# SISTEMA ELETRÔNICO DE VOTAÇÃO DA CÂMARA DOS DEPUTADOS: UM ESTUDO DE CASO À LUZ DA SEGURANÇA DA INFORMAÇÃO

Makslane Araújo Rodrigues

2012


**CENTRO UNIVERSITÁRIO DO DISTRITO FEDERAL – UDF**

**MBA em Governança em TI no Setor Público**

**MAKSLANE ARAÚJO RODRIGUES**

# SISTEMA ELETRÔNICO DE VOTAÇÃO DA CÂMARA DOS DEPUTADOS: UM ESTUDO DE CASO À LUZ DA SEGURANÇA DA INFORMAÇÃO

Brasília

2012

**MAKSLANE ARAÚJO RODRIGUES**

# SISTEMA ELETRÔNICO DE VOTAÇÃO DA CÂMARA DOS DEPUTADOS: UM ESTUDO DE CASO À LUZ DA SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado ao Curso de Pós-Graduação em Governança de TI no Setor Público, do Centro Universitário do Distrito Federal – UDF, como requisito parcial para obtenção do título de Especialista.

Orientador: Eliane Carneiro Soares, Msc.

Brasília

2012

**MAKSLANE ARAÚJO RODRIGUES**

# SISTEMA ELETRÔNICO DE VOTAÇÃO DA CÂMARA DOS DEPUTADOS: UM ESTUDO DE CASO À LUZ DA SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado ao Curso de Pós-Graduação em Governança de TI no Setor Público, do Centro Universitário do Distrito Federal – UDF, como requisito parcial para obtenção do título de Especialista.

22 de março de 2012

---

Prof. e orientador: Eliane Carneiro Soares, Msc

Universidade de Brasília

---

Examinador: Prof. Dr Wander Pereira da Silva

Universidade de Brasília

Brasília

2012

Á minha família

## RESUMO

A informação é considerada hoje um dos maiores ativos nas organizações, e, como tal, necessita ser protegida de forma adequada às necessidades do negócio. Conforme o valor da informação cresce, aumenta também o interesse em interceptar e adulterar seu conteúdo, levando a um comprometimento dos sistemas que suportam o negócio. A Câmara dos Deputados é um dos órgãos integrantes do Poder Legislativo Brasileiro e cabe a ela representar o povo, legislar sobre os assuntos de interesse nacional e fiscalizar a aplicação dos recursos públicos. Por meio de seu Sistema Eletrônico de Votação, ocorrem votações em que são tomadas decisões que afetam a vida de toda a nação. Com o uso da pesquisa documental, realizada a partir de um estudo de caso efetuado com base na análise de documentos existentes no âmbito da Coordenação do Sistema Eletrônico de Votação, este trabalho pretende comparar os controles de segurança da informação em uso e os controles recomendados para obtenção da certificação ISO 27001, para que se dê transparência ao processo de votação. Este trabalho apresenta como resultado o percentual dos controles recomendados pela norma que estão em uso, permitindo demonstrar que a segurança da informação é seriamente considerada durante o processo eletrônico de votação no Plenário Ulysses Guimarães da Câmara dos Deputados.



Palavras-chave: Sistema Eletrônico de Votação. Segurança da Informação.

**ABSTRACT**

Information is one of the most important assets for any organization today, and requires protection according to the organization's business. As the information values grows up, also increases the interest in to intercept and to tamper the information contents, leading to a compromise of the business. The legislative power is exercised by the national Congress, which is composed of the Federal Senate and the Chamber of Deputies that represents people more closely, making laws and verifying if public funds are spent according to the law. By using the Electronic Voting System of the Chamber of Deputies, it´s happens votations where decisions that affect all Brazilians take effect. By using the documental research, doing a case study by analyzing the existing documents in the Electronic Voting System Coordination, this work aims to compare the security controls in use by the Electronic Voting System Coordination and the ISO 27001 required controls, in order to bring more transparency to the voting process. The work shows, as result, the amount of the recommend controls effectively in use, demonstrating the information security is seriously considered during the electronic voting process in the Ulysses Guimarães Plenary of the Chamber of Deputies.

Key words: Electronic voting system. Information Security.

**SUMÁRIO**

# 1 INTRODUÇÃO

A Câmara dos Deputados é um dos órgãos integrantes do Poder Legislativo Brasileiro e desempenha três funções institucionais principais: representar o povo brasileiro, legislar sobre os assuntos de interesse nacional e fiscalizar a aplicação dos recursos públicos. É composta por representantes da população de todos os Estados e do Distrito Federal, o que resulta em uma organização com grande diversidade cultural e de ideias.

No Plenário Ulysses Guimarães da Câmara dos Deputados ocorrem votações de projetos de lei e emendas à Constituição entre outros. Para dar maior celeridade ao processo de votação faz-se uso do Sistema Eletrônico de Votação que faz parte da Coordenação do Sistema Eletrônico de votação do Centro de Informática. As atividades parlamentares do plenário da Câmara dos Deputados dependem fortemente do funcionamento desse sistema e sua indisponibilidade prejudicaria significativamente o andamento das sessões e aprovações de projetos.

A Coordenação do Sistema Eletrônico de Votação possui hoje uma política de segurança onde são definidas regras para liberação de novas aplicações, uso de software de terceiros, controle de acesso físico às dependências do ambiente de produção, controle de acesso lógico aos sistemas, separação de papéis, entre outros.

O Sistema Eletrônico de Votação da Câmara dos Deputados é um sistema de missão crítica tendo papel fundamental nas decisões tomadas para o futuro do País. Por ele são processadas as votações nominais e secretas que ocorrem no Plenário Ulysses Guimarães da Câmara dos Deputados e, portanto, deve ter altos índices de disponibilidade e confiabilidade.

É mister, portanto, que se garanta a transparência, correção e sigilo do processo de votação, para que seja assegurada à nação o seu direito à representatividade, de forma que o voto escolhido por seu representante seja sempre o voto efetivamente totalizado.

Assim é desejável que o Sistema Eletrônico de Votação seja certificado em segurança da informação por órgão independente da Câmara dos Deputados, garantindo que o sistema pode ser auditado, e segue normas conhecidas de segurança, conforme exigido pelas boas práticas em governança de tecnologia da informação.

A Coordenação do Sistema Eletrônico de Votação conduz sistematicamente uma grande quantidade de testes em cada novo software desenvolvido ou modificado. Quando realiza mudanças em seus sistemas mais críticos, convida outras áreas da Câmara dos Deputados para que realizem testes e homologuem a mudança, para que atestem o correto funcionamento do sistema. Além disso, mantém um rígido controle de acesso ao ambiente de produção tanto físico quanto lógico. Não há, no entanto, entidades externas à Câmara dos Deputados que conheçam a política de segurança e demais processos em uso. Assim, a percepção por parte do povo brasileiro de que o sistema de votação usado é ou não seguro está embasada na visão que se tem da instituição e não na realidade atual.

Qual será então o nível de aderência do Sistema Eletrônico de Votação às normas de segurança da informação? Dada a relevância do trabalho realizado na Câmara dos Deputados, este trabalho propõe-se verificar a aderência do Sistema Eletrônico de Votação às normas de segurança da informação, em especial, NBR ISO/IEC 27001:2005 - Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação - requisitos.

## 1.1 OBJETIVOS

### 1.1.1 Objetivos Gerais

Comparar os controles de segurança da informação aplicados pela Coordenação do Sistema Eletrônico de Votação com os controles exigidos para a obtenção da certificação ISO 27001 como forma de proporcionar transparência ao funcionamento do processo de votação da Câmara dos Deputados, assim como, estabelecer um critério de avaliação como forma de analisar as práticas de segurança da informação aplicadas ao órgão.

### 1.1.2 Objetivos Específicos

Dado o objetivo geral supracitado, pretende-se determinar se a Coordenação do Sistema Eletrônico de Votação, com relação ao Sistema Eletrônico de Votação:

- Identifica e gerencia os riscos aos ativos críticos de informação;
- Avalia e reavalia continuamente os riscos, de forma proativa e sistemática;

- Implementa controles de uma forma proporcional aos riscos;
- Detém e gerencia sistematicamente as brechas de segurança;
- Audita de forma independente o Sistema de Gestão de Segurança da Informação (SGSI) com respeito à conformidade e eficácia.

## 1.2 DELIMITAÇÃO DO ESTUDO

O órgão responsável pelos serviços de informática da Câmara dos Deputados é Centro de Informática (Cenin) posicionado na estrutura da Casa conforme mostrado na Figura 1. O Cenin é dividido em coordenações e, entre elas, está a Coordenação do Sistema Eletrônico de Votação, responsável por atender à Secretaria Geral da Mesa no que diz respeito a serviços de plenário.

