Segurança da Informação

Classificação de Segurança

Questões de um/a arquivista

Ao refletir sobre o apoio técnico que presto, para garantir boas praticas de gestão documental/processual, encontro o primeiro ativo informacional que tenho de proteger - informações de suporte à decisão/decisões de um determinado procedimento em aplicações (*Outlook*, *TEAMS*, *WhatsApp*), as quais não são alvo de *backup*, logo irrecuperáveis a longo prazo.

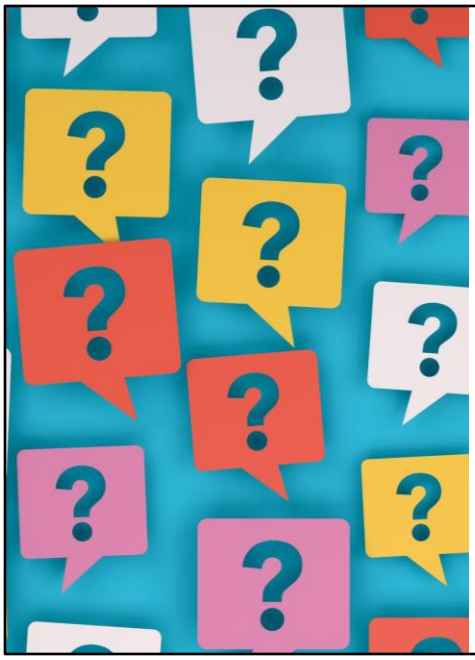
Numa outra lembrança ocorreu-me a proteção **através da obrigatoriedade da classificação da informação**, isto porque sem esta **não há avaliação do seu valor**, e consequentemente seleção para conservação (**adoção de medidas técnicas e organizativas de segurança da informação**) ou para eliminação (destruição segura e irrecuperável).

Paralelamente à memória da obrigatoriedade de classificação importa garantir a proteção dos ativos informacionais com o desenvolvimento dos níveis de confidencialidade, visto que, **e apesar de nosso sistema existir um botão confidencial**, a sua aplicação e manutenção não é ágil, ou seja, por defeito mantém acessível a todas as pessoas que já intervieram ou fazem parte do Serviço destinatário, o que não está correto – **deveria permitir a exclusão do acesso até então e inserção de acessos** em cada fase de desenvolvimento até ser público, **diminuindo assim gradualmente a confidencialidade**.

Caso Prático – Parecer CADA - 352/2025

Vem solicitar nomeadamente sobre Infraestrutura de *Datacenter*:

- Relatórios mensais (Anos de 2023, 2024 e 2025);
- Análise a disponibilidade de serviços críticos (Anos de 2023, 2024 e 2025);
- Atas das Reuniões mensais (Anos de 2023, 2024 e 2025);
- Ata *Site Survey*, Ano de 2023;
- Relatório de ocorrência de falha em serviços críticos (Anos de 2023, 2024 e 2025);
- Análises de risco (Anos de 2023, 2024 e 2025);
- Validar ativos (Anos de 2023, 2024);
- Listagem de todos os Ticket's abertos pelos diferentes municípios no ano de 2025, com data de abertura, tipo de incidente e data de encerramento;
- Cópias dos relatórios de acompanhamento da execução do contrato por parte do CIMAC nos anos de 2023, 2024 e 2025;
- Cópias, se existir, de comunicações por parte da CIMAC de incumprimento contratual;
- Cópias, se existir, de penalizações aplicadas.



A CADA

A CIMAC pede parecer como consulente, e o autor do pedido apresenta queixa à CADA porque não obteve resposta em tempo útil ao seu pedido... a CADA vem apensar os dois processos e dar resposta.

Consulente pede parecer à CADA

"... /Ora, os documentos em questão contêm informação crítica e confidencial sobre a atividade digital da CIMAC e dos seus municípios associados, podendo a sua partilha colocar em causa a segurança da informação, com a consequente exposição a ciberataques, o que contradiz as obrigações constantes no âmbito do RJSC. /Importa, igualmente, aferir se estes documentos se enquadram como documentos administrativos, (...). /"

Posição da CADA – Documento Administrativo

- Os documentos solicitados respeitam à execução de um contrato de aquisição de serviços de Operação e Gestão de Infraestrutura de «*Data Center*»;
- A LADA entende por documento administrativo qualquer conteúdo, ou parte desse conteúdo, que esteja na posse ou seja detido em nome dos órgãos e entidades» sujeitas à LADA, «seja o suporte de informação sob forma escrita, visual, sonora, eletrónica ou outra forma material, neles se incluindo, designadamente, aqueles relativos a; / - cf. artigo 3.º, 1, a) da LADA
  - i) Procedimentos de emissão de atos e regulamentos administrativos;
  - ii) Procedimentos de contratação pública, incluindo os contratos celebrados;
  - iii) Gestão orçamental e financeira dos órgãos e entidades;
  - iv) Gestão de recursos humanos, nomeadamente os dos procedimentos de recrutamento, avaliação, exercício do poder disciplinar e quaisquer modificações das respetivas relações jurídicas.

