Politécnico de Coimbra

RELATÓRIO DE AVALIAÇÃO INTERCALAR DO PLANO DE GESTÃO DE RISCOS – IPC E SASIPC

Outubro de 2022

Politécnico de Coimbra

Ficha Técnica

Título

Relatório de Avaliação intercalar do Plano de Gestão de Riscos – IPC e SASIPC

Coordenação

Ana Ferreira

Edição

Departamento de Planeamento, Auditoria e Qualidade do Instituto Politécnico de Coimbra

Outubro de 2022

Conteúdo

Introdução

Para a elaboração do presente relatório foi solicitado às UO do IPC que avaliassem o grau de implementação das medidas previstas para os processos de risco elevado do Plano de Gestão de Riscos do IPC 2021-2023 e indicassem as ações desenvolvidas tendo em vista a plena implementação dessas medidas.

Os relatórios, elaborados de acordo com um modelo pré-definido, foram disponibilizados durante os meses de setembro e outubro de 2022. O presente relatório resulta da consolidação e análise da informação disponibilizada.

Resultados a destacar e recomendações

1. Avaliação do grau de implementação das medidas previstas no Plano de Gestão de Riscos do IPC 2021-2023

- 38% das respostas indicaram não se terem iniciado medidas de mitigação ou eliminação do risco;
- 29% das respostas indicaram estarem em curso medidas de mitigação ou eliminação do risco;
- 26% das respostas indicaram que as medidas de mitigação ou eliminação do risco foram implementadas na totalidade;
- 8% das respostas não indicaram qualquer grau de implementação das medidas previstas.

A distribuição das respostas por unidade orgânica encontra-se descrita no quadro seguinte. Como se pode constatar, o grau de implementação das medidas previstas é muito díspar entre UO. Os Serviços Centrais, I2A e SASIPC (que apresentaram relatório conjunto, uma vez que partilham serviços nesta área de risco) e o ISCAC são as UO que apresentam um maior grau de implementação das medidas previstas, com mais de metade das mesmas implementadas na totalidade.

Subsiste um conjunto de respostas em que algumas UO consideram não lhes serem aplicáveis determinadas medidas do PGR, o que deverá ser clarificado.

Quadro 1 – Distribuição percentual das respostas relativas ao grau de implementação das medidas previstas no PGR 2021-2023 para os processos de risco elevado

	Medida por iniciar	Medida em curso	Medida implementada na totalidade	Não responde
ESAC	26%	47%	16%	11%*
ESEC	68%	16%	5%	11%
ESTESC	26%	47%	11%	16%*
ESTGOH	79%	21%	0%	0%
ISCAC	0%	26%	58%	16%*
ISEC	37%	26%	37%	0%
SC+I2A+SASIPC	26%	16%	58%	0%
Total	**38%**	**29%**	**26%**	**8%**

* A UO considera que a medida não lhe é aplicável;

** A UO justifica a ausência da resposta da seguinte forma:

- Medida 6.2.5 - «Na medida em que a ESEC não tem forma de mitigar a exploração de eventuais conflitos de interesse (ex: aluno da ESEC e funcionário dos serv. Académicos), não identificamos medidas para atuar sobre esta situação.»;
- Medida 6.2.7 - «A partilha de credenciais está limitada a um espetro muito reduzido de atuação (contas de e-mail dos gabinetes/centros/serviços) e a alteração desta metodologia tem um impacto considerável na atuação dos serviços.»

2. Ações desenvolvidas para a plena implementação das medidas previstas

A análise dos relatórios permite constatar:

- A existência de um elevado peso das medidas em curso ou implementadas na totalidade sem reporte de ações desenvolvidas tendo em vista a sua plena implementação (60%);
- Uma elevada disparidade de respostas entre UO relativamente às ações desenvolvidas tendo em vista a plena implementação das medidas previstas no PGR. Efetivamente, enquanto em algumas unidades se verificou um elevado peso da ausência de reporte das ações desenvolvidas para a plena implementação das medidas em curso ou implementadas na totalidade (ESAC, ESTESC, ESTGOH e ISCAC, com 100% de ausência de reporte nessas medidas), noutras esse peso foi reduzido ou nulo (ESEC e SC+I2A+SASIPC, com reporte de ações em todas as medidas em curso ou implementadas na totalidade; ISEC com ausência de reporte em 8% dessas medidas);
- A adoção de soluções idênticas em diversas medidas entre as UO que apresentam ações desenvolvidas, o que poderá indiciar a possibilidade de adoção de protocolos de atuação comuns nas diferentes UO do IPC e a adoção de estratégias e planos de implementação comuns.