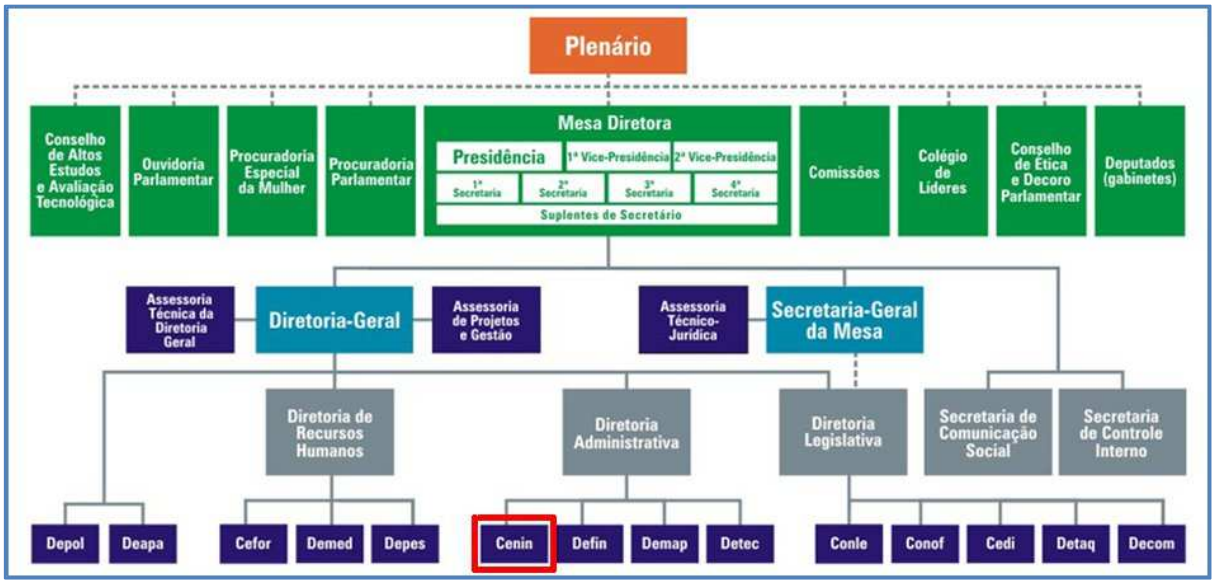


Figura 1 - Organograma da Câmara dos Deputados

A Coordenação do Sistema Eletrônico de Votação é dividida fisicamente em duas áreas principais: a área de operação e a área onde ficam os ambientes de desenvolvimento, laboratório e suporte à infraestrutura. Cada área está localizada em um prédio diferente.

Na área de operação está localizado o ambiente de produção com todos os ativos físicos e lógicos necessários ao funcionamento do Sistema Eletrônico de Votação, foco deste estudo, interligados por uma rede fisicamente isolada da rede coorporativa da Câmara dos Deputados.

# 2 REFERENCIAL TEÓRICO

Um dos maiores ativos nas organizações hoje é a informação, e, como ativo, necessita ser protegida de forma adequada às necessidades do negócio (NBR ISO/IEC 27002, 2005). Conforme o valor desse ativo cresce, com a constante demanda por tecnologia da informação, cresce também o interesse em interceptar e adulterar seu conteúdo, levando a um comprometimento dos sistemas que suportam o negócio de uma organização.

Para manter o correto funcionamento do negócio, nesse cenário de cada vez mais dependência de sistemas de informação, é necessária a criação de uma cultura da segurança que fique enraizada em todos os participantes do negócio (OECD, 2002), que devem seguir os seguintes princípios:

- Conscientização: todos os participantes devem estar cientes da importância da segurança da informação;
- Responsabilidade: todos os participantes são responsáveis pela segurança da informação;
- Reação: todos os participantes devem agir prontamente, de forma cooperativa, para responder aos incidentes relacionados à segurança da informação;
- Ética: todos os participantes devem respeitar os interesses legítimos dos outros;
- Democracia: os participantes devem assegurar que a segurança da informação deverá ser compatível com os valores democráticos;
- Avaliação de riscos: os participantes devem avaliar os riscos, para identificar ameaças e vulnerabilidades;
- Projeto e implantação seguros: os participantes devem ter a segurança como um elemento essencial dos sistemas de informação;
- Gerenciamento da segurança: os participantes devem adotar uma abordagem consistente de gerenciamento da segurança;
- Revisão constante: os participantes devem reavaliar a segurança dos sistemas de informação e fazer as modificações necessárias na política de segurança.

A segurança da informação surge com o propósito de garantir que os sistemas de informação preservem a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela organização. Para tornar efetiva a segurança da informação, as organizações devem elaborar sua política de segurança da informação, que guiará a gestão da segurança da informação, para que a organização assegure seus recursos computacionais e de informação (TRIBUNAL DE CONTAS DA UNIÃO, 2007). A política desenvolvida deverá ser capaz de entregar resultados ao negócio conforme as políticas e objetivos globais da organização (NBR ISO/IEC 27001, 2005), compondo o Sistema de Gestão de Segurança da Informação da organização.

A adoção de um Sistema de Gestão de Segurança da Informação deve ser uma decisão estratégica da organização, e sua especificação e implementação devem ser baseadas em suas necessidades. Diante disso, a norma (NBR ISO/IEC 27001, 2005) provê um modelo para estabelecer, implementar e operar, monitorar, analisar criticamente, manter e melhorar o Sistema de Gestão de Segurança da Informação da organização, prevendo uma implementação escalada conforme as necessidades da organização.

## 2.1 A FAMÍLIA ISO/IEC 27000

Em 1995 foi publicada a primeira versão da norma britânica BS7799 que era um código de práticas para gerenciamento de segurança em TI. Em 1998 uma profunda revisão foi realizada e uma nova versão foi liberada em 1999 em duas partes: a parte 1 “Código de práticas para gerenciamento de informações de segurança” e a parte 2 “Especificação para sistemas de gerenciamento de segurança de informações”. A parte 1, como um código de boas práticas, assumiu a forma de orientações e recomendações e, em 2000, se tornou a ISO/IEC 17799. Em 2002 a parte 2 foi revisada e significativamente modificada e, em 2005, foi renomeada como ISO/IEC 27001:2005 e a ISO/IEC 17799 passa a ser identificada como ISO/IEC 27002:2005, sem nenhuma outra alteração. A ISO/IEC 27001 forma a base para o Sistema de Gestão de Segurança da Informação (CALDER e WATKINS, 2008) e apresenta 133 controles de segurança.

A família de normas ISO/IEC 27000 constitui, assim, um conjunto de normas internacionais para a gestão da segurança da informação desenvolvido pela International Organization for Standardization (ISO) em Genebra e a International Electrotechnical

Commission (IEC). Estas normas fornecem um arcabouço para gerenciamento de segurança da informação. As designações corretas para a maioria destas normas incluem o prefixo ISO/IEC, e todos eles devem incluir um sufixo, que é a data da publicação. O nome da maioria destas normas, no entanto, tende a ser falado na forma abreviada. ISO/IEC 27001:2005, por exemplo, é muitas vezes denominado simplesmente ISO27001 (CALDER e WATKINS, 2008).

As normas são as seguintes:

- ISO/IEC 27000:2009 – SGSI – Visão Geral e Vocabulário
- NBR ISO/IEC 27001:2006 – SGSI – Requisitos
- NBR ISO/IEC 27002:2005 – Código de Prática para a Gestão da Segurança da Informação
- NBR ISO/IEC 27003:2011 – Guia de Implementação de um SGSI
- NBR ISO/IEC 27004:2010 – Gestão de Segurança da Informação – Medição
- NBR ISO/IEC 27005:2011 – Gestão de Riscos de Segurança da Informação
- ISO/IEC 27006:2007 – Requisitos para corpo de auditoria e certificação de SGSI
- ISO/IEC 27007 (em desenvolvimento) – Diretrizes para auditoria de SGSI

## 2.2 A CÂMARA DOS DEPUTADOS

Como órgão integrante do poder legislativo brasileiro, a Câmara dos Deputados vem buscando aprimorar seus processos internos e eficiência. Em sua declaração de missão, “Dar suporte à atividade parlamentar, com qualidade e ética, contribuindo para o seu contínuo fortalecimento, aperfeiçoamento e transparência” (CÂMARA DOS DEPUTADOS, 2009), assim como em seus objetivos estratégicos (Figura 2), a Câmara deixa claro seu compromisso com a transparência do processo legislativo.

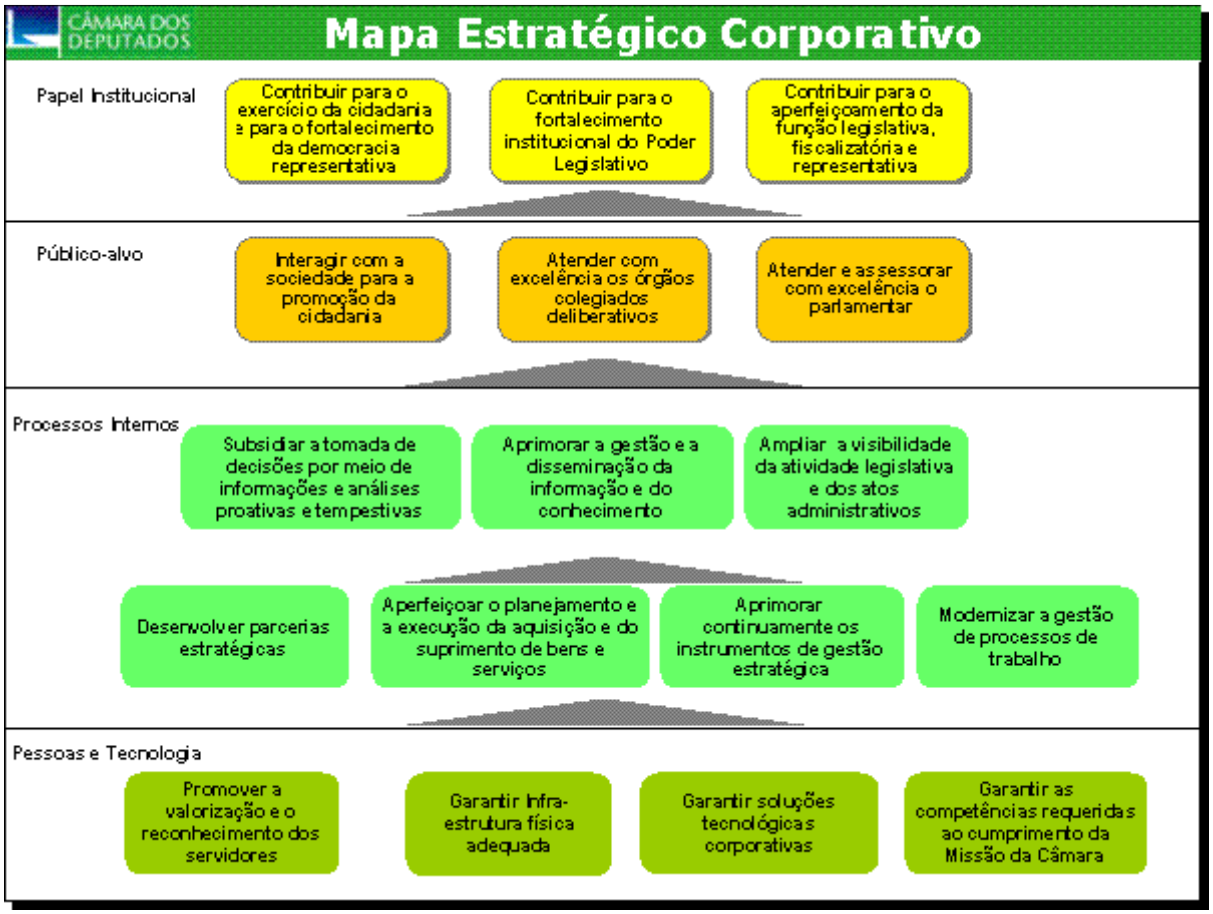


Figura 2 - Mapa Estratégico Coorporativo da Câmara dos Deputados

Dentre os objetivos relacionados no mapa estratégico, o objetivo “Contribuir para o fortalecimento institucional do Poder Legislativo” ilustra a preocupação da Casa em melhorar a percepção da sociedade com respeito à importância da atividade legislativa (CÂMARA DOS DEPUTADOS, 2009b).