Não pode haver duvidas que são documentos administrativos

A regra geral de acesso a documentos administrativos consta do artigo 5.º, 1, da LADA: «*Todos, sem necessidade de enunciar qualquer interesse, têm direito de acesso aos documentos administrativos, o qual compreende os direitos de consulta, de reprodução e de informação sobre a sua existência e conteúdo*».

Restrições de Acesso

Artigo 6.º / «1. Os documentos que contenham informações cujo conhecimento seja avaliado como podendo pôr **em risco interesses fundamentais do Estado** ficam sujeitos a interdição de acesso ou a acesso sob autorização, durante o tempo estritamente necessário, **através de classificação operada através do regime do segredo de Estado** ou por outros regimes legais **relativos à informação classificada**.».

Para já importa saber que o DL 20/2022 que aprova os procedimentos de identificação, designação, proteção e aumento da resiliência das infraestruturas criticas nacionais, e o seu anexo identificam o setor das infraestruturas digitais e prestadores de serviços digitais como infraestrutura critica.

Como visto atrás A consulente invoca que «*os documentos (...) contêm informação crítica e confidencial sobre a atividade digital da CIMAC e dos seus municípios associados*».

(1) -

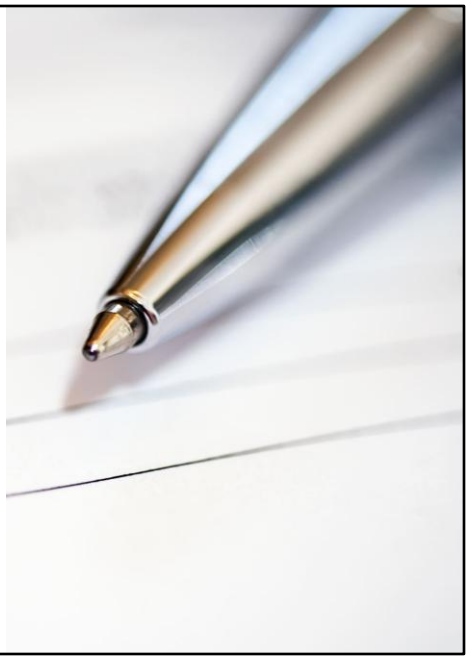
Na exceção do artigo 6.º, 1, da LADA, é condição de restrição, interdição de acesso ou acesso sob autorização, que tenha havido classificação operada através do regime do segredo de Estado ou ao abrigo de outro regime legal de classificação de informação. No caso esta não indicou que a documentação tivesse sido classificada nem explicitou qualquer regime ao abrigo do qual uma classificação dos documentos tivesse ocorrido. A mera alusão à existência de documento com informação confidencial, sem a concretização exigida pelo artigo 6.º, 1, da LADA, não traduz suficiente fundamentação para se perceber se

há lugar a derrogação de um direito com assento constitucional como o direito de acesso aos documentos administrativos.
Para que [os documentos] sejam, efetivamente, de acesso reservado é necessária a sua prévia classificação diretamente por lei ou pela entidade com competências para o fazer./ Não basta, por um lado, uma simples classificação de facto; é imperativo que o documento seja, de jure, um documento classificado./ (...) Se os documentos em questão forem documentos classificados, serão objeto de uma reserva de comunicação. No entanto, convirá notar que não basta a simples aposição de um carimbo (contendo uma das menções "Muito secreto", "Secreto"; "Confidencial"; "Reservado", ou rotulando um documento como Segredo
de Estado") para que a possibilidade de acesso seja restringida. É que, muitas vezes, acontece que tais "marcas" (sobretudo, as de confidencial e reservado) são colocadas por motivos de mera eficiência administrativa. Para que os documentos solicitados (...) sejam, realmente, de acesso condicionado, é necessário que tenham sido (e permaneçam) classificados, nos termos legais, por uma entidade com competência para o fazer, devendo o ato que que eventualmente denegue o acesso pretendido ser fundamentado.

