01 | Objetivo

O objetivo deste documento consiste em documentar todas as atividades e funções definidas para a operacionalização das medidas de cibersegurança.

Âmbito da certificação: Prestação de serviços de Ensino e Formação. Aluguer de espaços. Cibersegurança.

Locais onde a empresa desenvolve atividades: ESCO – Rua da Liberdade, 4 – Hilarião. 2560-374 Torres Vedras.

02 | Procedimento

Requisitos – Medidas de cibersegurança

O.ID – Identificação de funções ou atividades críticas

- Funções do Pessoal - **Pr.26 Funções do Pessoal**
- Manutenção e gestão do servidor e redes – Realizada pelo Técnico de Informática e Professora de TIC.
- Parque informático - Configuração, manutenção e gestão do parque informático e seus componentes (software e hardware) realizada pelo Técnico de Informática e Professora de TIC.
- eSchooling - Configuração, manutenção e gestão da plataforma de gestão escolar realizada pela Direção Pedagógica (Paulo Moreira) com o apoio da Codevision.
- Primavera - Configuração, manutenção e gestão do Primavera realizada pelo Técnico Superior de Gestão com o apoio da Sisopção.
- Site (Wordpress) - Configuração, manutenção e gestão do site realizada pelo Técnico Superior de Gestão.
- Moodle - Configuração, manutenção e gestão da plataforma de gestão escolar realizada pela Direção Pedagógica (Paulo Moreira).
- Moodle Formação de Adultos - Configuração, manutenção e gestão do moodle realizada pela Coordenadora da Formação de Adultos.
- Gestão de utilizadores – Criação, modificação e eliminação de utilizadores e contas de email realizada pelo Técnico de Infomática.
- Videovigilância – Configuração e gestão das câmaras e registos.
- Apoio informático – Técnico de Informática realiza apoio informático a toda a comunidade escolar.

O.IAC – Inventariação dos ativos e documentação da arquitetura de comunicação de dados

- **Portaria** – 1 Posto de trabalho
- **Secretaria / Reprografia** – 7 Postos de trabalho; 3 Impressora XEROX
- **SPO** – 4 Postos de trabalho
- **Sala de Professores** – 6 Portáteis; 14 Postos de trabalho

- **Centro de Recursos** – 1 Posto de trabalho; 6 Computadores de alunos; 1 Impressora XEROX
- **Direção Pedagógica** – 2 Portáteis; 3 Postos de trabalho;
- **Direção** – 1 Posto de Trabalho; 1 Portátil de reuniões
- **Sala dos Servidores** – 2 UPS; 2 NAS; 1 Firewall Watchguard; 1 Switch CISCO; 2 Servidores + 1 Storage Fujitsu; 1 Servidor HP; 1 Servidor Fujitsu, gerido por VMware com 10 Servidores Virtuais.
- **Gabinete de trabalho** – 1 Portátil; 3 Postos de trabalho; 2 Postos de trabalho (Professores Externos);
- **Sala 1 – Sala de Informática** – 1 Posto de trabalho (Computador do professor); 13 Computadores de alunos;
- **Sala 2 – Sala de Informática** – 1 Posto de trabalho (Computador do professor); 12 Computadores de alunos;
- **Sala 3/4 – Lab Mauser** – 3 Portáteis; 1 Bastidor de Rede; 1 NAS; 1 UPS; 4 Impressora 3D;
- **Sala 5 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 6 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 7 – Sala de Informática** – 1 Posto de trabalho (Computador do professor); 11 Computadores de alunos;
- **Sala 8 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 9 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 10 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 11 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 12 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 13 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 14 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 15 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 16/17 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 18 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 19 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Sala 20/21 – Sala de aula** – 1 Posto de trabalho (Computador do professor);
- **Restaurante** – 1 Posto de trabalho (Computador do professor);
- **Softwares/Plataformas** – Primavera; eSchooling; eCommunity; Site (Wordpress); Moodle; Moodle Formação de adultos; idOntime; Microsoft 365; GARE; Veam; Zoom; Shout; Sender.net
- **Redes Sociais** – Google My Business, Facebook, Twitter, Linkedin e Instagram
- Documentação do SGQ
- Pr.28 - PUA – Política de Utilização Aceitável
- Pr.29 - TLP – Traffic Light Protocol
- Pr. 30 - Procedimento – Cibersegurança
- Pr.31 Boas práticas de utilização de equipamentos e softwares
- Pr.32 Código de Ética e Conduta
- Pr.33 Plano de Gestão de Riscos de Segurança da Informação