Quadro 2 – Medidas em curso ou implementadas na totalidade sem reporte de ações desenvolvidas

	N.º de medidas em curso ou implementadas na totalidade sem reporte de ações desenvolvidas [1]	Total de medidas em curso ou implementadas na totalidade [2]	Não reporte em medidas em curso ou implementadas na totalidade (%) [1]/[2]
ESAC	12	12	100%
ESEC	0	4	0%
ESTESC	11	11	100%
ESTGOH	4	4	100%
ISCAC	16	16	100%
ISEC	1	12	8%
SC	0	14	0%
Total	**44**	**73**	**60%**

Avaliação do grau de implementação das medidas preventivas previstas nos processos de risco elevado

Processo 6.2 - Gestão de acessos a informação por intermédio de sistemas informáticos – Utilização de acessos

Medida	UO	Ações desenvolvidas para a plena implementação da medida	Grau de implementação da medida		
			Por iniciar	Em curso	Implementada na totalidade
6.2.1 - Definição e implementação de políticas que reforcem a segurança das credenciais de acesso utilizadas (ex.: aumento do número mínimo de caracteres, obrigatoriedade de alteração periódica)	ESAC	Não reportado		x	
	ESEC	Aumento de número mínimo de carateres e número mínimo de classes de carateres nas credenciais		x	
	ESTGOH	Não reportado		x	
	ESTESC	Não reportado			x
	ISCAC	Não reportado		x	
	ISEC	Implementada política de passwords com 8 caracteres e mínimos de uma letra, um número e um caracter alfanumérico.			x
	I2A	As mesmas ações desenvolvidas pelo DTIC-SC			x
	SC	Aplicação de restrições na definição de passwords ao nível dos sistemas de gestão de identidade e acessos, com vista ao reforço da sua segurança (resiliência a ataques de dicionário, etc)			x
	SASIPC	As mesmas ações desenvolvidas pelo DTIC-SC			x
6.2.2 - Implementação, sempre que possível, de mecanismos de autenticação forte em aplicações e sistemas informáticos críticos (e.g. cartão cidadão/certificados digitais, impressão digital ou autenticação duplo fator)	ESAC	Não aplicável à unidade orgânica	NR*	NR*	NR*
	ESEC	Implementação de autenticação de dois fatores para site e webmail	X		
	ESTGOH	Não reportado	X		
	ESTESC	Não reportado	X		
	ISCAC	Não aplicável à unidade orgânica	NR*	NR*	NR*
	ISEC	Não reportado	x		
	I2A	As mesmas ações desenvolvidas pelo DTIC-SC		x	
	SC	Avaliadas soluções de Autenticação Multifator (MFA) passíveis de serem aplicadas a sistemas mais críticos, nomeadamente, acessos VPN, sistema NONIO, etc		x	
	SASIPC	As mesmas ações desenvolvidas pelo DTIC-SC		x	
6.2.3 - Implementação de medidas visando a divulgação de normas de segurança e formação aos utilizadores sobre cibersegurança (Ciber Higiene)	ESAC	Não reportado		x	
	ESEC	Divulgação de ações de formação sobre cibersegurança		x	
	ESTGOH	Não reportado		x	
	ESTESC	Não reportado	x		
	ISCAC	Não reportado		x	
	ISEC	Não reportado	X		
	I2A	As mesmas ações desenvolvidas pelo DTIC-SC			x
	SC	Participação ativa na campanha ProtegeOTeuCampus, para sensibilização em cibersegurança, dinamizado			x

