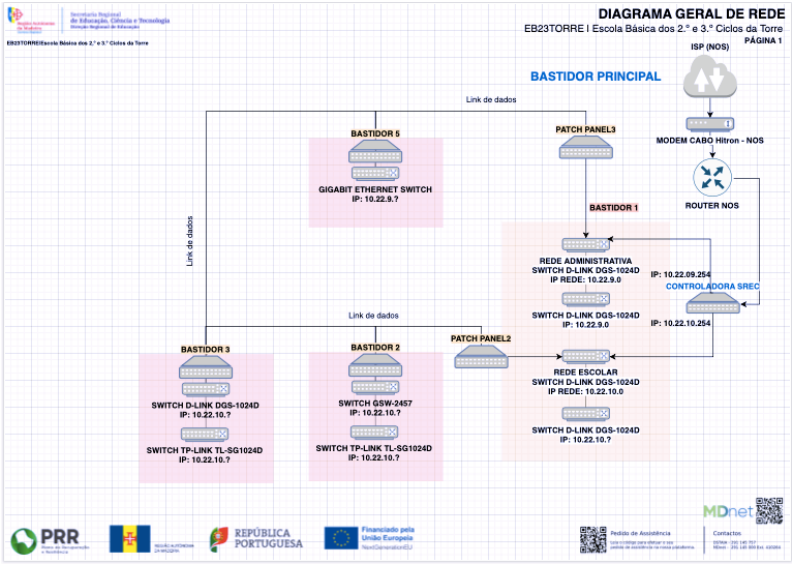


*Figura 1 - Digrama de rede do bastidor principal (Bastidor 1)*

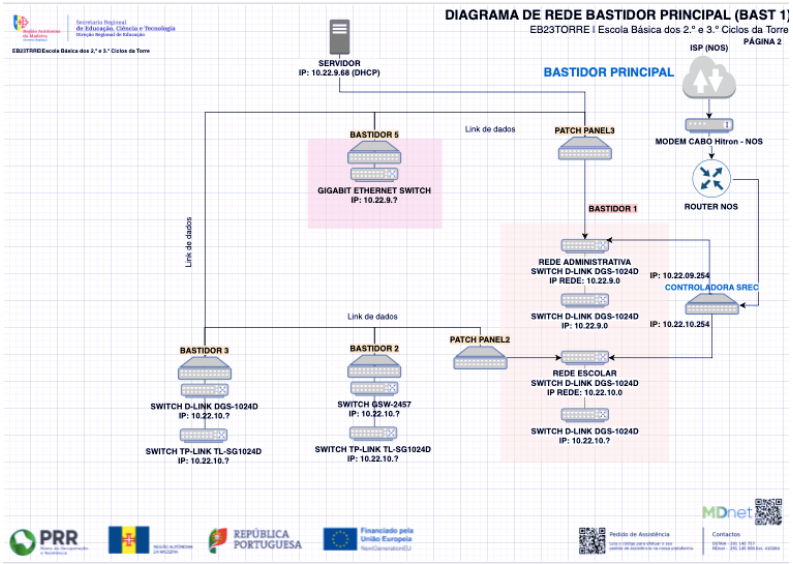


*Figura 2 - Diagrama geral de rede*

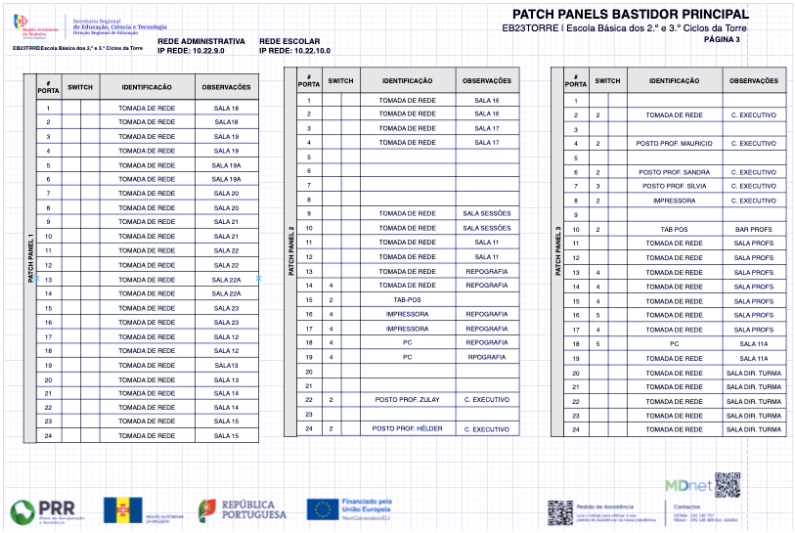


*Figura 3 – Exemplo do diagrama dos Patch Panels do Bastidor 1.*

Para facilitar este processo, utilizou-se a ferramenta online ***draw.io***, para ilustrar o levantamento da rede da nossa escola – o ficheiro com todos os pormenores (*Rede_EB23Torre.drawio*), já foi carregado para a plataforma da Ciber.Edu.