Até a publicação do presente trabalho não havia ainda uma política de segurança da informação institucional consolidada e publicada. No entanto, existem normas correlatas como, por exemplo, a resolução 29 de 1993 que trata da classificação de documentos sigilosos, informatizados ou não, sua guarda e prazo de validade do sigilo, e encontra-se em desenvolvimento na Casa, desde julho de 2011, a política de segurança da informação para a Câmara dos Deputados, conduzido por equipe interdisciplinar, com o objetivo de dotar a Casa de normas que viabilizem a proteção da informação (CRUZ, 2011).

## 2.3 O SISTEMA ELETRÔNICO DE VOTAÇÃO

Em 1972 surge o primeiro documento na Câmara dos Deputados manifestando a intenção de realização de votações por meio eletrônico. Em 1987 é usado pela primeira vez o painel eletrônico durante a Assembleia Constituinte (CÂMARA DOS DEPUTADOS, 1987). A seguir, segue resumo da legislação interna publicada nos últimos 40 anos a respeito do Sistema Eletrônico de Votação:

- Resolução da Câmara dos Deputados nº 30, de 1972: prevê a abertura de concorrência pública, para o registro eletrônico de presença e votação.
- Ato da Mesa nº 29, de 06/06/1973: constitui Grupo-Tarefa para realizar estudos e apresentar proposta para a implantação e funcionamento do futuro Centro Técnico de Votação Eletrônica, a ser criado junto à Secretaria Geral da Mesa, bem como executar as operações experimentais preliminares com o equipamento já instalado no Plenário.
- Resolução da Câmara dos Deputados nº 51, de 1977: altera o regimento interno, definindo que a votação nominal ocorrerá no sistema eletrônico de votos, com os nomes dos parlamentares aparecendo nos apregoadores instalados lateralmente no plenário, e que a presença do parlamentar na sessão será verificada por meio do registro eletrônico.
- Ato da Mesa nº 86, de 17/08/1978: constitui Grupo-Tarefa para dar continuidade aos trabalhos de implantação e funcionamento do Sistema Eletrônico de Votação.
- Resolução da Câmara dos Deputados nº 54, de 1979: prevê chamada nominal dos Deputados, caso o sistema eletrônico de votação não esteja operante.
- Ato da Mesa nº 46, de 21/03/1980: prorroga a duração do Grupo-Tarefa do Sistema Eletrônico de Votação.
- Ato da Mesa nº 7, de 15/04/1983: constitui Grupo-Tarefa tendo em vista a instalação e colocação em funcionamento do Sistema Eletrônico de Votação.
- Ato da Mesa nº 22, de 02/12/1983: prorroga a duração do Grupo de Trabalho do Sistema de Votação Eletrônica.

- Ato da Mesa nº 46, de 28/11/1984: prorroga a duração do Grupo de Trabalho do Sistema de Votação Eletrônica.
- Ato da Mesa nº 82, de 04/12/1985: prorroga novamente o prazo de duração do Grupo-Tarefa para o Sistema Eletrônico de Votação.
- Ato da Mesa nº 49, de 16/12/1987: Prorroga a duração do Grupo-Tarefa do Sistema de Votação Eletrônica.
- Ato da Mesa nº 133, de 24/05/1989: determina que as terças, quartas e quintas-feiras o registro de presença será feito, pelo sistema eletrônico de votação do Plenário e, quando ocorrer pedido de verificação de quórum, o registro de frequência será apurado pela respectiva lista de chamada, que prevalecerá sobre quaisquer outras.
- Ato da Mesa nº 143, de 26/07/1989: altera o ato 133, mantendo a determinação de que as terças, quartas e quintas-feiras o registro de presença será feito, pelo sistema eletrônico de votação do Plenário.
- Ato da Mesa nº 168, de 20/09/1989: determina que a presença dos parlamentares será aferida mediante registro eletrônico nas sessões em que haja matéria para deliberação, ou pelas listas de chamada nominal, caso o sistema não esteja funcionando.
- Resolução da Câmara dos Deputados nº 17, de 1989: da nova redação ao regimento interno, onde prevê o uso do sistema eletrônico de votação, ou cédula, para votações secretas.
- Ato da Mesa nº 20, de 27/11/1991: da continuidade aos trabalhos iniciados pelo Grupo-Tarefa designado pelo Ato da Mesa n° 29, de 1973, para implantação e funcionamento do Sistema Eletrônico de Votação, até aprovação da Resolução que alterar a estrutura dos órgãos da Câmara dos Deputados.
- Resolução da Câmara dos Deputados nº 3, de 1991: altera o regimento interno, modificando o horário de realização da ordem do dia com verificação prévia do quórum por meio do sistema eletrônico.
- Ato da Mesa nº 20, de 27/11/1991: da continuidade ao grupo tarefa criado anteriormente para implantação e funcionamento do Sistema Eletrônico de Votação.

- Resolução da Câmara dos Deputados nº 22, de 1992: altera o regimento interno prevendo chamada dos Deputados para votação nominal quando o sistema eletrônico não estiver em funcionamento.
- Ato da Mesa nº 90, de 30/09/1993: determina que o uso do registro eletrônico de presença nas sessões onde haja matéria para deliberação, podendo se usar listas de chamada nominal caso o sistema não esteja funcionando.
- Ato da Mesa nº 100, de 08/02/1994: determina que o comparecimento do parlamentar será registrado eletronicamente a partir do inicio da sessão, podendo usar listas de chamada nominal, caso o sistema não esteja em funcionamento.
- Resolução da Câmara dos Deputados nº 1, de 1995: altera o regimento mantendo o uso do registro eletrônico de presença.
- Portaria nº 164, de 27/11/1996: constitui Comissão com o objetivo de implantação de novo sistema eletrônico de votação no Plenário "Ulysses Guimarães", para, em 120 dias, especificar, elaborar projeto básico, realizar audiência pública e subsidiar a administração a respeito de detalhes técnicos do novo sistema.
- Ato da Mesa nº 92, de 02/04/1998: altera a estrutura da secretaria Geral da Mesa, criando o cargo de Diretor da Coordenação do Sistema Eletrônico de Votação, a quem compete coordenar as atividades relativas ao registro eletrônico das votações e da presença dos Deputados, gerência dos respectivos bancos de dados, emissão de relatório, guarda e manutenção dos equipamentos respectivos.
- Portaria nº 100, de 19/08/1999: atribui siglas as unidades orgânicas da casa, sendo a Coordenação do Sistema Eletrônico de Votação denominada COSEV.
- Ato da Mesa nº 99, de 29/11/2001: trata da transformação de cargos, devido as crescentes demandas ao Centro de Informática, como as voltadas para a administração do Sistema Eletrônico de Votação, da Secretaria Geral da Mesa.
- Ato da Mesa nº 119, de 09/05/2002: transfere a Coordenação do Sistema Eletrônico de Votação para o Centro de Informática, devido ao fim do

contrato com a empresa fornecedora do sistema. Entre as atribuições, da coordenação está o aperfeiçoamento do controle de acesso e visibilidade de dados do módulo de votação eletrônica, desenvolvimento do sistema de controle de acesso ao ambiente de produção com identificação biométrica e desenvolvimento de novos produtos relacionados com presença parlamentar e autenticação biométrica.

- Ato da Mesa nº 49, de 25/10/2004: aprova o regimento interno do Parlamento Jovem, determinando o uso do sistema de eletrônico de votação para eleição secreta dos membros da mesa, mantendo a possibilidade do uso de cédula em caso de avaria do sistema.
- Resolução da Câmara dos Deputados nº 45, de 2006: altera o regimento interno estabelecendo a obrigatoriedade de votação pelo sistema eletrônico para escolha dos membros da Mesa Diretora e demais eleições, podendo a eleição ser realizada por cédula em caso de não funcionamento do sistema.
- Ato da Mesa nº 66, de 14/07/2010: dispõe sobre o comparecimento dos deputados que, nas sessões deliberativas, será aferida pelo registro eletrônico a partir do início da sessão, ou por lista de chamada caso o sistema não esteja funcionando.

Em junho de 2008 inicia-se, na Coordenação do Sistema Eletrônico de Votação, um esforço para a elaboração e formalização de uma política de segurança da informação que possa levar, em um momento futuro, à certificação por entidade externa do Sistema Eletrônico de Votação, o que também ajudará a manter o foco na melhoria dos processos envolvidos em segurança da informação (CALDER e WATKINS, 2008).