- Pr.12 - Firewall – Rede Alunos

Diagrama de rede Wi-fi

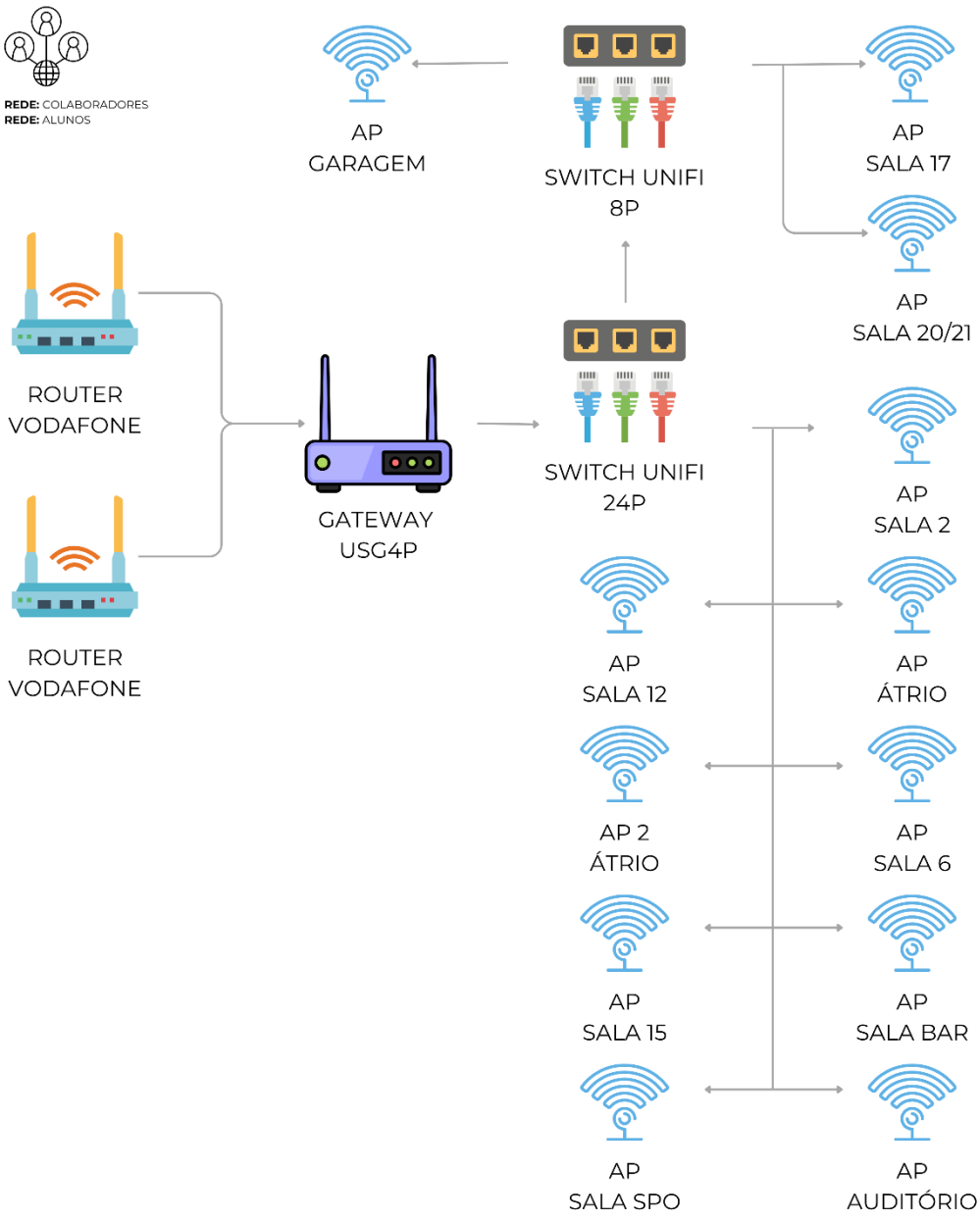
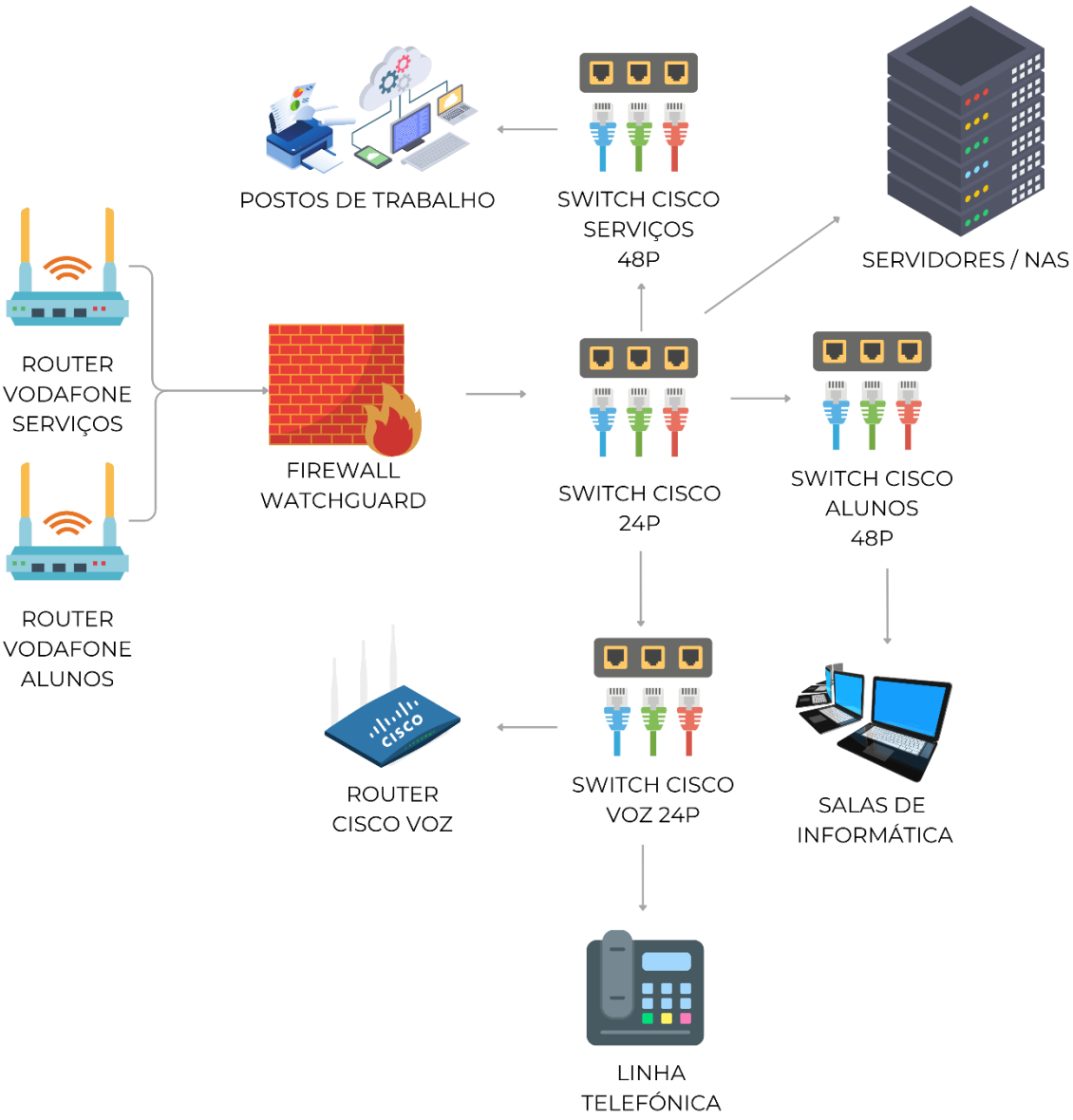


Diagrama de rede por cabo



O.PUA – Política de utilização aceitável

A PUA está definida no **Pr. 28 PUA – Política de Utilização Aceitável** e está divulgada no site da ESCO.