Medida	UO	Ações desenvolvidas para a plena implementação da medida	Grau de implementação da medida		
			Por iniciar	Em curso	Implementada na totalidade
		pelo Grupo de Trabalho de Cibersegurança da Meta rede; Realização continuada de ações de sensibilização aos trabalhadores.			
	SASIPC	As mesmas ações desenvolvidas pelo DTIC-SC			x
6.2.4 - Implementação de medidas visando a ativação dos registos de atividade (logs) de todos os sistemas e aplicações que disponham destes mecanismos	ESAC	Não reportado			x
	ESEC	Exportação e centralização de logs rsyslog em sistema de armazenamento centralizado Ativação de logs em todos os sistemas que não permitam a sua exportação		x	
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado		x	
	ISCAC	Não reportado			x
	ISEC	Os sistemas já efetuam registos, menos as firewalls que estão em fase de substituição.		x	
	I2A	As mesmas ações desenvolvidas pelo DTIC-SC			x
	SC	Ativação de registos de atividade em todos os sistemas informáticos que dispõem destes mecanismos; Implementação de mecanismos de auditoria em todos os sistemas informáticos desenvolvidos internamente.			x
	SASIPC	As mesmas ações desenvolvidas pelo DTIC-SC			x
6.2.5 - Implementação de medidas visando a minimização de situações conducentes a acumulação de perfis que possam resultar em conflito de interesses	ESAC	Não aplicável à unidade orgânica	NR*	NR*	NR*
	ESEC	Na medida em que a ESEC não tem forma de mitigar a exploração de eventuais conflitos de interesse (ex: aluno da ESEC e funcionário dos serv. Académicos), não identificamos medidas para atuar sobre esta situação.	NR*	NR*	NR*
	ESTGOH	Não reportado	x		
	ESTESC	Não aplicável à unidade orgânica	NR*	NR*	NR*
	ISCAC	Não reportado			x
	ISEC	Não reportado	x		
	I2A	As mesmas ações desenvolvidas pelo DTIC-SC	x		
	SC	Não reportado	x		
	SASIPC	Não reportado	x		
6.2.6 - Definição formal de políticas de segurança que sustentem a implementação de medidas com vista à "Restrição de acesso à informação baseado no princípio necessidade de conhecer"	ESAC	Não reportado	x		
	ESEC	Elaboração de política de segurança e proteção de dados	x		
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado	x		
	ISCAC	Não reportado			x

Medida	UO	Ações desenvolvidas para a plena implementação da medida	Grau de implementação da medida		
			Por iniciar	Em curso	Implementada na totalidade
	ISEC	Definição de grupos de utilizadores. Aplicação de permissões de acesso apenas pelos grupos a que seja necessário o acesso.			x
	I2A	As mesmas ações desenvolvidas pelo DTIC-SC			x
	SC	Definição no SIGQ de processos, subprocessos, orientações técnicas e modelos, que permitem apoiar a implementação da medida, nomeadamente: P-07.05 – Segurança informática; SP-07.05.01 – Gestão de acessos a recursos TIC; Modelo 749 - Recolha de dados para criação de credenciais de acesso a recursos TIC; OrT_07.01 - Política de gestão das contas de utilizador; OrT_07.02 - Regras de utilização dos recursos e serviços TIC; Modelo 746 - Ficha de Acesso a Recursos TIC.			x
	SASIPC	As mesmas ações desenvolvidas pelo DTIC-SC			x
6.2.7 - Implementação de medidas visando a eliminação da utilização de credenciais de acesso partilhadas por mais do que um recurso humano	ESAC	Não reportado			x
	ESEC	A partilha de credenciais está limitada a um espetro muito reduzido de atuação (contas de e-mail dos gabinetes/centros/serviços) e a alteração desta metodologia tem um impacto considerável na atuação dos serviços.	NR*	NR*	NR*
	ESTGOH	Não reportado		x	
	ESTESC	Não aplicável à unidade orgânica	NR*	NR*	NR*
	ISCAC	Não reportado			x
	ISEC	Não reportado	x		
	I2A	As mesmas ações desenvolvidas pelo DTIC-SC		x	
	SC	Eliminação gradual do recurso a credencias partilhadas ainda em uso nalguns sistemas.		x	
	SASIPC	As mesmas ações desenvolvidas pelo DTIC-SC		x	

Processo 6.3 - Gestão de acessos físicos a áreas de armazenamento e processamento de informação – acesso às áreas técnicas

Medida	UO	Ações desenvolvidas para a plena implementação da medida	Grau de implementação da medida		
			Por iniciar	Em curso	Implementada na totalidade
6.3.1 - Implementação de medidas visando a definição de procedimentos formais para controlo do acesso físico às áreas técnicas	ESAC	Não reportado			x
	ESEC	Elaboração de política de segurança e proteção de dados	x		
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado		x	