## 3 METODOLOGIA

A pesquisa documental procura investigar e explicar o problema a partir de fatos históricos relatados em documentos, sendo baseada em informações e dados obtidos de documentos que não receberam tratamento científico (REIS, 2008). Pesquisas elaboradas a partir de documentos são importantes, pois, apesar de não darem respostas definitivas a um problema, proporcionam uma melhor visão sobre este (RAMPAZZO, 2005).

Este é um trabalho de pesquisa documental realizada a partir de um estudo de caso efetuado com base na análise de documentos existentes no âmbito da Coordenação do Sistema Eletrônico de Votação, acerca de segurança da informação, como a política de segurança elaborada internamente, processo de mudança e liberação de novas versões de sistemas e procedimentos operacionais.

Para uma leitura objetiva da observação da aplicação dos os objetivos de controle e controles previstos pela norma NBR ISO/IEC 27001 organizou-se a informação por meio de quadros contendo os controles relacionados ao objetivo, conforme descrito no Quadro 1.

Quadro 1 – Forma de apresentação dos controles recomendados

| Controle | Selecionado | Observações |
|---|---|---|
| Recomendação da norma para assegurar segurança adequada para a proteção dos ativos de informação, proporcionando segurança às partes interessadas. | Informa se o controle está ou não em uso, ou se não se aplica ao caso estudado. | Comentários relativos ao controle, mostrando como este está em uso no Sistema Eletrônico de Votação, ou o motivo de não ter sido selecionado. |

O Quadro 1 estabelece como serão apresentados os controles previstos pela norma NBR ISO/IEC 27001, informando se cada controle foi selecionado pela Coordenação do Sistema Eletrônico de Votação, e discorrendo observações pertinentes onde necessário.

# 4 RESULTADOS

A aplicação do estudo de caso se dá no âmbito do Sistema Eletrônico de Votação localizado em ambiente fisicamente separado das demais áreas da coordenação, onde o acesso é permitido apenas a pessoas autorizadas. É nesse ambiente que é realizada a operação do Sistema Eletrônico de Votação.

Nas próximas sessões são apresentados os objetivos de controle e controles previstos pela norma NBR ISO/IEC 27001. Considera-se, ainda, como objeto deste estudo, se os controles apresentados na norma NBR ISO/IEC 27001 estão atualmente em uso na Coordenação do Sistema Eletrônico de Votação, assim como observações pertinentes acerca do tema Gestão da Segurança da Informação. A seguinte organização foi adotada: sessão da norma, objetivos de controle e, finalmente, tabela contendo os controles relacionados ao objetivo.

## 4.1 POLÍTICA DE SEGURANÇA

### 4.1.1 Política de segurança da informação

A política de segurança da informação de uma organização é uma orientação política da direção alinhada com os objetivos estratégicos do negócio, bem como leis e regulamentações pertinentes (NBR ISO/IEC 27002, 2005).

A política de segurança da informação atualmente em uso foi elaborada de forma a ser implantada de forma escalada conforme as necessidades da organização, por exemplo, uma situação simples requer uma solução de segurança simples.

Ao longo de diversas reuniões realizadas no âmbito da Coordenação do Sistema Eletrônico de Votação, com participações eventuais de representantes do controle interno da Câmara dos Deputados, buscou-se elaborar um documento que não fosse ótimo, mas sim bom. Esse documento então passaria por um processo de melhoria contínua para que se chegasse à situação ótima no futuro.

Quadro 2 – Controles relacionados ao objetivo “Política de segurança da informação”

| Controle | Selecionado | Observações |
|---|---|---|
| Documento da política de segurança da informação | Sim | O documento foi devidamente aprovado e assinado por todos os integrantes da Coordenação do Sistema Eletrônico de Votação. |
| Análise crítica da política de segurança da informação | Sim | Foram realizadas análise e adequação da política após a indicação da possibilidade de uso de desenvolvimento externo de aplicações |

## 4.2 ORGANIZANDO A SEGURANÇA DA INFORMAÇÃO

### 4.2.1 Organização interna

Esse objetivo visa dar subsídios para o gerenciamento da segurança da informação dentro da organização, e propõe que seja criada uma estrutura de gerenciamento, para controlar a implementação da segurança da informação e analisá-la criticamente (NBR ISO/IEC 27002, 2005).

No âmbito da Coordenação do Sistema Eletrônico de Votação, a segurança é coordenada pelo diretor da coordenação e toda análise, e subsequente alteração, passa pelo crivo de representantes das diversas áreas envolvidas, a fim de que se tenha um enfoque multidisciplinar (NBR ISO/IEC 27002, 2005).

Quadro 3 – Controles relacionados ao objetivo “Organização interna”

| Controle | Selecionado | Observações |
|---|---|---|
| Comprometimento da Direção com a segurança da informação | Sim | Há apoio da direção do Centro de Informática, tendo a política de segurança feita na Coordenação do Sistema Eletrônico de Votação servido de base para uma política do Centro. Está em elaboração uma política geral para a Câmara dos Deputados. |
| Coordenação da segurança da informação | Sim | Representantes de todas as áreas da Coordenação do Sistema Eletrônico de Votação participam das atividades de segurança da informação. |
| Atribuição das responsabilidades em segurança da informação | Sim | Estão definidas as responsabilidades de cada área no que diz respeito aos ativos que protege. |

| | | |
|---|---|---|
| Processo de autorização para os recursos de processamento da informação | Sim | Há procedimentos para instalação de novas máquinas. Não é permitida a conexão de dispositivos pessoais à rede coorporativa. |
| Acordos de confidencialidade | Não se aplica | As informações confidenciais dizem respeito apenas a códigos usados no processo de totalização de votos. Não é permitido o acesso a pessoas estranhas à área responsável. |
| Contato com autoridades | Sim | Há acesso às diversas áreas que suportam o sistema, por exemplo, brigada de incêndio, assessoria legislativa, e equipe de segurança de rede. |
| Contato com grupos especiais | Não | |
| Análise crítica independente de segurança da informação | Sim | A análise é feita quando da ocasião de mudanças significativas. |

### 4.2.2 Partes externas

Esse objetivo visa manter a segurança dos recursos usados no processamento da informação, e da própria informação, que são acessados ou gerenciados externamente (NBR ISO/IEC 27002, 2005).

Devido ao uso de rede isolada, as informações geradas pelo Sistema Eletrônico de Votação são disponíveis para partes externas por meio de um processo de exportação de dados.

Quadro 4– Controles relacionados ao objetivo “Partes externas”

| Controle | Selecionado | Observações |
|---|---|---|
| Identificação dos riscos relacionados com partes externas | Sim | Não há acesso lógico ou físico à rede do Sistema Eletrônico de Votação por partes externas. |
| Identificando a segurança da informação quando tratando com os clientes. | Sim | Às informações que podem ser concedidas aos clientes são exportadas para a rede coorporativa. |
| Identificando segurança da informação nos acordos com terceiros | Sim | Qualquer tipo de mudança deve ter autorização prévia. Há diretrizes para acesso de terceiros com devido registro quando o acesso é necessário. |

## 4.3 GESTÃO DE ATIVOS

### 4.3.1 Responsabilidade pelos ativos

Visa alcançar e manter um nível de proteção adequado aos ativos da organização, mantendo-se inventário atualizado, e identificando os proprietários de cada ativo (NBR ISO/IEC 27002, 2005).

Os ativos em uso no Sistema Eletrônico de Votação são mantidos em ambiente físico com acesso restrito, inclusive aos parlamentares. Diariamente cada ativo, seja lógico ou físico, é verificado para assegurar o seu perfeito funcionamento.

Quadro 5– Controles relacionados ao objetivo “Responsabilidade pelos ativos”

| Controle | Selecionado | Observações |
|---|---|---|
| Inventário dos ativos | Sim | É mantido um inventário atualizado de todos os ativos físicos e de software. São mantidas versões dos ativos de informação. |
| Proprietário dos ativos | Sim | Há definições claras dos responsáveis pela produção, manutenção e uso dos ativos. |
| Uso aceitável dos ativos | Sim | Não é permitido o acesso aos recursos de informação por meio de dispositivos não pertencentes à Coordenação do Sistema Eletrônico de Votação. |

### 4.3.2 Classificação da informação

Esse objetivo procura assegurar que cada informação seja protegida de forma adequada, conforme seu nível de sensibilidade e criticidade (NBR ISO/IEC 27002, 2005).

Existem basicamente dois tipos de informação sigilosa no âmbito do Sistema Eletrônico de Votação: a qualidade do voto dos parlamentares em votações secretas e eleições, ou durante uma votação nominal que está em andamento, e o código fonte usado para processar essas informações.

Os códigos usados são guardados criptografados e são visíveis apenas a algumas pessoas que trabalham na Coordenação do Sistema Eletrônico de Votação. Quando alguma

manutenção precisa ser efetuada, o código sendo trabalhado no computador local só pode ser gravado em uma área criptografada do disco.

A qualidade do voto é armazenada em forma criptografada até o momento da totalização da votação ou eleição, quando então, para o caso de votações secretas e eleições, é descartada.

Os equipamentos usados para eleição, que hoje são quiosques usados em outras atividades na Casa, têm o conteúdo de seu disco apagado de acordo com padrões internacionais de segurança e, após esse processo, são devolvidos às áreas de origem.

Quadro 6 Controles relacionados ao objetivo “Classificação da informação”

| Controle | Selecionado | Observações |
|---|---|---|
| Recomendações para classificação | Sim | Existem informações sigilosas que são armazenadas criptografadas, sigilosas por determinado período e então se tornam públicas, e sigilosas que são descartadas após um período determinado. |
| Rótulos e tratamento da informação | Não | As informações sigilosas são gravadas de forma criptografada, mas nenhum rótulo é adicionado. |

## 4.4 SEGURANÇA NOS RECURSOS HUMANOS

### 4.4.1 Antes da contratação

Visa assegurar todos os envolvidos, sejam funcionários, fornecedores ou terceiros, entendam suas responsabilidades a respeito da segurança da informação, reduzindo o risco de uso inadequado dos recursos, incluindo furto, roubo ou fraude (NBR ISO/IEC 27002, 2005).