# Recolha centralizada de registos (logs)

Os logs produzidos pelo sistema operativo e pelas aplicações de suporte à atividade são o principal instrumento de análise e investigação de um incidente de ciber-segurança. Neste contexto é essencial que a organização possua um repositório central para estes logs com um período mínimo de armazenamento de 1 (um) ano.

Os registos (Logs), a serem guardados, trimestralmente, deverão incidir sobre os servidores, sobre os computadores dos serviços administrativos, serviços de ação social e conselho executivo. Os registos deverão ser guardados em disco rígido externo, no cofre da escola.



PRR Plano de Recuperação e Resiliência
REGIÃO AUTÓNOMA DA MADEIRA
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU
V 1.0

## Criação de política de uso aceitável

A política de uso aceitável (PUA) dos recursos TIC internos é mais um elemento de regulação interna importante. Neste documento devem estar vertidas as linhas de orientação para a boa utilização destes recursos, para que esta seja feita de forma segura por todos os colaboradores com acesso aos mesmos.

É importante ter em conta que grande parte das ameaças a que se expõem as organizações no dia-a-dia estão diretamente relacionados com má utilização dos recursos tecnológicos por parte dos colaboradores. Daí que o estabelecimento adequado de uma PUA para os TIC da organização deva abranger temas como:

- Papéis e Responsabilidades;
- Manutenção dos postos de trabalho e ambiente de trabalho;
- Correta utilização do e-mail para uso profissional;
- Comportamento adequado na navegação na Internet;
- Utilização de dispositivos móveis para uso profissional;
- Instalação e utilização de software aplicacional;
- Respeito pelos princípios de ética e pela privacidade e proteção de dados pessoais;
- Administração do parque informático e do acesso aos recursos em rede.

## Manutenção de infraestruturas de cópias de segurança e reposição (Backup/Restore)

É importante contar com equipamento que permita a salvaguarda de

informação considerada prioritária para a organização, possibilitando a respetiva reposição em caso de necessidade.

Dependendo da complexidade da infraestrutura da organização, bem como do volume e criticidade dos dados, o hardware deve ser dimensionado para dar resposta adequada. Os períodos e abrangência dos backups a efetuar devem levar em linha de conta o que for determinado em sede análise de risco (ver A 1.6), assim como, os procedimentos adequados à reposição.

Poderá ser adequado, em casos específicos que o justifiquem devido à importância da informação, prever o armazenamento de backups off-site (fora das instalações da organização), com recurso a cofres ou infraestruturas resistentes a catástrofes.

No sentido de verificar periodicamente a integridade dos suportes de backup e da qualidade dos mecanismos de reposição, estes devem ser sujeitos a testes periódicos, como parte de um plano no quadro da política de segurança interna.

## Proteção e gestão de equipamentos

Instalação de antivírus com visibilidade sobre todo o parque informático, ou em alternativa, no mínimo para os serviços críticos e para os dispositivos dos administradores de sistemas, uma vez que as máquinas dos administradores de sistemas devem ser tratadas com nível máximo de criticidade por terem acesso a todos os recursos que processam e armazenam a informação da organização.

## Definição de planos de continuidade

O Plano de Continuidade é um elemento complementar importante à política de segurança interna. Usualmente, este plano é, ele próprio, constituído por outros planos, designadamente os de Contingência, Gestão de Crises, Recuperação de Desastres e Continuidade operacional.

Devem fazer parte deste plano os elementos essenciais que permitam à organização continuar em operação perante um qualquer desastre ou incidente que cause (ou tenha potencial para causar) uma disrupção significativa ou até total na atividade.

O plano deve fazer referência a:

- Critérios de ativação;
- Contactos de pessoas ou organizações-chave;
- Papéis e responsabilidades na ativação;
- Procedimentos a adotar na ativação;
- Cadeia de pessoas ou departamentos a envolver nos fluxos de informação;
- Instalações alternativas;
- Serviços alternativos;

- Recursos a mobilizar (internos e externos);
- Eventuais procedimentos para reposição de sistemas ou serviços essenciais.

## Definição de procedimentos de reação a incidentes

Esta ação pressupõe a identificação dos tipos de ataque mais comuns e a criação de um procedimento para a respetiva mitigação ou resolução. O conjunto de procedimentos que resulta desta ação deve ser aprovado pelo departamento jurídico e pela administração da organização.

Também deve ser criado um procedimento interno para notificação de incidentes que indique como um colaborador deve proceder perante um incidente ou um evento suspeito.