POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

O objetivo da Política de Segurança da Informação da Unidade Local de Saúde de Braga (ULSB) é estabelecer a estratégia e referencial de segurança da informação e proteção dos dados que a ULSB necessita para exercer a sua atividade. A estratégia e todas as políticas e procedimentos da ULSB devem refletir os prossupostos deste documento.

2. ÂMBITO

Aplica-se a todos os colaboradores, fornecedores e parceiros da ULSB, bem como a qualquer pessoa ou entidade que tenha acesso a equipamentos ou sistemas de informação da ULSB (por exemplo: utentes, visitantes).

3. RESPONSABILIDADES

A Política de Segurança da Informação (PSI) deve ser:

- **Aprovada** pelo Conselho de Administração (CA) da ULSB;
- **Publicada** para consulta de todos os colaboradores na *intranet* da ULSB, para utentes, parceiros e fornecedores no site da ULSB;
- **Comunicada** internamente e externamente pelo Responsável da Segurança de Informação (CISO);
- **Revista** anualmente pelo Diretor do Serviço de Sistemas de Informação e pelo Responsável pela Proteção de Dados (DPO);
- **Atualizada** pelo CISO.

4. REFERÊNCIAS, DEFINIÇÕES, ABREVIATURAS, PALAVRAS CHAVE E PRINCIPAIS ALTERAÇÕES

Critérios de Referência [Manual CHKS, 2022]: 14.3, 14.4, 14.5, 14.6, 14.8.

CA – Conselho de Administração

CISO – *Chief Information Security Officer* – Responsável pela Segurança da Informação

PSI – Política de Segurança da Informação

SSI – Serviço de Sistemas de Informação

ULSB – Unidade Local de Saúde de Braga

Palavras Chave: Cibersegurança, CISO, Dados, Informação, ISO 27001, Segurança.

Principais Alterações:

- Alargamento do âmbito do documento para a ULSB.

5. DESCRIÇÃO DO PROCESSO

5.1 Princípios Fundamentais

A Segurança da Informação é a proteção de informação de um amplo conjunto de ameaças através de um processo de gestão de riscos, garantindo a continuidade de negócio e maximizando o retorno em investimentos efetuados. A PSI define os procedimentos a adotar para proteger a informação que a ULSB necessita para realizar o seu propósito. Isto inclui, em conformidade com a norma ISO/IEC 27000:2016, perceber e gerir riscos quanto à confidencialidade, integridade e disponibilidade da informação, bem como de legitimidade, como a autenticação e a não repudiação.

- Confidencialidade – assegurar que a informação é acessível somente por pessoas devidamente autorizadas. O acesso à informação é, por conseguinte, restrito a utilizadores considerados legítimos.
- Integridade – garantir a veracidade, autenticidade e exatidão da informação, bem como os seus métodos de processamento ao longo de todo o processo, garantindo que o conteúdo não seja adulterado.
- Disponibilidade – assegurar o acesso à informação, a quem se encontre devidamente credenciado e legitimamente autorizado. A informação está acessível quando se revelar necessária.
- Legitimidade – a recolha da informação é feita nos estritos limites da lei que é aplicável ao objeto da recolha.

5.2 Princípios Gerais de Segurança da Informação

Os colaboradores da ULSB:

- Devem comunicar imediatamente qualquer falha ou não conformidade identificada na Segurança da Informação de acordo com o PRO.027 – *Notificação de Eventos Adversos*;
- Não devem fazer passar-se por outra pessoa ou dissimular sua identidade quando utilizam os recursos de sistemas de informação da ULSB;
- Responsabilizar-se pela sua identidade eletrónica, *passwords*, credenciais de autenticação, autorização ou outro dispositivo de segurança, não partilhando com ninguém esta informação;
- Responder pela utilização indevida das suas contas e dos recursos ao seu dispor em qualquer circunstância;

- Não divulgar informação interna e/ou confidencial, exceto nas situações previstas na lei, devendo, para tal efeito, recorrer a aconselhamento deontológico e jurídico, nas respetivas entidades internas;
- Não conectar dispositivos externos a equipamentos ou infraestrutura da ULSB, nomeadamente pen's, Discos Externos, Routers, Dispositivos Wi-Fi, etc. ;
- Não abrir emails de origem desconhecida que contenham links ou anexos;
- Não executar aplicações não autorizadas previamente pelo SSI.

5.3 Organização da Segurança da Informação

As responsabilidades ao nível da segurança da informação estão distribuídas pelas várias Direções da ULSB. Para realizar uma adequada gestão da Segurança da Informação é fundamental a existência de uma estrutura organizacional que a suporte e esteja consciente da sua relevância, bem como exista uma coordenação e alinhamento estratégico, e uma abordagem multidisciplinar à Segurança da Informação na ULSB.