Por se tratar de um órgão público, a Câmara dos Deputados tem um processo claro de contratação de pessoas, por meio de concurso público, e fornecedores de produtos e serviços, por meio de licitação. No entanto, não há alinhamento entre o processo de contratação e a segurança da informação, pois ainda não foi publicada uma política de segurança institucional.

Quadro 7– Controles relacionados ao objetivo “Antes da contratação”

| Controle | Selecionado | Observações |
|---|---|---|
| Papéis e responsabilidades | Não | Não há ainda uma política de segurança geral. Sendo assim, não há garantias de que cada contrato contenha a definição de papéis de acordo à segurança da informação. |
| Seleção | Sim | Há critérios bem definidos de seleção para servidores (concurso) e fornecedores (licitação). |
| Termos e condições de contratação | Não | Não há ainda uma política de segurança geral. Sendo assim, não há garantias de que cada contrato contemple aspectos relativos à segurança da informação. |

### 4.4.2 Durante a contratação

Visa assegurar que os funcionários, fornecedores e terceiros, estejam a par das ameaças e preocupações existentes com respeito à segurança da informação, conscientizando-os, para que apoiem a política de segurança da informação da organização (NBR ISO/IEC 27002, 2005).

Não há alinhamento entre o processo de contratação e a segurança da informação, pois ainda não foi publicada uma política de segurança institucional, mas há um processo formal de fiscalização contratual para acompanhamento da execução do contrato. No que diz respeito à Coordenação do Sistema Eletrônico de Votação, há exigência de que todos os envolvidos sigam a política de segurança estabelecida localmente.

Quadro 8– Controles relacionados ao objetivo “Durante a contratação”

| Controle | Selecionado | Observações |
|---|---|---|
| Responsabilidades da Direção | Sim | Há exigência, por parte do Centro de Informática, de que todos os envolvidos sigam a política de segurança estabelecida localmente. |
| Conscientização, educação e treinamento em segurança da informação | Sim | Por meio de controle de acesso físico e lógico, e separação de papéis, procura-se fazer com que o sistema seja seguro independentemente das pessoas envolvidas, por exemplo, com o uso de senhas divididas em que cada pessoa conhece apenas parte da senha. |

| | | |
|---|---|---|
| Processo disciplinar | Sim | Existe processo administrativo disciplinar formal em caso de não aderência às normas internas vigentes. |

### 4.4.3 Encerramento ou mudança da contratação

Visa garantir que funcionários, fornecedores e terceiros deixem a organização de forma controlada, com devolução de equipamentos usados e revogação de direitos (NBR ISO/IEC 27002, 2005).

Estão definidos procedimentos que são executados por todas as áreas pertencentes à Coordenação do Sistema Eletrônico de Votação, quando da saída de um colaborador ou mesmo quando ocorre mudança de área dentro da própria coordenação.

É mantida uma base de dados com o objetivo de conter todo o conhecimento gerado pelas pessoas que fazem parte da coordenação. Assim, quando da saída de alguém, o conhecimento é mantido na coordenação.

Quadro 9– Controles relacionados ao objetivo “Encerramento ou mudança da contratação”

| Controle | Selecionado | Observações |
|---|---|---|
| Encerramento de atividades | Sim | Estão definidas as responsabilidades de cada área, para execução dos procedimentos de saída ou movimentação de pessoas. |
| Devolução de ativos | Sim | Não há movimentação de ativos físicos ou lógicos para fora da coordenação, a não ser as informações que são públicas. |
| Retirada de direitos de acesso | Sim | São executados procedimentos para revogação de direitos de acesso lógico, mudança de senhas comuns à área afetada, mudança de senhas divididas, troca de chaves de portas, entre outros. |

4.5 SEGURANÇA FÍSICA E DO AMBIENTE

### 4.5.1 Áreas seguras

Esse objetivo tem por fim prevenir o acesso físico não autorizado, assim como danos e interferências nas instalações e informações da organização, dando um nível de proteção adequado aos riscos identificados (NBR ISO/IEC 27002, 2005).

O ambiente de produção da Coordenação do Sistema Eletrônico de Votação é uma área de acesso restrito, onde nem Parlamentares podem entrar, e não possui sequer janelas. É monitorado 24h pelo circuito fechado de Tv da Câmara dos Deputados.

Quadro 10– Controles relacionados ao objetivo “Áreas seguras”

| Controle | Selecionado | Observações |
|---|---|---|
| Perímetro de segurança física | Sim | O ambiente da operação é isolado fisicamente e gerenciado por servidores efetivos. |
| Controles de entrada física | Sim | O ambiente da operação fica permanentemente trancado, ficando suas chaves de posse de pessoal autorizado. São definidos procedimentos para acesso temporário, emergencial, e sempre com registro em livro. |
| Segurança em escritórios salas e instalações | Sim | Apenas acesso autorizado é permitido. |
| Proteção contra ameaças externas e do meio-ambiente | Sim | Cópias de segurança são armazenadas em ambiente separado protegidas em um cofre. Há proteção adequada para casos de incêndio. |
| O trabalho em áreas seguras | Sim | O trabalho é supervisionado e todo o ambiente é fisicamente trancado. |
| Acesso do público, áreas de entrega e de carregamento | Não se aplica | Não há pontos de acesso público, como áreas de entrega e carregamento. |

### 4.5.2 Segurança de equipamentos

Visa impedir o comprometimento dos ativos e interrupção do negócio, propondo que os equipamentos usados sejam protegidos contra ameaças físicas e do meio ambiente (NBR ISO/IEC 27002, 2005).

Com exceção dos equipamentos usados diretamente pelos parlamentares, e equipamentos usados na operação em Plenário, todos os demais equipamentos são mantidos em área física com acesso restrito.

Quadro 11– Controles relacionados ao objetivo “Segurança de equipamentos”

| Controle | Selecionado | Observações |
|---|---|---|
| Instalação e proteção do equipamento | Sim | Todos os servidores e equipamentos de rede são fisicamente protegidos dentro do ambiente da operação, longe de interferências eletromagnéticas externas, e em temperatura controlada. |
| Utilidades | Sim | Todos os equipamentos são ligados em um sistema próprio de proteção contra falhas elétricas (fonte de alimentação ininterrupta). Um gerador externo está disponível em caso de falhas prolongadas. |
| Segurança do cabeamento | Sim | O cabeamento é todo subterrâneo. |
| Manutenção dos equipamentos | Sim | É mantido registro de quaisquer falhas e manutenções ocorridas. Qualquer disco existente que precise sair para manutenção em seu conteúdo apagado de forma segura. |
| Segurança de equipamentos fora do local | Não se aplica | Não há uso de servidores ou equipamentos fora do ambiente de produção. O Plenário Ulysses Guimarães, onde ficam os equipamentos necessários à interação com o Parlamentar, é constantemente monitorado. |
| Reutilização e alienação seguras de equipamentos | Sim | As mídias de armazenamento são apagadas de forma segura ou destruídas, antes de descartadas, de forma a tornar as informações gravadas irrecuperáveis. |
| Remoção de propriedade | Sim | Não há retirada de ativos sem a devida autorização. |

## 4.6 GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

### 4.6.1 Procedimentos e responsabilidades operacionais

Visa garantir que a operação seja realizada de forma correta e segura, propondo que sejam definidos procedimentos e responsabilidades com respeito ao processamento das informações, e que funções sejam segregadas quando possível (NBR ISO/IEC 27002, 2005).

Um dos pilares que move a Coordenação do Sistema Eletrônico de Votação é que o Sistema Eletrônico de Votação seja seguro independentemente das pessoas. Para tornar isso uma realidade uma das medidas adotadas é o uso da segregação de papéis tanto quanto possível, de forma que operações críticas não possam ser realizadas por uma pessoa isoladamente.

Quadro 12– Controles relacionados ao objetivo “Procedimentos e responsabilidades operacionais”

| Controle | Selecionado | Observações |
|---|---|---|
| Documentação dos procedimentos de operação | Sim | Estão definidos procedimentos para execução das atividades operacionais, incluindo listas de verificação para início das atividades diárias, ligar e desligar servidores, criação de cópias de segurança, entre outros. |
| Gestão de mudanças | Sim | Todas as mudanças de hardware, software e aplicativos criados internamente são controladas, e devem ser autorizadas antes de serem implantadas em produção. Há registro de todas as mudanças efetuadas nas aplicações e procedimentos rígidos de testes. Software de terceiros são atualizados apenas quando há real necessidade, e o procedimento contempla testes de todos os sistemas envolvidos. |
| Segregação de funções | Sim | Operações críticas, como mudança de aplicações ou modificações no banco de dados, não podem ser efetuadas por uma pessoa de forma isolada. Além disso, as diversas áreas componentes da coordenação apenas tem acesso aos recursos necessários ao seu trabalho. São mantidos registros de acesso de todas as operações. |
| Separação dos ambientes de desenvolvimento, teste e de produção | Sim | Há ambientes físicos distintos para produção, homologação e testes. |

### 4.6.2 Gerenciamento de serviços terceirizados

Objetiva manter e implementar o adequado nível de segurança da informação quando da entrega de serviços por terceiros (NBR ISO/IEC 27002, 2005).

Não há uso de serviço terceirizado para processamento de informações, no que diz respeito ao Sistema Eletrônico de Votação.

Quadro 13– Controles relacionados ao objetivo “Gerenciamento de serviços terceirizados”

| Controle | Selecionado | Observações |
|---|---|---|
| Entrega de serviços | Não se aplica | |
| Monitoramento e análise crítica de serviços terceirizados | Não se aplica | |
| Gerenciamento de mudanças para serviços terceirizados | Não se aplica | |

### 4.6.3 Planejamento e aceitação dos sistemas

Esse objetivo procura minimizar as falhas nos sistemas de informação, para garantir a disponibilidade adequada de recursos, propondo estabelecimento de requisitos e testes antes da aceitação de novos sistemas, assim como projeção de requisitos futuros de capacidade (NBR ISO/IEC 27002, 2005).

