



## Plano de Ação para Cibersegurança

Selo "Clean & Safe" 2022

O **Plano de Ação para Cibersegurança**, no âmbito do Selo Clean & Safe, é um plano preventivo e reativo, que visa apoiar a *Entidade Aderente* (adiante designada por Estabelecimento) no conhecimento do risco e na tomada das medidas de prevenção, preparação, resposta e recuperação adequadas para reduzir a vulnerabilidade do Estabelecimento, tendo em vista a minimização das suas consequências negativas, na sequência de ataques cibernéticos que envolvam qualquer atividade ou prática ilícita na rede ou sistema tecnológico do Estabelecimento, desde a disseminação de vírus, roubo de dados pessoais, falsidade ideológica, acesso a informações confidenciais e tantos outros.

Através do Plano de Ação, é estimulada a adequada e necessária articulação do estabelecimento com as entidades competentes em matéria de cibersegurança.

O Plano de Ação deve ser revisto sempre que necessário, quer devido a atualizações resultantes de orientações das entidades competentes, quer devido a alterações para melhoramento dos procedimentos adotados internamente.

### COORDENAÇÃO DO PLANO

Designar o/a coordenador/a do Plano de Ação para Cibersegurança que é responsável pela definição dos procedimentos aplicáveis ao Estabelecimento, pela implementação deste Plano e pela articulação com entidades relevantes.

#### Identificação do/da coordenador/a do Plano / responsáveis por equipa (quando pertinente)

Diretora Geral – Andreia de Brito

#### Lista de contactos relevantes a serem divulgados

Centro Nacional de Cibersegurança - 210 497 399 | [cncs@cncs.gov.pt](mailto:cncs@cncs.gov.pt)  
Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica - 211 967 000

### RISCOS E VULNERABILIDADES

A identificação das vulnerabilidades associadas ao ecossistema digital da empresa varia muito e pode abranger riscos como:

- Interrupção de atividade e downtime em todos ou alguns departamentos da organização com custos associados;
- Perda de dados pessoais de clientes;
- Custos com fornecedores externos e recursos internos para recuperar os sistemas e dados;
- Destruição da imagem de reputação da organização, perante os clientes, fornecedores e público em geral;

## Plano de Ação para Cibersegurança

Selo "Clean & Safe" 2022

- Roubo de propriedade intelectual e informação confidencial.

As medidas a definir e implementar no âmbito dos capítulos seguintes deverão incidir sobre cibersegurança.

### MITIGAÇÃO DO RISCO

O Plano identifica as ações, registos de informação e meios de comunicação e divulgação que visem melhorar a preparação face aos possíveis ataques cibernéticos. Todos/as os/as colaboradores/as recebem por correio eletrónico o Plano.

A formação de todos/as os/as colaboradores/as, incluindo os/as ocasionais, é imprescindível para uma correta atuação na mitigação do risco e na fase de emergência. Na formação são abordadas todas as matérias do Plano, incluindo sensibilização e treino para comportamentos e atitudes (mais) seguras e responsáveis no uso da tecnologia e do ciberespaço e formação especializada nos vários domínios da cibersegurança.

A garantia da segurança das infraestruturas tecnológicas, das redes e sistemas de informação depende da capacidade de os utilizadores finais adotarem medidas que previnam os riscos e vulnerabilidades a que se poderão encontrar expostos. Após a identificação dos riscos e vulnerabilidades é fundamental a adequação da alocação de recursos de forma proporcional aos riscos identificados e a monitorização dos riscos identificados, sabendo que a segurança do ciberespaço resulta de um exercício complexo, e contínuo, mas verificável.

A formação aqui descrita não se sobrepõe ou isenta da responsabilidade de frequência de outras formações exigidas no âmbito da Segurança e Saúde no Trabalho.