O.RSI – Identificação de responsável pela função de Segurança da Informação

Responsáveis pela função de Segurança da Informação:

- Luís Couto – Técnico Superior de Gestão / Gestor da Qualidade e Cibersegurança (luiscouto@sefo.pt)

- Sérgio Rodrigues - Técnico de Informática / Responsável pela Segurança da Informação (sergiorodrigues@sefo.pt)
- Cláudia Barros Pinto – Coordenadora do Curso de Informática (claudiapinto@sefo.pt)
- Susana Esteves – Professora de TIC / Apoio ao Parque Informático (susanaesteves@sefo.pt)

T.CS – Cópias de Segurança

- Wordpress – Plugin Duplicator: Criadas cópias de segurança todos os anos pelo Gestor do site.
- eSchooling: Backups realizados todas as semanas pela CodeVision.
- Primavera – Clone da Empresa realizado todos os anos pela ESCO. Cópias de segurança pontuais realizadas pela consultora Sisopção.
- Freewares: Download e armazenamento de freewares em https://ninite.com/ e em Pens no gabinete de informática.
- Videovigilância: O Sistema de vídeo vigilância faz gravação em circuito fechado, está em plena gravação no período das 7h às 00h de segunda a sábado. Das 00h às 6h59m está em gravação por deteção de movimento entre segunda a sábado. Aos domingos, as 24h estão por deteção de movimento. As gravações estão acessíveis até 30 dias atrás. Nº de Câmaras – 15 unidades | Nº de Gravadores (DVR's) – 2 unidades.
- OneDrive: Cópias de segurança realizadas automaticamente em caso de eliminação de um ficheiro ou pasta mal-intencionada (Salvaguardado na reciclagem por 90 dias). Histórico do Onedrive permite reverter para versões anteriores de documentos.
- Cópias de Segurança: Realizadas automaticamente todos os dias através do Veeam cópias incrementais e completas, que permitem repor de forma rápida uma máquina ou um servidor na íntegra até 5 dias. As cópias são feitas para 3 NAS alojadas em localizações diferentes.

T.AS – Atualizações de Segurança

- Wordpress: Realizadas atualizações conforme necessidade, pelo Técnico Superior de Gestão.
- Softwares: Realizadas atualizações conforme necessidade, pelo Técnico de informática ou consultoras.
- Hardwares: Realizadas atualizações conforme necessidade, pelo Técnico de informática, após pedido à Direção.

T.PPT – Proteção de postos de trabalho

Todos os postos de trabalho têm antivírus atualizado e palavra-passe por utilizador. Está instalado também um antivírus em todos os dispositivos móveis da ESCO. Têm também acesso bloqueio de ecrã por password.

T.PPI – Proteção perimetral e da infraestrutura

A política de segurança foi definida no Ponto 2 - Segurança do **Pr.28 Política de Utilização Aceitável (PUA).**

T.CWC – Conformidade Webcheck

Os sites da ESCO têm o Certificado Digital SSL atualizado todos os anos, funcionam em modo de segurança (HTTP/S, HSTS e contêm cabeçalhos de segurança) e contém o SPF - Sender Policy Framework configurado no Office 365 e Cloudflare e DKIM configurado.

T.AM – Atualização multifator

A autenticação multifator encontra-se ativa na plataforma de e-mail da escola – Microsoft Authenticator.

T.PF – Plano de formação

Está contemplada formação interna em cibersegurança no plano interno de formação da escola.

Foram também definidos os Procedimentos relativos à cibersegurança, PUA e questionário de cibersegurança.