Quaisquer mudanças no Sistema Eletrônico de votação só ocorrem após planejamento e garantia de que foram desenvolvidas conforme planejado. Para isso, um plano de testes detalhado é elaborado e, quando os sistemas envolvidos vão para o ambiente de homologação, ele é executado, para que seja assegurada a correção da mudança.

Quadro 14– Controles relacionados ao objetivo “Planejamento e aceitação dos sistemas”

| Controle | Selecionado | Observações |
|---|---|---|
| Gestão de capacidade | Sim | Apesar de não haver grandes variações na carga a que são submetidos os sistemas, há monitoramento do espaço requerido pela base de dados, e os ajustes são feitos com antecedência, caso sejam previstos aumentos de carga. |
| Aceitação de sistemas | Sim | Após a especificação de um novo sistema ou mudança em um sistema existente, é elaborado um plano de testes que cobre todos os ativos envolvidos na mudança. Finalizado o desenvolvimento, os sistemas afetados são exaustivamente testados antes de colocados em produção. Só após passar em todos os testes, a mudança é formalmente aceita e sua execução autorizada em produção. Há ainda procedimentos para retornar os sistemas à versão anterior, caso ocorram problemas durante a implantação. |

### 4.6.4 Proteção contra códigos maliciosos e códigos móveis

Objetiva assegurar a integridade da informação e dos programas usados em seu processamento, recomendando precauções para prevenir e detectar a introdução de códigos maliciosos e não autorizados (NBR ISO/IEC 27002, 2005).

Todo código executado no Sistema Eletrônico de Votação é verificado com respeito à introdução de códigos maliciosos. É mantido um histórico de versões de todos os sistemas desenvolvidos que pode ser utilizado para verificação de todas as mudanças introduzidas em um sistema. Essa verificação evita que bombas lógicas sejam introduzidas.

Quadro 15– Controles relacionados ao objetivo “Proteção contra códigos maliciosos e códigos móveis”

| Controle | Selecionado | Observações |
|---|---|---|
| Controle contra códigos maliciosos | Sim | Só são utilizados softwares licenciados e previamente aprovados pela coordenação. São desativadas, onde possível, as interfaces USB, CD-ROM e DVD-ROM. Quando necessário, só são usadas mídias removíveis, no ambiente de produção, de uso exclusivo da coordenação. Todo arquivo proveniente de ambiente externo é verificado com programas antivírus. |
| Controles contra códigos móveis | Não | Não há movimentação de códigos entre computadores que sejam executados automaticamente. |

### 4.6.5 Cópias de segurança

Esse objetivo visa manter a integridade e disponibilidade da informação e recursos necessários ao seu processamento, recomendando o uso de procedimentos de rotina para criação de cópias das informações usadas no negócio (NBR ISO/IEC 27002, 2005).

Todos os dados e informações relevantes armazenados digitalmente pela Coordenação do Sistema Eletrônico de Votação, incluindo os ambientes de produção homologação e desenvolvimento, são copiados para outras mídias, para que seja garantida sua recuperação, caso necessário. É considerado relevante todo dado que, se perdido ou corrompido, trará prejuízo ao negócio.

Quadro 16– Controles relacionados ao objetivo “Cópias de segurança”

| Controle | Selecionado | Observações |
|---|---|---|
| Cópias de segurança das informações | Sim | São realizadas cópias de segurança diárias de informação e aplicativos, seguindo os procedimentos definidos para esse fim. As cópias de segurança são armazenadas em ambiente separado protegidas em um cofre. |

### 4.6.6 Gerenciamento da segurança em redes

Esse objetivo tem por fim assegurar a proteção da informação em redes de computadores, bem como sua infraestrutura de suporte (NBR ISO/IEC 27002, 2005).

A fim de incrementar a segurança, a rede onde funciona o Sistema Eletrônico de Votação é fisicamente separada de quaisquer outras redes.

Quadro 17– Controles relacionados ao objetivo “Gerenciamento da segurança em redes”

| Controle | Selecionado | Observações |
|---|---|---|
| Controles de redes | Sim | São mantidos registros de acesso aos recursos ligados à rede. |
| Segurança dos serviços de rede | Não se aplica | Não há serviços de rede providos externamente. |

### 4.6.7 Manuseio de mídias

Esse objetivo recomenda a criação de procedimentos operacionais para que se previna divulgação não autorizada, modificação, remoção ou destruição dos ativos, impedindo a interrupção do negócio (NBR ISO/IEC 27002, 2005).

Na Coordenação do Sistema Eletrônico de Votação não é permitido o tráfego de qualquer informação sigilosa em mídia removível, sem o devido tratamento criptográfico. Todas as mídias removíveis usadas para cópias de segurança são guardadas em local seguro.

Quadro 18– Controles relacionados ao objetivo “Manuseio de mídias”

| Controle | Selecionado | Observações |
|---|---|---|
| Gerenciamento de mídias removíveis | Sim | Mídias usadas em cópias de segurança são guardadas em cofre. |
| Descarte de mídias | Sim | Qualquer mídia não mais utilizada tem seu conteúdo destruído para evitar recuperação, incluindo o descarte de documentos em papel. |
| Procedimentos para tratamento de informação | Sim | Apenas pessoas autorizadas têm acesso às mídias armazenadas. Não há uso de mídias removíveis para transmitir informações sigilosas. |
| Segurança da documentação dos sistemas | Sim | Especificações de sistemas e códigos gerados são acessíveis apenas a pessoas autorizadas. |

### 4.6.8 Troca de informações

Esse objetivo propõe que se estabeleçam procedimentos e normas formais, para que se proteja a informação presente em mídias em trânsito, interna ou externamente à organização (NBR ISO/IEC 27002, 2005).

Não são trocadas informações sigilosas entre o Sistema o Sistema Eletrônico de Votação e o ambiente externo. Quaisquer informações disponibilizadas para uso externo são necessariamente públicas.

Quadro 19– Controles relacionados ao objetivo “Troca de informações”

| Controle | Selecionado | Observações |
|---|---|---|
| Políticas e procedimentos para troca de informações | Sim | Apenas informações públicas trafegam para fora do Sistema Eletrônico de Votação, e têm sua integridade checada no destino. |
| Acordos para a troca de informações | Sim | As informações trafegadas para fora do Sistema Eletrônico de Votação são definidas em acordos com a Secretaria Geral da Mesa. |
| Mídias em trânsito | Sim | |
| Mensagens eletrônicas | Sim | As mensagens trafegadas são protegidas contra modificação. |
| Sistemas de informações do negócio | Sim | Há controle de acesso lógico e físico, para garantir que apenas pessoas autorizadas acessarão os sistemas. Não há conexão com redes externas. |

### 4.6.9 Serviços de comércio eletrônico

Esse objetivo visa garantir a segurança de transações e serviços de comércio eletrônico, considerando a integridade e disponibilidade da informação publicada eletronicamente (NBR ISO/IEC 27002, 2005).

Não se aplica ao Sistema Eletrônico de Votação.

Quadro 20– Controles relacionados ao objetivo “Serviços de comércio eletrônico”

| Controle | Selecionado | Observações |
|---|---|---|
| Comércio eletrônico | Não se aplica | |
| Transações On-Line | Não se aplica | |
| Informações publicamente disponíveis | Não se aplica | |

### 4.6.10 Monitoramento

O monitoramento visa detectar atividades não autorizadas com relação ao processamento da informação, por meio do acompanhamento do registro de eventos de segurança da informação, assegurando que problemas existentes sejam identificados (NBR ISO/IEC 27002, 2005).

São gerados registros de todas as transações ocorridas no Sistema Eletrônico de Votação, incluindo registros de falhas e indisponibilidades. No entanto, não são gerados registros que comprometam o sigilo do voto.

Quadro 21– Controles relacionados ao objetivo “Monitoramento”

| Controle | Selecionado | Observações |
|---|---|---|
| Registros de auditoria | Sim | Os registros gerados identificam a data e hora da transação, assim como o local e quem a gerou, e também se a transação teve sucesso ou não. |
| Monitoramento do uso do sistema | Sim | São gerados registros de todos os acessos ao sistema. |
| Proteção das informações dos registros (logs) | Sim | Os arquivos contendo dados de auditoria antigos são arquivados mensalmente mantendo-se a proibição de acesso pelos usuários auditados ao meio de armazenamento utilizado para arquivamento. |

| | | |
|---|---|---|
| Registros (log) de Administrador e Operador | Sim | Os registros contém informação de quem fez o acesso, a hora e a máquina usada. |
| Registros (logs) de falhas | Sim | Falhas detectadas são priorizadas e corrigidas. |
| Sincronização dos relógios | Sim | Todos os equipamentos integrantes da rede do Sistema Eletrônico de Votação têm seus relógios constantemente sincronizados. |

## 4.7 CONTROLE DE ACESSOS

### 4.7.1 Requisitos de negócio para controle de acesso

Visa controlar o acesso à informação, baseado nos requisitos de segurança da informação e negócio (NBR ISO/IEC 27002, 2005).

Além do isolamento físico da rede do Sistema Eletrônico de Votação, são concedidos aos usuários apenas direitos mínimos necessários à execução de suas tarefas.

Quadro 22– Controles relacionados ao objetivo “Requisitos de negócio para controle de acesso”

| Controle | Selecionado | Observações |
|---|---|---|
| Política de controle de acesso | Sim | Há política de controle de acesso físico e lógico, incluindo política de senhas onde estão definidos procedimentos para senhas pessoais e impessoais. |

### 4.7.2 Gerenciamento de acesso do usuário

Com a recomendação da criação de procedimentos formais que cubram todo o ciclo de vida do acesso do usuário aos sistemas de informação, esse objetivo visa garantir o acesso ao usuário que está autorizado a tê-lo, e negá-lo aos demais (NBR ISO/IEC 27002, 2005).