E, assim, se os documentos não tiverem sido classificados nos termos da lei, não há razão para não disponibilizar o acesso pretendido.» **Atenção, credenciação GNS para material classificado.**

Restrições de Acesso

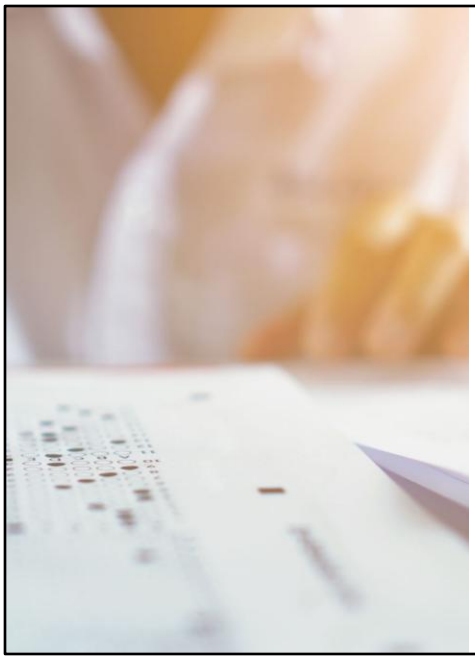
Artigo 6.º / «6. Um terceiro só tem direito de acesso a **documentos administrativos que contenham segredos comerciais, industriais ou sobre a vida interna de uma empresa** se estiver munido de autorização escrita desta ou demonstrar fundamentadamente ser titular de um interesse direto, pessoal, legítimo e constitucionalmente protegido suficientemente relevante após ponderação, no quadro do princípio da proporcionalidade, de todos os direitos fundamentais em presença e do princípio da administração aberta, que justifique o acesso à informação.».



(2) -

Diz ainda a consulente: «*Ao aceder a este tipo de informação sobre a gestão e operação da infraestrutura de Data Center, a referida empresa ganharia vantagens comerciais na apresentação de uma proposta comercial ao próximo procedimento contratual*».

Existir alguma informação sujeita a restrição de acesso, nomeadamente, em razão de segredo comercial, é necessária uma concretização mínima./ 7. Na verdade, não basta a mera alegação, genérica, desprovida de concretização factual, sendo que ela deve ser feita, preferencialmente, em relação a cada um dos documentos que integram o procedimento em causa. Por exemplo na *delimitação do que seja um segredo comercial e industrial juridicamente relevante deverá atender ao disposto no artigo 313.º, n.º 1, do Código da Propriedade Industrial, aprovado pelo Decreto Lei n.º 110/2018, de 10 de dezembro*.



Restrições de Acesso

Artigo 6.º / «7. Sem prejuízo das demais restrições legalmente previstas, os documentos administrativos **ficam sujeitos a interdição de acesso ou a acesso sob autorização**, durante o tempo estritamente necessário à salvaguarda de outros interesses juridicamente relevantes, **mediante decisão do órgão ou entidade competente, sempre que contenham informações cujo conhecimento seja suscetível** de: /a) (...); /b) **Colocar em causa a capacidade operacional ou a segurança das (...) e das infraestruturas críticas**; / (...)»

(3) –

A consulente refere ainda que a «*partilha* [da informação crítica e confidencial sobre a atividade digital da CIMAC e dos seus municípios associados pode] *colocar em causa a segurança da informação, com a consequente exposição a ciberataques, o que contradiz as obrigações constantes no âmbito do RJSC*.» Há, contudo, que ter presente que a decisão sobre a medida da restrição - «*interdição do acesso ou a acesso sob autorização, durante o tempo estritamente necessário à salvaguarda de outros interesses juridicamente relevantes*» - deve:

a) Ser fundamentada, cabendo à consulente concretizar, para cada documento, o motivo pelo qual o conhecimento de cada informação é suscetível de colocar em causa a segurança da infraestrutura crítica;

b) Ser tomada pelo órgão ou entidade competente.