Anualmente, no início do ano letivo, durante a reunião de responsáveis de processo, é realizada a análise SWOT, Matriz GUT (Análise de risco), é realizado um briefing sobre cibersegurança e feita a apresentação dos procedimentos a adotar.

Aquando da entrada de novos colaboradores é entregue o guia de acolhimento e são apresentados os procedimentos nesta área na formação inicial – **mod.063 – Acolhimento de novos colaboradores**.

T.FIC – Fontes de informação e canais de comunicação

- Verificação dos alertas emitidos pelo CNCS – Realizada subscrição da Newsletter
- RGPD – Consulta permanente
- A ESCO é Academia CISCO – Consulta anual de nova regulamentação da Academia CISCO
- Antivírus – Consulta semanal das notificações e alertas emitidos pelas entidades parceiras da ESCO.
- Wordpress – Consulta mensal de atualizações e alertas
- Primavera e eSchooling – Consultoras externas enviam regularmente notas e alertas relacionadas com atualizações e proteção do software.
- Microsoft Office 365 – Gestor do Office recebe regularmente novidades e atualizações.

- TLP – Consulta anual da www.first.org/tlp
- Certificadora eiC - Realizada subscrição da Newsletter
- ISO 9001:2015
- DNP TS 4577-1:2021
- Incidentes de Cibersegurança - https://docs.microsoft.com/pt-pt/security/compass/incident-response-process
- Reação a Incidentes CNCS

O.PP – Política de palavra-passe

Todas as contas da ESCO são pessoais e intransmissíveis, sendo a garantia de identidade assegurada pela posse de um segredo (palavra-passe, palavra-chave ou password) detida por cada Utilizador.

Os utilizadores não podem comunicar a sua password a terceiros.

As passwords são gravadas centralmente de forma cifrada, sendo do conhecimento exclusivo de cada utilizador.

Os utilizadores não devem usar a password de utilizador da ESCO para se registarem noutros sistemas (ex: homebanking, Skype, Gmail, etc.).

Sempre que for necessária a autenticação e autorização de acesso, será usado um nome de utilizador e palavra-chave que cumpram os requisitos a seguir descritos, definidos em função do vínculo e perfil de uso que o utilizador mantém com a ESCO.

Para garantir a segurança dos utilizadores, as palavra-passe devem considerar:

- Histórico de reutilização – não pode usar a última palavra-passe
- Não conter o nome de utilizador
- O comprimento mínimo de 8 carateres;
- Pelo menos uma letra minúscula;
- Pelo menos uma letra maiúscula;
- Pelo menos um número;
- Pelo menos um caracteres não alfabético (~@^&*()_+{ }|:"<>?/.,';][=-`)
- A password não pode conter outros caracteres (Ex: €, !, #, $, %, á, è, Í, etc)

As palavras-passe têm um tempo de expiração de 365 dias e devem ser renovadas após esse período. Haverá um mecanismo de notificação automático, que iniciará 1 semana antes da expiração da password. Será disponibilizado mecanismo do tipo self-service para a emissão de novas passwords, que obrigarão à prova inequívoca de identidade do Utilizador.

Os elementos dos TIC nunca solicitarão ao utilizador a indicação da password, sendo que, por esse motivo poderão apenas despoletar o processo de emissão de uma nova. Para tal, será exigida prova de identidade, podendo ainda assim ser negada a emissão em caso de suspeita de fraude ou de insuficiência ou inconsistência de elementos, indicando métodos suplementares a seguir.

Recuperação da palavra-passe: Existe um mecanismo de recuperação/reposição da palavra-passe através de e-mail ou número de telefone.

O.PAP – Política de acessos e permissões

Todos os acessos e permissões partem de uma premissa de *need-to-know* e *least privilegie*.

Existe uma diferenciação primordial entre alunos e colaboradores. Os alunos estão num servidor próprio e não têm permissão para fazer alterações ou instalações nos computadores da escola. Os colaboradores têm níveis de acesso distinto, conforme os departamentos onde estão inseridos.