#### Identificação dos responsáveis e funções no âmbito da mitigação de riscos

**Coordenador/a do Plano:**

Andreia de Brito ( único membro da equipa)– Função: gestão dos procedimentos, revisão e melhoria do plano;

**Responsável pelos canais digitais de comunicação:**

Andreia de Brito – Função: coordenação comunicação e marketing empresa

**Responsável pela gestão da rede e sistema informático:**

– Andreia de Brito – Função: Diretora Geral

## Plano de Ação para Cibersegurança

Selo "Clean & Safe" 2022



### Programa de formação/informação dos/as colaboradores/as sobre Cibersegurança e procedimentos aplicáveis no Estabelecimento

Especificação das ações : O único membro da equipa realizou a formação "Cidadão Ciber Seguro" Desenvolvido pela Comissão Nacional de Ciber Segurança

### Medidas preventivas do Estabelecimento para um ataque cibernético

- **Verificar os URL dos sites** - verificar sempre se o link coincide com o nome da entidade que pretende visitar e confirmar se endereço inicia por https:// e é seguido de um cadeado; outra forma de confirmar a segurança das páginas a visitar, é verificar se existem erros ortográficos, de pontuação ou traduções desajustadas;
- **Ter cuidados extra com operações bancárias** – evitar efetuar operações bancárias através de redes wi-fi públicas; não entrar no site do banco através de nenhum link recebido por e-mail ou mensagem, por exemplo; entrar no site do banco através da sua app oficial, descarregada de app store oficial (nunca a partir de um link); mesmo que lhe solicitado durante a operação, nunca instalar uma aplicação; perante um pedido de dados que pareça suspeito contactar de imediato a entidade bancária, através dos contactos oficiais;
- **Manter os antivírus, antispyware, firewall e proteção antispam, sempre atualizados;**
- **Desconfiar de e-mails ou SMS com sorteio de prémios** - Nestes casos, além de não clicar no link enviado, os especialistas aconselham a eliminar estas mensagens;
- **Utilizar palavras passwords complexas** - A definição de uma palavra password forte é fundamental para manter a segurança online; definir passwords distintas para cada acesso e o mais complexas possível, por exemplo, utilizando letras maiúsculas e minúsculas, números e caracteres especiais é uma boa estratégia;
- **Não partilhar dados pessoais dos colaboradores ou clientes nas redes sociais;**
- **Não utilizar o email da empresa para plataformas de vendas online** - Um dos ataques cibernéticos que mais tem crescido nos últimos tempos é a burla através do MBWay.

### Informação de apoio que o Estabelecimento deve reunir

- **Ferramentas específicas para a investigação do ataque cibernético, da criminalidade tecnológica e da decifragem de dados;**
- **Regime Jurídico de Segurança do Ciberespaço**, que transpõe a diretiva europeia relativa à segurança das redes e da informação, exercendo as competências de regulação e de supervisão para os diferentes setores de atividade económica;
- **Regime legal de proteção de dados pessoais;**



## Plano de Ação para Cibersegurança

Selo "Clean & Safe" 2022

- **Código dos Direitos de Autor e Direitos Conexos**, incluindo a interferência e o desbloqueio de formas de proteção tecnológica de bens e de serviços.

### Articulação entre o Estabelecimento e Entidades relevantes no âmbito da mitigação do risco

Centro Nacional de Cibersegurança - 210 497 399 | [cncs@cncs.gov.pt](mailto:cncs@cncs.gov.pt)  
Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica - 211 967 000

## FASE DE EMERGÊNCIA

O Plano identifica as ações de resposta, aquando de uma ocorrência de ataque cibernético.

### Identificação dos meios próprios (técnicos e humanos) a mobilizar em situação de ocorrência de ataque cibernético

- Andreia de Brito

### Ações imediatas após ataque cibernético

- Tentar recolher o máximo de provas que sejam possíveis;
- Caso se trate de uma transação bancária, é contactado imediatamente o banco e feito um pedido de reclamação sobre a transação efetuada; - E Apresentar sempre queixa junto da Polícia Judiciária;
- Acionar a estratégia de comunicação para colaboradores e clientes que minimize o impacto associado;

## FASE DE REABILITAÇÃO

O Plano identifica as atividades de recuperação destinadas à reposição da normalidade no funcionamento do Estabelecimento e das condições dos/as colaboradores/as e clientes.

### Ações de reposição da normalidade no funcionamento do Estabelecimento, junto de colaboradores e clientes

- Procedimentos a implementar no âmbito da continuidade de negócio;
- Considerar a existência de uma equipa de avaliação preliminar de danos;

## Plano de Ação para Cibersegurança

Selo "Clean & Safe" 2022