É por isso necessário detalhar o compromisso, as atividades e as responsabilidades de todos os envolvidos no que concerne à temática da Segurança da Informação da ULSB.

5.3.1 Responsabilidades do Conselho de Administração

O CA deve fomentar ativamente a Segurança da Informação na ULSB, através de orientações claras, demonstração de envolvimento, delegação de tarefas explícitas e evidenciando o conhecimento das responsabilidades de Segurança da Informação. Neste sentido, o CA deve:

- Assegurar que os objetivos da Segurança da Informação identificados se encontram alinhados com os requisitos de negócio do Hospital e estão integrados nos processos relevantes.
- Rever e aprovar as políticas de Segurança da Informação.
- Rever a efetividade da implementação das políticas de Segurança da Informação.
- Aprovar planos e programas de sensibilização dos colaboradores do Hospital relativamente à Segurança da Informação.
- Aprovar a definição de responsabilidades específicas para a Segurança da Informação transversalmente a todas as Direções e Serviços da ULSB.

- Assegurar que a implementação dos controlos de Segurança da Informação é coordenada transversalmente no Hospital.
- Facultar orientações claras e demonstrar *commitment* relativamente às iniciativas de Segurança da Informação.
- Assegurar os recursos necessários e adequados à implementação efetiva da Segurança da Informação na ULSB.
- Informar as entidades externas que prestem serviços na ULSB (ex.: prestador de serviços de Sistemas de Informação ou de segurança física) sobre as políticas e regulamentos de Segurança da Informação em vigor.

5.3.2 Funções da Segurança da Informação

O CA tem a responsabilidade máxima pela Segurança da Informação na ULSB, neste sentido, delega no SSI a responsabilidade de definir, coordenar e supervisionar a implementação do plano de Segurança da Informação na ULSB, nomeadamente no que respeita à implementação das políticas e regulamentos de Segurança da Informação, bem como assegurar que os procedimentos definidos no âmbito da Segurança da Informação estão a ser seguidos. Têm como responsabilidade, coordenar em conjunto com as outras Direções e Serviços da ULSB, com responsabilidades no âmbito da Segurança da Informação, a implementação efetiva do plano de Segurança da Informação.

É responsabilidade do CA a nomeação dentro dos elementos do SSI do Responsável da Segurança de Informação (CISO) e do Contacto Permanente de Segurança. O CISO será normalmente o Diretor do SSI, mas o CA poderá nomear outro colaborador dentro da equipa do SSI. O Contacto Permanente de Segurança deverá ter disponibilidade contínua de 24 horas por dia e de sete dias por semana e tem como função a assegurar os fluxos de informação de nível operacional e técnico com o CNCS – Centro Nacional de Cibersegurança.

- Responsável da Segurança de Informação (CISO – *Chief Information Security Officer*)
    - Responsabilidades:
        - Elaborar e manter atualizada a PSI;
        - Elaborar e manter atualizado o Plano de Segurança;
        - Elaborar o Relatório Anual;
        - Assegurar que as atividades de Segurança da Informação são realizadas em conformidade com a política de Segurança da Informação da ULSB.
        - Gerir não conformidades e assegurar que as mesmas estão a ser endereçadas.

- Propor metodologias e processos para a Segurança da Informação, tais como, avaliação do risco, classificação da informação, entre outros.
- Avaliar o impacto, na Segurança da Informação, de eventuais alterações ao ambiente envolvente da ULSB, na vertente de tecnologias de informação e de processos de negócio.
- Avaliar a existência de competências no que concerne à Segurança da Informação e coordenar, pelo envolvimento das pessoas com as competências adequadas, a implementação de controlos de Segurança da Informação.
- Identificar a necessidade de obter aconselhamento interno e/ ou externo no âmbito da Segurança da Informação e rever/ coordenar os resultados obtidos.
- Promover a formação e sensibilização dos colaboradores, em relação à Segurança da Informação, de forma transversal na ULSB.
- Avaliar a informação recolhida nas atividades de monitorização e auditoria e avaliação e reporte de incidentes de Segurança da Informação, e recomendar ações de melhoria alinhadas com os incidentes identificados.