Grupos de permissões: Direção, Professores, Qualidade, Secretaria, Contabilidade, Comunicação, Técnico, Coordenadores, Direção Pedagógica e Formação de Adultos.

Existe uma Política de autorização por departamento – Cada departamento dentro da organização possui permissões únicas de tratamento de dados de forma exclusiva. Por exemplo, o departamento de Qualidade tem permissão total na pasta da Qualidade, enquanto os restantes colaboradores conseguem apenas visualizar e fazer download de modelos/templates, sem acesso às subpastas de conteúdo mais sensível.

No Site, Kwiksurveys, Primavera, eSchooling, Moodle e Moodle da Formação de Adultos existem também níveis de acesso e permissões definidos pelos respetivos gestores de plataforma.

O.GMO – Gestão da mudança organizacional

A Gestão de utilizadores funciona conforme definido no processo **C06 – Gerir Utilizadores**.

O.PRI – Plano de reação a incidentes de Cibersegurança

Independentemente da quantidade e qualidade dos mecanismos de prevenção instalados, os incidentes de cibersegurança têm-se mostrado mais frequentes e complexos.

O Plano de Resposta a Incidentes de Segurança Cibernética (ou IRP, do inglês Incident Response Plan) é um documento elaborado com o objetivo de identificar e traçar ações que devem ser colocadas em prática caso algum evento de cibersegurança que impacte negativamente a empresa ocorra.

É tendo esse plano como guia, que as equipas da área de Segurança da Informação conseguem lidar de forma eficiente

com imprevistos e, assim, garantir que a operação da empresa não seja gravemente prejudicada ou interrompida quando acontecem ameaças e ciberataques.

O quê?	Quem?	Quando Contactar?	Tarefas / Ações (Responsabilidades)	Ferramentas, tecnologias e recursos
Ransomware e outros ataques informáticos	Sérgio Rodrigues (Téc. Informática) Susana Esteves (Professora TIC)	24/7	• Diagnóstico • Consultar autoridades e avisos • Consultar logs • Bloquear acessos e passwords • Reposição de backups • Reconfiguração do sistema • Testes	• Antivírus • Backups • Watchguard • Servidores
Vírus	Sérgio Rodrigues (Téc. Informática)	Horário de trabalho	• Diagnóstico • Remoção do vírus	• Antivírus • Backups • Watchguard
Picos de energia	Sérgio Rodrigues (Téc. Informática) Cláudia Pinto (Professora TIC)	Horário de trabalho	• Configuração da UPS • Iniciar equipamentos que não têm arranque automático	• Servidores • UPS • Router • Switchs secundários
Roubo ou assalto	Sérgio Rodrigues (Téc. Informática) Cláudia Pinto (Professora TIC) Susana Esteves (Professora TIC)	Horário de trabalho	• Levantamento do material roubado • Encomenda • Montagem / Instalação / Configuração	• Realizar pesquisa de mercado • Fazer requisição do equipamento
Destruição de equipamento	Sérgio Rodrigues (Téc. Informática) Cláudia Pinto (Professora TIC) Susana Esteves (Professora TIC)	Horário de trabalho	• Levantamento do material destruído • Encomenda do material de substituição • Montagem / Instalação / Configuração	• Realizar pesquisa de mercado • Fazer requisição do equipamento
Eliminação de informação por lapso	Sérgio Rodrigues (Téc. Informática) Cláudia Pinto (Professora TIC) Susana Esteves (Professora TIC)	Horário de trabalho	• Ponto de restauro no sistema	• Backups / Veeam • Softwares de recuperação • Watchguard
Fuga de informação (Ex: Phishing,	Sérgio Rodrigues (Téc. Informática) Cláudia Pinto	Horário de trabalho	• Diagnóstico • Consultar logs • Bloquear acessos e passwords	• Backups • Servidores • Gestão de users • Antivírus

…)	(Professora TIC)		• Reconfiguração	• Watchguard

Assim, o plano de resposta a incidentes é um programa estruturado e elaborado para ajudar a identificar, gerir e enfrentar incidentes cibernéticos. A criação deste plano de resposta foi considerada essencial para a proteção da empresa, sabendo que a sua gestão envolve constantes atualizações e formações.