Medida	UO	Ações desenvolvidas para a plena implementação da medida	Grau de implementação da medida		
			Por iniciar	Em curso	Implementada na totalidade
	ISCAC	Não reportado			x
	ISEC	Identificação do utilizador através de sistema de cartão nos Departamentos: DEE, EEM, DEIS e Serviços Administrativos. Outros em Curso			x
	SC		x		
6.3.2 - Implementação de medidas visando a salvaguarda das chaves de acesso aos locais recorrendo a mecanismos mais robustos (cofres com controlo de acesso por PIN ou biométricos, entre outros)	ESAC	Não reportado	x		
	ESEC	Aquisição de estrutura modular resistente a intrusão	x		
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado		x	
	ISCAC	Não reportado			x
	ISEC	Chaveiros protegidos por cofres com código localizados nos Departamentos e Sala dos Funcionários.			x
	SC	Aquisição de cofres com PIN e acesso biométrico para guardar as chaves de acesso às áreas técnicas.			x
6.3.3 - Implementação de mecanismos de controlo de acesso mais robustos nas áreas técnicas mais críticas (por ex. centro de dados)	ESAC	Não reportado	x		
	ESEC	Aquisição de estrutura modular resistente a intrusão	x		
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado		x	
	ISCAC	Não reportado			x
	ISEC	Acesso exclusivo ao SGIT. Porta especial com segurança reforçada.			x
	SC	Implementação de um sistema de controlo de acesso eletrónico aplicado às portas das áreas técnicas mais críticas, por intermédio de cartões RFID, dotada de com gestão centralizada.			x
6.3.4 - Implementação de sistemas de videovigilância nas áreas técnicas mais críticas	ESAC	Não reportado	x		
	ESEC	Aquisição e instalação de câmaras IP	x		
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado	x		
	ISCAC	Não reportado			x
	ISEC	Não reportado		x	
	SC	Não reportado	x		
6.3.5 - Implementação de mecanismos de registo automático de acessos às áreas mais críticas, preferencialmente com alarmística	ESAC	Não reportado	x		
	ESEC	Aquisição de estrutura modular resistente a intrusão	x		
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado			x
	ISCAC	Não aplicável à unidade orgânica	NR*	NR*	NR*

Medida	UO	Ações desenvolvidas para a plena implementação da medida	Grau de implementação da medida		
			Por iniciar	Em curso	Implementada na totalidade
	ISEC	Sensores de Movimento.			x
		Alarmística		x	
	SC	Registo de acesso associado ao mecanismo de controlo de acesso com gestão centralizada implementado na medida 6.3.3			x

Processo 6.10 - Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos em situação de catástrofe

Medida	UO	Ações desenvolvidas para a plena implementação da medida	Grau de implementação da medida		
			Por iniciar	Em curso	Implementada na totalidade
6.10.1 - Implementação de medidas visando a criação de um plano de continuidade de negócio, baseado nas recomendações da norma internacional ISO/IEC 27031	ESAC	Não reportado		x	
	ESEC	Constituição de data center redundante em site secundário para sistemas críticos	x		
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado	x		
	ISCAC	Não reportado		x	
	ISEC	Não reportado	x		
	I2A	As mesmas ações desenvolvidas pelo DTIC-SC	x		
	SC	Não reportado	x		
	SASIPC	As mesmas ações desenvolvidas pelo DTIC-SC	x		
6.10.2 - Implementação de um centro de dados destinado a sustentar processos de recuperação de desastre (Disaster Recovery), como parte integrante do plano de continuidade de negócio	ESAC	Não reportado		x	
	ESEC	Constituição de datacenter redundante em site secundário para sistemas críticos	x		
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado		x	
	ISCAC	Não reportado		x	
	ISEC	Existe um segundo centro de dados, mas com condições precárias. Falta um espaço próprio, climatização adequada, equipamentos que permitam HA em caso de falha.		x	
	SC	Definida e preparada a área técnica remota para acolher a instalação do DR (Residências R1/R2); Realizada a aquisição dos equipamentos necessários à implementação do DR; Iniciado projeto de implementação.		x	

Processo 6.14 - Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - sistemas de armazenamento de informação