Resumo da posição da CADA

Não é um carimbo ou um botão de confidencial no sistema de gestão documental que vai garantir a segurança da informação, até no âmbito da transparência administrativa

- *Não basta uma simples classificação de facto; é preciso que o documento seja, de jure, um documento classificado (...)». / E, assim, se os documentos não tiverem sido classificados nos termos da lei, não há razão para não disponibilizar o acesso pretendido:*
- *Mediante decisão do órgão competente, a interdição de acesso deve ser fundamentada para cada documento, com o motivo pelo qual o conhecimento de cada informação é suscetível de colocar em causa a segurança da infraestrutura critica;*

Gabinete Nacional de Segurança – Framework Segnac 1

Classificação de segurança - Fundamentada

Conclusão do Parecer

A regra é a da publicidade e transparência dos contratos públicos, tanto na fase da formação como na fase da execução, tendo em vista o escrutínio da atividade administrativa;

Essa documentação é, em regra, livremente acessível;

A documentação relativa à operação e gestão de infraestrutura de «*Data Center*» **poderá justificar a aplicação de restrição de acesso**, nos termos previstos no artigo 6.º, 7, *b)*, da LADA;

Perante cada pedido de documento, cabe à entidade requerida verificar a existência de restrições ao direito de acesso;

A recusa do acesso deve ser comunicada ao requerente, de forma concreta e fundamentada em relação a cada documento, nos termos do artigo 15.º, 1, c), da LADA, não bastando a mera alusão genérica à existência de restrição ao acesso.

É neste PODERÁ JUSTIFICAR a APLICAÇÃO DE RESTRIÇÃO DE ACESSO que a mim me parece que deve ser trabalhado a classificação documental.

É pois ao nível da **Determinação da comunicabilidade de documentos e informação, atribuição de níveis de Segurança à informação e forma de fundamentação, por politica ou regulamento institucional de Classificação de Segurança da Informação** (Entrada na Tabela de Seleção 300.30.300)


Segurança
da
Informação

O RJSC

O RJSC impõe medidas que devem:

Garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes e, se aplicáveis, **as normas europeias e internacionais pertinentes**, bem como os custos de execução e a viabilidade financeira destes;

Medidas de Cibersegurança que abranjam por exemplo a Segurança dos recursos humanos, **políticas seguidas em matéria de controlo do acesso e gestão de ativos**;

O que me leva no caso a algumas notas

Notas

- Na gestão de ativos, concretiza-se a avaliação de risco mediante o valor que o ativo possui para a entidade assim como a probabilidade de divulgação ou acesso indevido acontecer. Na Administração Pública os ativos de informação poderem ser considerados documentos administrativos e por regra de acesso livre, o que **leva à necessidade de um controlo para concretizar uma real medida de segurança** contra o acesso "legal" à informação, quando esta é crítica ou referente a infraestruturas críticas; **ESTE É UM RISCO A SER IDENTIFICADO**

- Consultando a portaria arquivística, temos por exemplo (e agarrando no caso prático do parecer em análise) que para a implementação de redes e sistemas tecnológicos 300.40.508 ou para monitorização de redes e sistemas tecnológicos 300.40.510 com um PCA de 10 anos ou até mesmo o processamento de pedidos de serviços de suporte 300.50.801 com PCA de 5 anos;

- Questão? Que arquivos possuem estas informações após procedimento... ou melhor, que Serviços de Tecnologia após esta informação passar a processo a faz chegar a arquivo? E estará corretamente classificada perante o Regulamento para a Classificação e Avaliação da Informação Arquivística da Administração Local?

A AVALIAÇÃO DE RISCO, vai permitir a adoção de controlos para mitigar o RISCO. Na identificação de um risco de acesso a informação critica via Lei de Acesso a Documentos Administrativos, e permitindo esta alguns tipos de restrição que devem ser fundamentados e regulados internamente, o Controlo de GESTÃO DE ATIVOS com CLASSIFICAÇÃO DE SEGURANÇA e CONTROLO DE ACESSOS parece-me Fundamental.

A Classificação Arquivística não pode ser só vista como a forma de organizar o sistema de informação que permita determinar prazos de conservação (e obviamente a conservação) e destinos finais, mas deve ser também usada para determinar o valor dos ativos de informação, classificá-los fundamentadamente quanto à sua segurança e conseguir gerir os níveis de acesso ao longo da sua vida. É todo um serviço de gestão da informação, onde a gestão da sua segurança está integrada, e importa saber que para quem trabalha a gestão da informação, tem acesso à mesma com as inerentes responsabilidades.