Destacamos as 6 etapas que identificámos como essenciais:

1. **Preparação**

Esta fase é o ponto de partida do plano de resposta a incidentes e, em última análise, talvez a fase mais importante para proteger o negócio como um todo.

É preciso garantir que os colaboradores estejam devidamente capacitados acerca das suas responsabilidades e funções, caso ocorra um incidente. O plano deve ser bem fundamentado, detalhando as funções e responsabilidades de todos. Para assegurar que cada um desempenhe o papel que lhe foi atribuído, é preciso colocar o plano à prova. Para isso, é preciso avaliar o seu nível de proteção e resposta. São conduzidas, ocasionalmente, invasões ou violações de dados simulados. Quanto mais bem preparados estiverem os funcionários, menor será a probabilidade de cometerem erros críticos. Certificamo-nos de que todos os aspetos do plano de resposta sejam aprovados e que os recursos necessários estejam disponíveis antecipadamente, quando possível. “Prevenir é melhor do que remediar”. Aspiramos a ser proativos, não reativos.

2. **Identificação**

Nesta etapa, é determinada a possível violação. Um incidente, pode originar-se de várias maneiras. Por isso, é o momento de abordar algumas questões essenciais para a identificação:

Perguntas a serem abordadas:

- Quando é que o evento/incidente ocorreu?
- Como foi detetado?
- Quem o detetou?
- Quais as áreas que foram impactadas?
- Qual é o alcance do comprometimento?
- As operações foram afetadas?
- A falha ou a origem do incidente foi descoberta?

3. **Contenção**

Quando um incidente ocorre, a reação inicial pode ser de apagar tudo o mais rápido possível para que o problema

simplesmente desapareça. No entanto, isso é prejudicial a longo prazo, visto que pode destruir evidências úteis para determinar a origem da violação e para ajudar num plano de prevenção para evitar que algo ocorra novamente.

O melhor a fazer é conter a violação para que não se propague e cause mais danos ao negócio. Se possível, são desconectados da internet os dispositivos afetados. Existem estratégias de contenção de curto e longo prazo já preparadas. É crucial um bom sistema de backup para ajudar a restaurar as operações comerciais. Assim, qualquer dado ou ativo comprometido não será perdido definitivamente.

Este é o momento de atualizar e corrigir os sistemas, rever protocolos de acesso, alterar todas as credenciais de acesso de utilizadores e administrativos.

4. **Erradicação**

Uma vez contida a situação, é preciso encontrar e eliminar a causa da violação. Portanto, os sistemas devem ser corrigidos, atualizações devem ser aplicadas, e isso tem de ser realizado de modo minucioso, para que não haja vestígios de malware ou qualquer outra questão de segurança nos sistemas.

5. **Recuperação**

Esta é a etapa de restauração e restituição dos sistemas e dispositivos afetados, do seu ambiente digital. É fundamental que seja bem estruturada para garantir a continuidade dos negócios e para restabelecer a normalidade dos sistemas.

6. **Takeaways**

Depois de concluída a investigação, é preciso perceber o que foi aprendido com o incidente. Por isso, é importante reunir todas as partes envolvidas para discutir e analisar e registar o que foi feito e o que pode ser feito futuramente, avaliando o que correu bem no plano de resposta e onde houve alguma falha. As lições aprendidas, tanto numa simulação quanto num incidente real, ajudarão a fortalecer os sistemas contra possíveis ataques no futuro. É preciso abordar as seguintes perguntas:

- Que mudanças devem ser feitas na segurança?
- O que poderia ter sido feito, que não foi feito?
- Que falhas foram exploradas pela violação?
- Como garantir que uma violação semelhante não aconteça novamente?

Ninguém quer passar por um incidente de segurança. Mas, planear e estar preparado é essencial. Responsabilidade

digital, é saber o que fazer se, ou quando, algo acontecer.