Com base na política de segurança criada, foram definidos procedimentos para concessão e revogação de senhas e chaves. Foi criada uma matriz de acesso, onde é feito um mapeamento entre os ativos e as diversas áreas componentes da Coordenação do Sistema

Eletrônico de Votação, para que fosse identificado o que cada área pode acessar e de que forma, por exemplo, com senha de conhecimento apenas da área ou dividida com outra área.

Quadro 23– Controles relacionados ao objetivo “Gerenciamento de acesso do usuário”

| Controle | Selecionado | Observações |
|---|---|---|
| Registro de Usuário | Sim | Há procedimentos definidos para concessão e revogação de direitos em cada área envolvida. As senhas impessoais são modificadas em um prazo pré-determinado. |
| Gerenciamento de privilégios | Sim | Sempre que for possível, as contas com privilégios especiais são contas pessoais, para a identificação do usuário. Quando isso ocorre, as contas impessoais correspondentes são bloqueadas. Procura-se, sempre que possível, criar nos sistemas rotinas que evitem o uso de acesso privilegiado por parte das pessoas. |
| Gerenciamento de senha do usuário | Sim | São definidos tipos de senha, tamanhos, procedimento de guarda e uso, perfis de executor e autorizador de atividades, entre outros aspectos. |
| Análise crítica dos direitos de acesso de usuário | Sim | Sempre que há movimentação de pessoas são executados os procedimentos para revogação ou adequação de acesso físico e lógico. |

### 4.7.3 Responsabilidades dos usuários

Esse objetivo visa prevenir o acesso não autorizado e evitar o comprometimento da informação e dos recursos usados em seu processamento, incluindo furto. Recomenda a conscientização dos usuários com relação às suas responsabilidades, como, por exemplo, o uso de senhas e segurança de equipamentos (NBR ISO/IEC 27002, 2005).

Todos os integrantes da Coordenação do Sistema Eletrônico de Votação são conscientizados das responsabilidades que têm, mas evita-se que a segurança da informação dependa de conscientização, pelo uso de uma forte divisão de papéis e restrição de acesso.

Quadro 24– Controles relacionados ao objetivo “Responsabilidades dos usuários”

| Controle | Selecionado | Observações |
|---|---|---|
| Uso de senhas | Sim | É proibido guarda de senha em papel, em dispositivos de forma desprotegida e scripts. As senhas são alteradas em prazos pré- |

| | | |
|---|---|---|
| | | determinados, e sempre que há movimentação de pessoas. |
| Equipamento de usuário sem monitoração | Sim | Os equipamentos ficam em ambiente isolado fisicamente, e possuem mecanismo de bloqueio com tela de proteção com senha. |
| Política de mesa limpa e tela protegida | Sim | Documentos impressos com informação sensíveis são destruídos logo após o uso. Cópias de segurança são guardadas em cofre. Computadores usam sistema de travamento de tela e teclado protegido por senha, após certo período de inatividade. |

### 4.7.4 Controle de acesso à rede

Visando prevenir o acesso não autorizado aos serviços disponíveis na rede, esse objetivo recomenda o controle de todo e qualquer acesso, seja ele interno ou externo (NBR ISO/IEC 27002, 2005). Não há acesso externo à rede do Sistema Eletrônico de Votação, devido ao isolamento físico desta. Acessos internos são controlados mantendo-se os direitos ao mínimo necessário para execução dos trabalhos.

Quadro 25– Controles relacionados ao objetivo “Controle de acesso à rede”

| Controle | Selecionado | Observações |
|---|---|---|
| Política de uso dos serviços de rede | Sim | Todos os usuários tem acesso apenas aos recursos necessários ao seu trabalho. |
| Autenticação para conexão externa do usuário | Não se aplica | Não é possível fazer acesso remoto. |
| Identificação de equipamento em redes | Não | Está prevista a implementação futura de controle de acesso para cada hardware conectado. |
| Proteção e configuração de portas de diagnostico remotas | Sim | Serviços e recursos não utilizados são desabilitados. |
| Segregação de redes | Sim | A rede de produção é separada fisicamente de todas as outras redes da Casa. |
| Controle de conexão de rede | Não se aplica | Não é possível fazer acesso remoto. Não há compartilhamento de redes. |
| Controle de roteamento de redes | Não se aplica | Não há roteamento entre redes. |

### 4.7.5 Controle de acesso ao sistema operacional

Objetivando restringir os acessos não autorizados aos sistemas operacionais em uso pela organização, é recomendado o controle de acesso com o uso de autenticação e registro de todas as tentativas de acesso, entre outros (NBR ISO/IEC 27002, 2005).

Estão definidas diretrizes para o controle de acesso lógico aos recursos computacionais ligados à rede do Sistema Eletrônico de Votação. Elas contemplam o controle de acesso à rede, aos sistemas operacionais, aos aplicativos e o gerenciamento de acesso dos usuários.

Quadro 26– Controles relacionados ao objetivo “Controle de acesso ao sistema operacional”

| Controle | Selecionado | Observações |
|---|---|---|
| Procedimentos seguros de entrada no sistema (log-on) | Sim | É requisitado usuário e senha quando do acesso ao sistema operacional. As tentativas de acesso são registradas. |
| Identificação e autenticação de usuário | Sim | Todos os usuários só têm acesso ao sistema após a entrada de identificador de usuário único e senha. Existem contas impessoais vinculadas a um grupo ou perfil de usuários, serviço, sistema ou outro recurso. Têm o objetivo de permitir o acesso a um recurso quando não há a necessidade de identificar a pessoa que está acessando um dado recurso. |
| Sistema de gerenciamento de senha | Sim | Há restrições quanto ao tamanho mínimo das senhas. As senhas não aparecem na tela. |
| Uso de utilitários de sistema | Sim | Não é permitido o uso de programas não autorizados. |
| Desconexão de terminal por inatividade | Sim | São ativadas telas de proteção com senha após um período de inatividade. |
| Limitação de horário de conexão | Não se aplica | Devido à natureza do processo legislativo (CÂMARA DOS DEPUTADOS, 2011), não é possível restringir o horário para uso dos recursos computacionais. |

### 4.7.6 Controle de acesso à aplicação e informação

Com o propósito de prevenir o acesso não autorizado à informação, recomenda-se o uso de recursos que restrinjam o acesso lógico aos sistemas de informação, por exemplo, restringindo as funcionalidades acessíveis nas aplicações de acordo com a política de acesso definida (NBR ISO/IEC 27002, 2005).

Além dos controles de acesso em nível de sistema operacional, cada aplicação com acesso à rede do Sistema Eletrônico de Votação tem seu próprio controle de acesso, para garantir que só usuários autorizados possam acessar as aplicações. Ainda, as aplicações mais sensíveis têm um controle interno de perfil, possibilitando que o usuário corrente use apenas as funcionalidades a que tem direito.

Quadro 27– Controles relacionados ao objetivo “Controle de acesso à aplicação e informação”

| Controle | Selecionado | Observações |
|---|---|---|
| Restrição de acesso à informação | Sim | É necessário o uso de identificação e senha para acessar as funcionalidades das aplicações. |
| Isolamento de sistemas sensíveis | Sim | As aplicações mais críticas rodam em sistemas dedicados, com o hardware protegido fisicamente. |

### 4.7.7 Computação móvel e trabalho remoto

Esse objetivo visa garantir a segurança da informação ao serem utilizados recursos de computação móvel e trabalho remoto, recomendando que se definam mecanismos de proteção de acordo com o risco identificado (NBR ISO/IEC 27002, 2005).

Computadores de uso privativo da Coordenação do Sistema Eletrônico de Votação podem ser usados como terminais de votação, caso atualmente em uso para acessibilidade, estritamente durante as sessões ocorridas no Plenário Ulysses Guimarães, e são ligados à rede por cabo.

Quadro 28– Controles relacionados ao objetivo “Computação móvel e trabalho remoto”

| Controle | Selecionado | Observações |
|---|---|---|
| Computação e comunicação móvel | Sim | É usada criptografia na comunicação entre o computador móvel usado como posto de votação, e esse fica fisicamente preso no plenário. Ao término das sessões plenárias o computador é recolhido e o cabo usado desconectado da rede. |
| Trabalho remoto | Não se aplica | Não é permitido execução de trabalho remoto. |

## 4.8 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

### 4.8.1 Requisitos de segurança de sistemas de informação

Esse objetivo visa assegurar que segurança faz parte dos sistemas de informação da organização, incluindo sistemas operacionais, produtos de prateleira, aplicações

desenvolvidas internamente, entre outros, recomendando que todos os requisitos de segurança sejam levantados na fase de definição de requisitos de um projeto (NBR ISO/IEC 27002, 2005).

Todo sistema desenvolvido para o Sistema Eletrônico de Votação deve ter um rigoroso registro de ações, para auditoria futura. Qualquer sistema desenvolvido deve passar por rigoroso processo de testes, antes de ser liberado para o ambiente de produção.

Quadro 29– Controles relacionados ao objetivo “Requisitos de segurança de sistemas de informação”

| Controle | Selecionado | Observações |
|---|---|---|
| Análise e especificação dos requisitos de segurança | Sim | São especificados requisitos para auditoria e controle de acesso. Há testes formais no caso de qualquer tipo de desenvolvimento interno ou não. |

### 4.8.2 Processamento correto de aplicações

Recomenda-se que controles, como validadores de dados de entrada, saída e processamento interno, sejam colocados nas aplicações de forma a assegurar o correto processamento das informações, prevenindo a ocorrência de erros e mau uso das informações (NBR ISO/IEC 27002, 2005).

Toda aplicação que roda na rede do Sistema Eletrônico de Votação deve passar por processo de autenticação, antes que execute qualquer tarefa. Nesse processo, é verificado se a assinatura do programa executável é o mesmo que foi instalado mediante autorização.

