RELATÓRIO FINAL DE AUDITORIA Nº 04/2025 – PROCESSO Nº 1908/2025

PLANO DE AUDITORIA INTERNA 2025 – RESOLUÇÃO ADMINISTRATIVA Nº 008/2025

UNIDADE RESPONSÁVEL	AUDITORIA INTERNA
ENTIDADE	CÂMARA MUNICIPAL DE VIANA
CNPJ	27.427.277/0001-51
GESTOR	JOILSON BROEDEL
CARGO	PRESIDENTE
OBJETO	VERIFICAÇÃO DE CONFORMIDADE SOBRE AS APLICAÇÕES DE TECNOLOGIA DA INFORMAÇÃO, TOMANDO POR COMPARAÇÃO OS RECURSOS DE SOFTWARES E HARDWARES EXISTENTES E SUAS EFETIVAS APLICAÇÕES SOBRE OS PROCESSOS INTERNOS, TAIS COMO SEGURANÇA CIBERNÉTICA, VIRTUALIZAÇÃO, ENTRE OUTROS ASPECTOS QUE DEPENDEM O/OU MOVEM A INFRAESTRUTURA TECNOLÓGICA INSTALADA.
UNIDADE EXECUTORA	SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

I. OBJETIVO E ESCOPO

Auditoria de Conformidade para verificar a relação da tecnologia com o ambiente operacional, os controles existentes, e o grau de utilização do novo parque de Tecnologia da Informação instalado. Vamos analisar aspectos de segurança envolvendo os servidores e os equipamentos em operação; a existência de um inventário completo dos hardwares instalados, inclusive com gerenciamento da vida útil e contratos de manutenção; o planejamento e desenvolvimento de programas de capacitação dos servidores sobre as melhores práticas de segurança cibernética. Nesse contexto, o objetivo da Auditoria busca jogar luz sobre o melhor uso dos recursos instalados, na expectativa de que eles possam ser otimizados em favor dos processos operacionais, da virtualização ao armazenamento em nuvens, garantindo segurança, transparência e agilidade na gestão dos recursos da Câmara Municipal.

Avenida Florentino Ávidos, nº40 – Centro- Viana/ES- CEP 29.130-065
http://www.camaraviana.es.gov.br

Todo o trabalho seguiu a metodologia abaixo e a matriz de planejamento anexa.

II. DA METODOLOGIA APLICADA

A **Secretaria de Tecnologia da Informação e Comunicação** e seus registros são as fontes deste trabalho. Temos como foco identificar o inventário de TIC (patrimônio); o planejamento; o desenvolvimento de estratégias, inclusive treinamento; o nível de integração das soluções (softwares) contratadas; as medidas de segurança cibernética e o backup de dados; as ações operadas a partir do Datacenter. O trabalho busca identificar ações que ultrapassem as práticas corretivas que vigoravam antes da instalação do parque atual. Os esforços devem se voltar também para o campo preventivo. Assim, nossos trabalhos consistiram em, junto com os dirigentes da Secretaria de TIC, observar o alcance dos recursos instalados, sejam nos cuidados de segurança exigidos, na propagação de sinais através de uma rede interna (Intranet), sempre considerando que os usuários/servidores são parte imprescindível para o funcionamento desses processos, os quais, portanto, devem ser treinados para extração dos melhores resultados de todo investimento tecnológico colocado à disposição.

Observar também as medidas de segurança sobre proteção de dados e garantia de confidencialidade, com olhar sobre firewalls, antivírus, controle de acesso sobre câmeras de monitoramento, política de senhas, backups regulares, nobreak, licenças para uso de softwares, contratos de manutenção, sem perder de vista o sistema de controle do imobilizado.

IV. BASE LEGAL

Lei Nº 9.609, de 19 de Fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, as normas estabelecidas para o processo de contratação pública, o cumprimento dos prazos e demais requisitos legais.

Lei 12.527, de 18 de Novembro de 2011 – Lei de Acesso a Informação (LAI). Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da

Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991;

Lei 13.709, de 14 de Agosto de 2018 – Lei Geral de Proteção de Dados – LGPD - dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

IV. RESULTADOS E CONCLUSÃO

Os itens trazidos pelos autos 1403/2024, em atendimento às solicitações desta Auditoria, possuem materialidade suficiente para análise performada na Matriz de Planejamento e Metodologia Aplicada. O objetivo foi verificar os mecanismos de controle utilizados nos processos de instalação e utilização dos recursos de Tecnologia da Informação e Comunicação (TIC) instalados.

A análise foi desenvolvida buscando responder as questões de auditoria trazidas pela Matriz de Planejamento, quais sejam:

Questão 1) Há uma política de governança dedicada a Tecnologia da Informação e Comunicação?

Objetivamente, a governança é um sistema de direcionamento e controle do uso atual e futuro da TIC, garantindo que as ações de TI estejam alinhadas aos objetivos estratégicos da organização e que as estratégias estejam alinhadas aos objetivos do negócio, promovendo o uso eficiente dos recursos, a gestão de riscos, a transparência, a responsabilidade e o retorno dos investimentos.

Pela nossa análise, parece lógico supor que o atual cenário da câmara, levando em conta os recentes investimentos em recursos tecnológicos, não só impõe a construção de um **"Planejamento Estratégico"** para o setor, mas também a instituição de um **"Comitê interno"** que possa orientar a aplicação das estratégias de TIC, como forma de mensurar desempenhos e mitigar riscos;

Avenida Florentino Ávidos, nº40 – Centro- Viana/ES- CEP 29.130-065
http://www.camaraviana.es.gov.br

Questão 2) Existe uma gestão sobre os recursos de TIC (gestão de ativos, contratos, licenças, hardware, software)?