Contactos do CNCS

- Gabinete Nacional de Segurança | Centro Nacional de Cibersegurança
- Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11
- cncs@cncs.gov.pt

T.GP – Gestão da palavra-passe

- Algumas passwords de softwares e aplicações fulcrais ao negócio estão alojadas no cofre e com a Chefe dos Serviços Administrativos.
- A gestão dos utilizadores e passwords online são geridas através do Active Directory.
- Os users podem consultar as passwords online/offline no chrome, caso as tenham guardado.

T.PAD – Privilégios de acesso diferenciados

O princípio do privilégio mínimo (PoLP, na sigla em inglês) é um conceito de segurança da informação no qual um usuário recebe os níveis mínimos de acesso necessários para desempenhar suas funções de trabalho. É uma prática de segurança cibernética muito recomendada, além de ser uma etapa fundamental na proteção do acesso privilegiado a dados e ativos de alto valor. Esse conceito acaba por ser baseado na frase “Menos é Mais” de Ludwig Mies van der Rohe, um dos arquitetos mais influentes do Século XX. Ou seja, menos privilégios, mais segurança.

Entretanto, na segurança digital, o privilégio mínimo vai além do acesso humano. Afinal, pode ser estendido a aplicativos, sistemas ou dispositivos conectados que requerem privilégios para executar uma tarefa. Isso garante que a ferramenta não humana tenha o acesso necessário – e nada mais.

Neste contexto, a aplicação de privilégios mínimos requer uma maneira diferenciada de gerir e proteger de forma centralizada as credenciais, juntamente com controlos flexíveis que possam equilibrar os requisitos de segurança cibernética e conformidade com as necessidades operacionais e do usuário final.

Na ESCO é aplicado este conceito na atribuição de acessos, sendo atribuídas permissões conforme os grupos de trabalho em que está inserido.

T.SC – Securização *(hardening)* de configurações

Os equipamentos mais recentes têm ativada a tecnologia TPM 2.0, nos mais antigos não é aplicável. Esta tecnologia é um padrão internacional para um processador criptográfico seguro, um microcontrolador dedicado projetado para

proteger o hardware por meio de chaves criptográficas integradas.

O SecureBoot UEFI está configurado e a BIOS está protegida por palavra-passe.

Cabe a cada utilizador instalar o adblock nos seus browsers, caso assim o entendam.

O Watchguard está configurado na escola, com regras de entrada e saída de dados, nomeadamente controlo de browser. Este sistema contém definidas as políticas de firewall. Estão ativados os serviços de webblocker para sites não categorizados ou categorizados como inseguros, por predefinição. Está configurado também o controlo de bloqueio por aplicações (Ex: aplicações como bittorrent, facebook, crypto, …). Este procedimento pode ser consultado mais em detalha em **Pr.12 - Firewall – Rede Alunos.**

A VPN permite aos users entrarem no sistema e rede da escola, quando fora da mesma. Estando aplicadas as mesmas regras, políticas e restrições.

T.CA – Controlo aplicacional

A Política de utilizador definida e configurada para alunos e colaboradores, não tendo estes, permissões para instalação. Quando existem necessidades de instalação deve ser feito o pedido ao departamento de TIC.

T.RAR – Recolha e armazenamento de registos

Os logs podem ser consultados nos servidores no Windows Logs.

03 | Termos e definições

- PUA – Política de Utilização Aceitável
- ESCO – Escola de Serviços e Comércio do Oeste
- SWOT – Strengths, Weaknesses, Opportunities, and Threats
- GUT – Gravidade, Urgência e Tendência
- SPF – Sender Policy Framework
- HTTPS – Hyper Text Transfer Protocol Secure
- DKIM – Domain Keys Identified Mail
- HSTS – HTTP Strict Transport Security
- NAS – NAS (Network Attached Storage
- DVR – Digital Video Recorder
- TIC – Tecnologia de Informação e Comunicação
- ISO – International Organization for Standardization

- DNP TS – Documento Normativo Português – Especificação Técnica
- TPM – Trusted Platform Module
- IRP – Incident Response Plan
- CNCS – Centro Nacional de Cibersegurança
- VPN – Virtual Private Network