- <u>Contacto Permanente de Segurança</u>
  - Responsabilidades:
    - A articulação inter-setorial, incluindo a eficácia da resposta a incidentes de segurança com impacto a nível dos setores;
    - A obtenção de informação operacional e técnica, na sequência de notificação de incidentes com impacto relevante ou substancial submetida pela mesma ou outra entidade;
    - A obtenção e atualização de informação de situação integrada no contexto de um incidente com impacto relevante ou substancial;
    - A partilha de informação quando estejam ativados planos de emergência de proteção civil diretamente relacionados ou com impacto ao nível da segurança do ciberespaço, bem como de planos no âmbito do planeamento civil de emergência do ciberespaço ou dos planos de segurança das infraestruturas críticas nacionais ou europeias;
    - A operacionalização dos procedimentos fixados no âmbito de um plano de emergência de proteção civil quando tenham impacto no funcionamento das redes e sistemas de informação, ou do planeamento civil de emergência do ciberespaço;

- A receção das instruções técnicas emitidas ao abrigo do disposto no n.º 5 do artigo 7.º do Regime Jurídico da Segurança do Ciberespaço e no artigo 18.º;
- A operacionalização dos procedimentos fixados no âmbito dos planos de segurança previstos no artigo 7.º

5.3.3. Responsabilidades do Serviço de Sistemas de Informação

O SSI tem as seguintes responsabilidades no âmbito da Segurança da Informação:

- Apoiar na definição e manutenção das políticas e regulamentos de Segurança da Informação.
- Elaborar e formalizar os procedimentos de Segurança da Informação que suportam a operacionalidade das políticas e regulamentos de Segurança da Informação definidos no âmbito dos Sistemas de Informação.
- Implementar medidas/ controlos necessários à operacionalização das políticas, regulamentos e procedimentos de Segurança da Informação nos domínios da sua abrangência, definida no REG.001 – *Regulamento Interno*.
- Garantir a implementação das iniciativas de Segurança da Informação no âmbito dos Sistemas de Informação.
- Apoiar na elaboração e manutenção de uma metodologia de análise de risco, incluindo a identificação de vulnerabilidades, a probabilidade de ocorrência das ameaças e o impacto dos riscos identificados no negócio.
- Assegurar que as medidas/ controlos de Segurança da Informação se encontram efetivamente operacionais e operam conforme previsto no âmbito dos Sistemas de Informação.
- Definir os requisitos de Segurança da Informação para novos desenvolvimentos de Sistemas de Informação.
- Analisar os planos estratégicos dos Sistemas de Informação em curso, assegurando o seu desenvolvimento em alinhamento com a estratégia de Segurança da Informação da ULSB.
- Colaborar com ações de auditoria relacionadas com a Segurança da Informação, nomeadamente, ao nível dos Sistemas de Informação. Concluída a auditoria, a Direção do SSI deverá analisar e assegurar a coordenação e acompanhamento da implementação das ações de melhoria que permitam mitigar as deficiências identificadas.
- Identificar possíveis vulnerabilidades no âmbito da Segurança da Informação, bem como, atuar perante incidentes de Segurança da Informação com potencial impacto na prestação de cuidados de saúde.

No âmbito da segurança física é da responsabilidade do Serviço de Sistemas de Informação:

- Zelar pela manutenção de todos os ativos físicos/infraestruturas informáticas nas suas instalações (nomeadamente dentro do *Datacenter)* ou outras onde se encontrem localizados ativos da ULSB (nomeadamente de suporte à informação);

No âmbito da conformidade, a Direção do SSI é responsável por:

- Assegurar a conformidade dos Sistemas de Informação com as políticas e regulamentos de Segurança da Informação definidos pela ULSB.
- Assegurar a proteção da informação da ULSB de acordo com a legislação aplicável em vigor.
- Assegurar a existência de mecanismos de segurança física no *Datacenter* e noutras localizações onde se encontrem ativos físicos/infraestruturas informáticas da ULSB.
- Definir planos de recuperação de SI/ TI alinhados com a política de gestão da continuidade de negócio da ULSB.

5.3.4. Responsabilidades Transversais

As Direções e Serviços da ULSB devem definir, em colaboração com o proprietário da informação (titular dos dados), os perfis de acesso às aplicações informáticas e de seguida informar formalmente o SSI (Serviço responsável pela implementação) dos perfis de acesso definidos.

As Direções e Serviços da ULSB responsáveis pela seleção de entidades externas (fornecedoras de bens ou serviços) devem seguir as políticas e regulamentos definidos e aplicáveis a este processo.

As Direções e Serviços da ULSB devem comunicar aos colaboradores as suas responsabilidades, em matéria de Segurança da Informação, tais como: confidencialidade da informação, utilização dos sistemas de informação de acordo com as políticas e regulamentos definidos, código de conduta/ ética aplicável, entre outros.

Todos os colaboradores da ULSB são responsáveis pelo cumprimento das políticas e regulamentos de Segurança da Informação em vigor, assim, estes deverão cumprir com as cláusulas de confidencialidade, utilização adequada e responsável dos equipamentos informáticos e documentos físicos, zelar pela segurança dos ativos da ULSB e comunicar qualquer incidente de Segurança da Informação identificado.