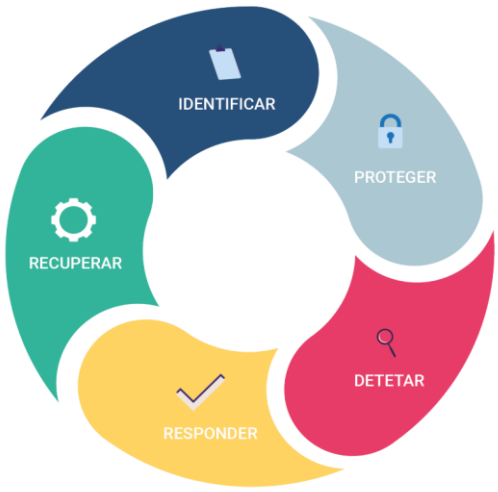


Figura 8- Objetivos de Segurança

QUADRO NACIONAL DE REFERÊNCIA PARA A CIBERSEGURANÇA

A legislação fala na aplicação de normas europeias ou internacionais para **Garantir um nível de segurança das redes e dos sistemas de informação.**

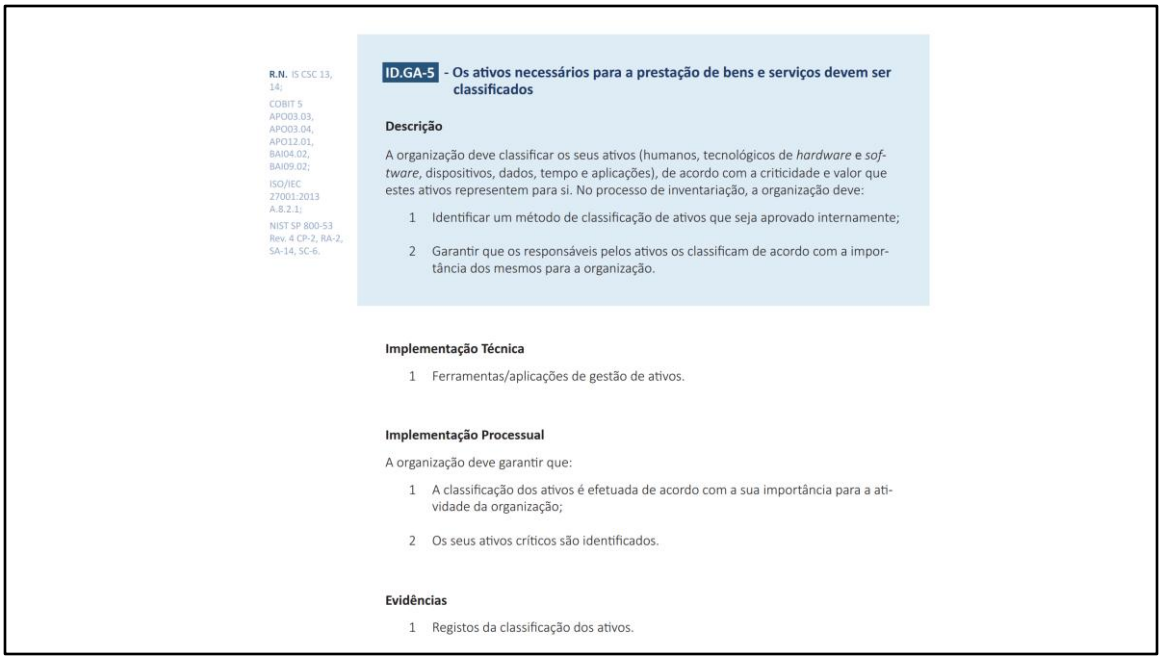
O QNRC é desenvolvido pelo nosso CNCS, e tem por base algumas das normas internacionais mais conhecidas na área da segurança da informação, e por isso o fui buscar como exemplo, até porque também passa a ser possível a certificação de uma entidade em termos de conformidade com o Quadro Nacional de Referência para a Cibersegurança e que permite que as organizações públicas e privadas possam atestar, através da certificação, a implementação das suas práticas de cibersegurança organizativas, processuais, tecnológicas e humanas.

O QNRC apresenta medidas de segurança/controlos nas diferentes fases de segurança, como apresenta a imagem.