Medida	UO	Ações desenvolvidas para a plena implementação da medida	Grau de implementação da medida		
			Por iniciar	Em curso	Implementada na totalidade
6.14.1 - Definição e implementação de planos de manutenção de hardware	ESAC	Não reportado		x	
	ESEC	Elaboração e execução de plano de manutenção	x		
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado		x	
	ISCAC	Não reportado			x
	ISEC	Limpeza de PC, upgrades de discos e memória.		x	
	SC	Definição no SIGQ do processo SP-07.04.02– Manutenção das infraestruturas e equipamentos TIC			x
6.14.2 - Definição e implementação de planos de manutenção de software	ESAC	Não reportado		x	
	ESEC	Elaboração e execução de plano de manutenção	x		
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado		x	
	ISCAC	Não reportado			x
	ISEC	Reinstalação anual dos computadores dos laboratórios.			x
	SC	Elaboração e execução de plano de manutenção			x

* NR : Não Reportado

Medida	UO	Ações desenvolvidas para a plena implementação da medida	Grau de implementação da medida		
			Por iniciar	Em curso	Implementada na totalidade
6.14.3 - Implementação de planos de backup e de replicação da informação, que garantam objetivos de recuperação devidamente ajustados à criticidade dos sistemas	ESAC	Não reportado		x	
	ESEC	Execução da política de backups			x
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado		x	
	ISCAC	Não reportado			x
	ISEC	Implementação de plano de backups utilizando a solução da Quest – Rapid Recovery, com periodicidade e retenção possível pela storage existente.			x
	SC	Definição no SIGQ de processos, subprocessos e orientações técnicas, com o objetivo de definir os procedimentos associados à realização de cópias de segurança da informação digital, nomeadamente, P-07.05 – Segurança informática; SP-07.05.02 – Cópias de segurança; OrT_07.03 - Plano de Backup de sistemas/infraestruturas TIC.			x
6.14.4 - Replicação da informação para sistemas de armazenamento deslocalizados de forma a garantir resiliência da informação em caso de destruição dos sistemas de armazenamento principais.	ESAC	Não reportado		x	
	ESEC	Constituição de datacenter redundante em site secundário para sistemas críticos	x		
	ESTGOH	Não reportado	x		
	ESTESC	Não reportado		x	
	ISCAC	Não reportado		x	
	ISEC	Não reportado	x		
	SC	Implementado processo de cópia diária de backups (backups 2ª linha) para uma localização remota ao data center principal.			x

Processo 6.15 - Gestão de segurança de informática

Medida	UO	Ações desenvolvidas para a plena implementação da medida	Grau de implementação da medida		
			Por iniciar	Em curso	Implementada na totalidade
6.15.1 - Definição formal e operacionalização de uma estrutura de suporte às questões relacionadas com a segurança informática (SI), que atue ao nível de toda a instituição e que esteja devidamente dotada dos meios humanos e materiais, necessários para: • Coordenar e apoiar as várias unidades orgânicas na reposta a incidentes de segurança informática e respetiva articulação com o CERT.PT, CNCS e CNPD (no caso de violações de dados pessoais); • Promover ações de esclarecimento e sensibilização à comunidade na área da ciber segurança; • Implementar mecanismos de segurança passíveis de serem utilizados por todas as UO (dns firewall, entre outros); • Auditar serviços e redes informáticas, com o objetivo de identificar potenciais falhas e aconselhar a mitigação das mesmas; • Definição de políticas de segurança.	ESAC	Não reportado		x	
	ESEC	Elaboração e execução da política de segurança e proteção de dados	x		
	ESTGOH	Não reportado		x	
	ESTESC	Não aplicável à unidade orgânica			
	ISCAC	Não aplicável à unidade orgânica			
	ISEC	Não reportado	x		
	I2A	As mesmas ações desenvolvidas pelo DTIC-SC	x		
	SC	Não reportado	x		
	SASIPC	As mesmas ações desenvolvidas pelo DTIC-SC	x		

Assinado por : **CRISTIANA DA LUZ CUNHA TOURAIS**
Num. de Identificação Civil: BI085363855
Data: 2022.10.10 10:26:18 Hora de Verão de GMT

CARTÃO DE CIDADÃO

Relatório aprovado a ____/____/_____ por:

_____

(Órgão da UO/ nome e cargo do dirigente que aprovou o relatório)