A gestão de ativos sobre os recursos de TIC pressupõe alcançar hardware e softwares através de um inventário, que não só cumpra a função técnica do registro contábil, mas busque prevenir riscos e autorizar a governança sobre recursos como contratos, licenças, infraestrutura de rede, intranet, capacitação interna, entre outros. Pelo caráter administrativo envolvido, a sugestão é que uma **"Instrução Normativa (IN)"** possa regular as ações necessárias à gestão dos ativos;

Questão 3) Existe política para infraestrutura de TIC (conectividade, servidores, datacenter)?

Ao tratar de infraestrutura, referimo-nos a problemas decorrentes de conectividade, Datacenter, Beckup, Helpdesk, firewalls, Antivírus, entre outros. As evidências demonstram que nosso ecosistema tecnológico interno precisa qualificar o uso desses recursos, com o intuito de permitir integrações mais resolutivas, em favor da segurança e da qualidade que os trâmites operacionais requerem. Aqui vale indicar que o **"Governo do ES disponibiliza gratuitamente o Edocs"** (https://edocs.es.gov.br/), o qual, pelo sua base estrutural, tem por mérito, além de atualização frequente, a garantia de mais produtividade e transparência, com extensão à sociedade;

Questão 4) Existe uma política de segurança para sistemas e acessos?

Em ambiente tecnológico institucional a segurança é gênero que se aplica a vários setores, em alguns casos com especificidades próprias de cada setor. Sendo assim, também por essa razão, parece natural que no quesito segurança cibernética a instituição deva elaborar uma uma "Instrução Normativa (IN)" que dê lastro a uma Política de Segurança (PSI), visando gerenciar desde as permissões de acessos aos **sistemas operacionais administrativos**, até os **acessos às câmaras de videomonitoramento interno.** É imperativo que a política de segurança defina seus objetivos institucionais, demarcando os limites em que se possa promover a interoperabilidade, garantindo transparência, sem fragilizar o ambiente operacional interno.

V. RECOMENDAÇÕES

1) Construção de um **"Planejamento Estratégico"** específico para TIC – Tecnologia da Informação e Comunicação e a instituição de um **"Comitê Interno"** que possa orientar a aplicação das estratégias delineadas no planejamento, como forma de mensurar desempenhos e mitigar riscos;

2) Elaboração de uma **"Instrução Normativa (IN)"** possa regular as ações necessárias à gestão dos ativos, sejam eles baseados em softwares ou hardwares, inclusive seus respectivos contratos e/ou licenças;

3) Indicação gratuita do Edocs, disponbilizado pelo Governo do ES através da Prodest (https://edocs.es.gov.br/), o qual, pelo sua base estrutural, tem por mérito, além de atualização frequente, a garantia de mais produtividade e transparência, com extensão à sociedade;

4) Elaborar uma uma **"Instrução Normativa (IN)"** visando gerenciar, desde as permissões de acessos aos **sistemas operacionais administrativos**, até os **acessos às câmaras de videomonitoramento interno.** A política de segurança cumpre objetivo institucional e demarca os limites da interoperabilidade, garantindo transparência, sem fragilizar o ambiente operacional interno.

Apresentamos o Relatório Final para conhecimento da Presidência e setor auditado, o qual deve retornar a esta Auditoria para consequente publicação.

Viana, 10 de Novembro de 2025.

Avenida Florentino Ávidos, nº40 – Centro- Viana/ES- CEP 29.130-065
http://www.camaraviana.es.gov.br

MATRIZ DE PLANEJAMENTO

OBJETIVO: verificar conformidade sobre as aplicações de Tecnologia da Informação, tomando por referências os recursos de software e hardware existentes e o cumprimento de suas funções no ambiente operacional.

	Tabela Referencial	Questões de Auditoria	Informações Requeridas	Fontes de Informações	Procedimentos de Auditoria	Possíveis Achados
Q1	2.2.13	Há uma política de governança dedicada a Tecnologia da Informação e Comunicação?	Planejamento Estratégico específico para TIC; Comitê técnico para área de TIC.	Um plano estratégico alinhado ao planejamento institucional da câmara; Um comitê atuante que toma decisões estratégicas sobre TIC.	Verificar a existência de um plano de trabalho; as diretrizes; a mitigação de riscos e o desempenho mensurado.	Inexistência de um planejamento estruturado para TIC.
Q2	2.2.13	Existe uma gestão sobre os recursos de TIC?	Gestão de ativos; contratos e licenças; a banda de internet disponível e a capacitação da equipe.	Os contratos e serviços vigentes; inventário sobre hardware e software; a qualificação e treinamento dos servidores de TIC.	Verificar existência da gestão de ativos, do inventário atualizado e da capacitação da equipe.	Inexistência de uma política de gestão sobre os recursos de TIC.
Q3	2.2.13	Existe política destinada à infraestrutura de TIC?	Redes de conectividade; servidores e Data Center; Beckup e Recuperação de Desastres; Suporte Técnico e Helpdesk.	Infra adequada a demanda; servidores e data center/segurança e desempenho;beckup sob teste regular; registros das chamadas do suporte técnico.	Verificar a existência de uma política destinada a infraestrutura de TIC.	Inexistência de política de infraestrutura de TIC.
Q4	2.2.13	Existe uma política de segurança para sistemas e acessos?	Política segurança (PSI); Controle de acessos; sistemas operacionais; interoperabilidade.	Gestão de permissões e acessos; sistemas funcionam e são mantidos; integração entre sistemas/retrabalho.	Verificar política de segurança, com alcance sobre os sistemas internos e suas integrações.	Documentação que regule as permissões de acessos aos sistemas operacionais.

Avenida Florentino Ávidos, nº40 – Centro- Viana/ES- CEP 29.130-065
http://www.camaraviana.es.gov.br