5.4 Políticas, Processos e Documentos da Segurança de Informação

5.4.1 Processo de Gestão da Segurança de Informação

O nível desejado de segurança da informação estabelece-se através de políticas, procedimentos, comportamentos, gestão do risco e controlo, ao longo dos seguintes processos:

- **Prevenção**: Assegurar que os incidentes de segurança não acontecem;
- **Deteção**: Deteção rápida e eficaz de incidentes que não podem ser previstos;
- **Correção**: Resposta de recuperação eficaz aos incidentes após a sua deteção.

A cada um destes processos associam-se os seguintes documentos:

Prevenção:

- PRO.SSI.001 – *Gestão de Backups*
- PRO.082 – *Gestão de Passwords e Log-on Seguro*
- PRO.105 – *Utilização do Correio Eletrónico*
- PRO.108 – *Gestão de Acessos a Sistemas*
- IDT.090 – *Acessos Externos a Sistemas de Informação*

Deteção:

- PRO.080 – *Pedidos de Helpdesk*
- POL.076 – *Atuação e Caso de Avaliação de Dados Pessoais*

Correção:

- PRO.109 – *Contingência para Falhas no Sistema*
- POL.066 – *Gestão da Continuidade do Negócio*
- POL.076 – *Atuação e Caso de Avaliação de Dados Pessoais*

5.4.2. Documentos Obrigatórios

- Plano de Segurança (Artigo 7.º do Decreto-Lei n.º 65/2021)

  A USLB deve elaborar e manter atualizado um plano de segurança, devidamente documentado e assinado pelo responsável de segurança, que contenha:

  - A política de segurança, incluindo a descrição das medidas organizativas e a formação de recursos humanos;

- A descrição de todas as medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes;
- A identificação do responsável de segurança;
- A identificação do ponto de contacto permanente.

- Relatório Anual (Artigo 8.º do Decreto-Lei 65/2021)

  A ULSB deve elaborar um relatório anual que, em relação ao ano civil a que se reporta, contenha os seguintes elementos:

  - Descrição sumária das principais atividades desenvolvidas em matéria de segurança das redes e dos serviços de informação;
  - Estatística trimestral de todos os incidentes, com indicação do número e do tipo dos incidentes;
  - Análise agregada dos incidentes de segurança com impacto relevante ou substancial, com informação sobre:
    - Número de utilizadores afetados pela perturbação do serviço;
    - Duração dos incidentes;
    - Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
  - Recomendações de atividades, de medidas ou de práticas que promovam a melhoria da segurança das redes e dos sistemas de informação;
  - Problemas identificados e medidas implementadas na sequência dos incidentes;
  - Qualquer outra informação relevante.

5.5 Desenvolvimento de Competências Digitais

Colaboradores com boas competências digitais, estarão melhor habilitados para valorizar a importância desta política e serão ativos relevantes na deteção, prevenção e correção de incidentes de segurança de informação. Colaboradores com poucas ou nenhumas competências digitais poderão representar maior vulnerabilidade para os sistemas e segurança da informação.

O SSI deverá promover informação e formação regular, quer (1) ajudando anualmente o Serviço de Gestão de Recursos Humanos a identificar as ações de formação mais adequadas para cada tipo de perfil, bem como, (2) promovendo iniciativas de informação e diagnóstico do nível de maturidade e exposição dos

colaboradores às diferentes ameaças de segurança, como, por exemplo, através da realização de ações de *pishing* simuladas, organização de workshops, partilhando vídeos formativos, etc..

6. DOCUMENTOS RELACIONADOS

- POL.066 – Gestão da Continuidade do Negócio
- POL.076 – Atuação em Caso de Violação de Dados Pessoais
- PRO.080 – Pedidos de *Helpdesk*
- PRO.082 – Gestão de *Passwords* e *Log-on* Seguro
- PRO.105 – Procedimento de Utilização do Correio Eletrónico
- PRO.109 – Contingência para Falhas no Sistema
- PRO.108 – Gestão de Acessos a Sistemas
- IDT.090 – Acessos Externos a Sistemas de Informação
- PRO.SSI.001 - Gestão de *Backups*

Referências:

- Plano Estratégico da ULSB
- Decreto-Lei n.º 65/2021 - Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019;
- Framework de referência de Governação, Gestão e Operação do eSIS;
- ITIL 4: Information Technology Infrastructure Library
- RESILIA® Cyber Resilience Best Practice
- COBIT® 5: A Business Framework for the Governance and Management of Enterprise IT
- ISO/IEC 27000:2016. Information technology – Security techniques – Information security management systems – Overview and vocabulary.
- ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.
- ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security controls.
- ISO 27799:2008. Health informatics – Information security management in health using ISO/IEC 27002

REVISTO	APROVADO
Coordenadora Interina do Serviço de Sistemas de Informação Maria do Céu Vivas	Presidente do Conselho de Administração Domingos Sousa Vogal Executivo Américo Afonso