Identificar

CATEGORIA	DESCRIÇÃO	SUBCATEGORIAS
ID.GA **Gestão de ativos**	A organização deve identificar os dados, colaboradores, equipamentos, sistemas e instalações que permitem cumprir os seus objetivos no decorrer da sua atividade. Devem ser identificados e geridos de forma consistente com aquela que é a sua relevância no cumprimento dos objetivos da organização e com a estratégia de gestão do risco.	ID.GA-1 ID.GA-2 ID.GA-3 ID.GA-4
	cibersegurança.	
ID.AR **Avaliação do risco**	A organização tem noção dos riscos de cibersegurança no âmbito da sua atividade (incluindo missão, funções, imagem ou reputação), ativos organizacionais e pessoas.	ID.AR-1 ID.AR-2 ID.AR-3 ID.AR-4 ID.AR-5

Logo no identificar temos a medida de Gestão de Ativos e Avaliação de Risco, onde temos os dados e onde a classificação da informação, usando uma tabela de seleção, pode e deve ajudar na determinação do valor do ativo em questão.



R.N. IS CSC 13, 14;
COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02;
ISO/IEC 27001:2013 A.8.2.1;
NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6.

ID.GA-5 - Os ativos necessários para a prestação de bens e serviços devem ser classificados

Descrição

A organização deve classificar os seus ativos (humanos, tecnológicos de *hardware* e *software*, dispositivos, dados, tempo e aplicações), de acordo com a criticidade e valor que estes ativos representem para si. No processo de inventariação, a organização deve:

1 Identificar um método de classificação de ativos que seja aprovado internamente;

2 Garantir que os responsáveis pelos ativos os classificam de acordo com a importância dos mesmos para a organização.

Implementação Técnica

1 Ferramentas/aplicações de gestão de ativos.

Implementação Processual

A organização deve garantir que:

1 A classificação dos ativos é efetuada de acordo com a sua importância para a atividade da organização;

2 Os seus ativos críticos são identificados.

Evidências

1 Registos da classificação dos ativos.

O ID.GA-5 que faz parte da fase de IDENTIFICAR estabelece a medida inserida na Avaliação de Risco:

OS ATIVOS NECESSÁRIOS PARA A PRESTAÇÃO DE BENS E SERVIÇOS DEVEM SER CLASSIFICADOS

Para os ativos DADOS/INFORMAÇÃO faz todo o sentido usar a tabela de seleção, o histórico de arquivo na entidade, e trabalhar internamente e com os responsáveis/proprietários dos ativos a classificação de segurança, partindo da tabela de seleção (Até porque mesmo na transposição desta classificação de segurança para a Gestão Documental, ficará mais digamos... automatizada)

Proteger

CATEGORIA	DESCRIÇÃO	SUBCATEGORIAS
PR.GA **Gestão de identidades, autenticação e controlo de acessos**	Os acessos aos ativos físicos, lógicos e às instalações associadas devem ser limitados às pessoas, processos e equipamentos autorizados. Estes devem ser geridos de acordo com a avaliação do risco de acesso não autorizado.	PR.GA-1 PR.GA-2 PR.GA-3 PR.GA-4 PR.GA-5 PR.GA-6 PR.GA-7

Também no proteger temos a Gestão de Identidades e controlo de acessos. Ao longo da vida de um ativo de informação é importante que o responsáveis pelo serviço de gestão da informação, arquivo, tenham capacidade de trabalhar este controlo de acessos, tal como ELENCADO pelo/a arquivista logo no meu primeiro SLIDE "– **deveria permitir a exclusão do acesso até então e inserção de acessos** em cada fase de desenvolvimento até ser público"

Monitorizar

DE.MC **Monitoriza-ção Contínua de Segurança**	As redes e sistemas de informação devem ser monitorizadas para identificação de eventos de cibersegurança e verificação da eficácia das medidas de proteção aplicadas.	DE.MC-1 DE.MC-2 DE.MC-3 DE.MC-4 DE.MC-5 DE.MC-6 DE.MC-7 DE.MC-8

Será que em termos de monitorização não existe aqui também uma responsabilidade do serviço de gestão da informação/serviço de arquivo? Que mais não seja na deteção de falhas procedimentais e medidas aplicadas que devem ser melhoradas ou alteradas? Também como elencado no primeiro SLIDE na identificação de uma falha no arquivo de dados de mensagens de correio eletrónico ou mensagens instantâneas?

Obrigado

São medidas de segurança/controlos que têm de ser desenvolvidos por meio de políticas ou regulamentos internos, e que se tratando de ativos de informação quer física como digital, e cujo conteúdo seja critico para a operacionalidade e segurança da entidade, os serviços de gestão de informação/arquivo têm de fazer parte nas suas definições, para se evitar situações como as que apresentei neste caso prático.