Quadro 30– Controles relacionados ao objetivo “Processamento correto de aplicações”

| Controle | Selecionado | Observações |
|---|---|---|
| Validação dos dados de entrada | Sim | Os dados são validados pela aplicação. |
| Controle do processamento interno | Sim | Há tratamento de erros e, de acordo com a severidade, a aplicação é encerrada. É validada a assinatura do arquivo executável da aplicação, bem como de arquivos que possam ser transferidos eletronicamente. |
| Integridade de mensagens | Sim | As mensagens trafegam por canal |

| | | |
|---|---|---|
| | | criptografado. |
| Validação de dados de saída | Sim | Os dados de saída são alvo do processo de testes. Há procedimentos operacionais para verificar os dados de saída de processos que requerem esse comportamento. |

### 4.8.3 Controle criptográfico

Com o objetivo de proteger a confidencialidade, autenticidade e integridade das informações, recomenda-se o uso de mecanismos criptográficos com o uso de gerenciamento de chaves para apoiá-los (NBR ISO/IEC 27002, 2005).

É usada criptografia para guarda temporária de registros sensíveis, tráfego de informações e autenticação de aplicações, buscando proteger o sigilo e integridade dos dados.

Quadro 31– Controles relacionados ao objetivo “Controle criptográfico”

| Controle | Selecionado | Observações |
|---|---|---|
| Política para o uso de controles criptográficos | Sim | Os controles criptográficos em uso estão definidos na política de segurança local. |
| Gerenciamento de chaves | Não | Não há política formal de gerenciamento de chaves. |

### 4.8.4 Segurança dos arquivos do sistema

Recomenda-se que sejam controlados os acessos aos arquivos de sistema e aos códigos fonte, e que se evite a exposição de dados sensíveis em ambientes de teste, de forma a garantir a segurança dos arquivos de sistema (NBR ISO/IEC 27002, 2005).

O acesso a arquivos de sistema e códigos fonte é dado apenas a quem precisa do acesso a estes arquivos para execução de suas tarefas.

Quadro 32– Controles relacionados ao objetivo “Segurança dos arquivos do sistema”

| Controle | Selecionado | Observações |
|---|---|---|
| Controle de software operacional | Sim | Há área definida para tratar do controle de softwares operacionais. Não é permitido o uso de códigos em desenvolvimento ou |

| | | |
|---|---|---|
| | | ferramentas de desenvolvimento no ambiente de produção. Estão documentadas as versões dos softwares em uso. Atualizações são efetuadas apenas quando há necessidade de negócio envolvida. |
| Proteção dos dados para teste de sistema | Sim | Dados sigilosos não são utilizados no ambiente de homologação, sendo modificados quando da cópia para esse ambiente. |
| Controle de acesso ao código fonte de programas | Sim | Apenas a equipe de desenvolvimento tem acesso aos códigos fonte das aplicações, ficando estes armazenados em ambiente distinto da operação. A geração do programa executável é feita sempre a partir de cópia do repositório de códigos fonte. |

### 4.8.5 Segurança em processos de desenvolvimento e de suporte

Com o objetivo de manter a segurança de sistemas aplicativos e da informação, recomenda-se o controle estrito dos ambientes de projeto e suporte, analisando-se criticamente as mudanças propostas antes de aplica-las (NBR ISO/IEC 27002, 2005).

Para garantir a correção e segurança das aplicações desenvolvidas, há um processo de desenvolvimento definido que contempla desde as fases iniciais de levantamento de requisitos até a fase de testes. Há um processo de autorização formal para realização de quaisquer mudanças nos ambientes integrantes da Coordenação do Sistema Eletrônico de Votação, sejam físicas ou lógicas.

Quadro 33– Controles relacionados ao objetivo “Segurança em processos de desenvolvimento e de suporte”

| Controle | Selecionado | Observações |
|---|---|---|
| Procedimentos para controle de mudanças | Sim | Há procedimentos formais de controle de mudança apoiados em ferramenta de controle desenvolvida internamente, que permite que se obtenham relatórios com as mudanças realizadas em determinado momento. |
| Análise crítica das aplicações após mudanças no sistema operacional | Sim | Quaisquer mudanças nos sistemas operacionais em uso são precedidas de testes que garantam que todas as aplicações envolvidas continuem funcionando sem problemas. |
| Restrições sobre mudanças em pacotes de Software | Sim | Pacotes de software são atualizados apenas quando necessário para manter o nível do |

| | | |
|---|---|---|
| | | negócio, e são precedidas de testes rigorosos. |
| Vazamento de informações | Sim | São realizados procedimentos para detecção de código troiano. Toda comunicação é mantida em ambiente controlado. |
| Desenvolvimento terceirizado de software | Sim | Apesar de não ter sido realizado desenvolvimento por terceiros, está prevista esta possibilidade. Código que venha a ser desenvolvido por terceiros passará pelo mesmo procedimento de testes já definido e executado por equipe interna. Não há acesso de terceiros ao repositório de códigos. |

### 4.8.6 Gestão de vulnerabilidades técnicas

Esse objetivo visa reduzir os riscos resultantes da exploração de vulnerabilidades conhecidas, recomendando a implantação efetiva e sistemática da gestão de vulnerabilidades técnicas, incluindo-se sistemas operacionais e quaisquer outras aplicações usadas pelo negócio (NBR ISO/IEC 27002, 2005).

Apesar de rodar em uma rede isolada fisicamente, atualizações de segurança liberadas para os softwares em uso são aplicadas ao Sistema Eletrônico de Votação logo que possível. Vulnerabilidades detectadas nas aplicações são analisadas e corrigidas seguindo o processo interno de gerenciamento de mudanças.

Quadro 34– Controles relacionados ao objetivo “Gestão de vulnerabilidades técnicas”

| Controle | Selecionado | Observações |
|---|---|---|
| 12.6.1 Controle de vulnerabilidades técnicas | Sim | São avaliados os riscos da atualização antes de sua aplicação, e se a vulnerabilidade resolvida afeta o negócio. |

## 4.9 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

### 4.9.1 Gestão de incidentes de segurança da informação

Para assegurar que eventos de segurança da informação associados a sistemas de informação sejam comunicados e corrigidos a tempo, recomenda-se que se estabeleçam procedimentos formais de registro e escalonamento e que todos os envolvidos estejam conscientes a respeito da sua importância (NBR ISO/IEC 27002, 2005).

Todos os incidentes ocorridos, estejam ou não relacionados à segurança da informação, são registrados em um sistema de controle desenvolvido internamente. Caso sejam necessárias mudanças para resolver o problema que gerou o incidente, este é vinculado ao relatório de mudanças do ativo afetado, e a mudança é especificada, executada e testada.

Quadro 35– Controles relacionados ao objetivo "Gestão de incidentes de segurança da informação"

| Controle | Selecionado | Observações |
|---|---|---|
| Notificação de eventos de segurança da informação | Sim | O evento deve ser relatado no sistema de gerenciamento de incidentes, com registro de todas as informações descobertas a respeito dele, seja no registro inicial, ou em fases posteriores. |
| Notificando fragilidades de segurança da informação | Sim | Toda fragilidade encontrada deve ser notificada no sistema interno de gerenciamento de incidentes, para análise e correção. Testes de fragilidade podem ser executados no ambiente de homologação. |

### 4.9.2 Gestão de incidentes de segurança da informação e melhorias

Com o objetivo de assegurar que haja um enfoque consistente e efetivo na gestão de incidentes de segurança da informação, recomenda-se que sejam definidos responsabilidades e procedimentos, para o tratamento dos eventos de segurança da informação e fragilidades, aplicando-se um processo de melhoria contínua às respostas (NBR ISO/IEC 27002, 2005). Com o monitoramento constante de incidentes por parte das áreas envolvidas, faz-se a devida priorização, análise e definição das mudanças necessárias, para que o incidente não mais ocorra.

Quadro 36– Controles relacionados ao objetivo "Gestão de incidentes de segurança da informação e melhorias"

| Controle | Selecionado | Observações |
|---|---|---|
| Responsabilidades e procedimentos | Sim | Cada incidente é encaminhado para a área mais adequada a analisá-lo. |
| Aprendendo com os incidentes de segurança da informação | Sim | Com a base de dados de incidentes e mudanças existente, é possível consulta-la |

| | | |
|---|---|---|
| | | quando da ocorrência de novo incidente, para determinar se já houve incidente similar anteriormente e a solução dada. |
| Coleta de evidências | Não | Não estão definidos procedimentos para coleta de evidências para uso em fins judiciais. No entanto, há registros contínuos em circuito interno de televisão sob a guarda da Polícia Legislativa. |

## 4.10 GESTÃO DA CONTINUIDADE DO NEGÓCIO

### 4.10.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação

Para impedir a interrupção do negócio, protegendo os processos críticos contra efeitos de falhas, e garantindo a retomada do negócio em tempo hábil, caso tenha sido interrompido, recomenda-se a implantação de um processo de continuidade do negócio que identifique os processos críticos e contemple ações de prevenção e recuperação. (NBR ISO/IEC 27002, 2005)

Da continuidade dos serviços prestados pelo bom funcionamento do Sistema Eletrônico de Votação, dependem decisões cruciais para a nação brasileira. Leis quando, postas em votação no Plenário Ulysses Guimarães, passaram por um longo ciclo de gestação, análises por diversas áreas, debates e, finalmente, acordos políticos. O processo de votação é extremamente sensível politicamente. Uma votação não realizada por ocorrência de falhas técnicas no sistema causaria um impacto muito prejudicial para a população, provavelmente rompendo acordos feitos com denúncias de sabotagem, entre outras conjecturas. Sendo assim, o compromisso com a continuidade do negócio está profundamente enraizado entre os integrantes da Coordenação do Sistema Eletrônico de Votação.

Quadro 37– Controles relacionados ao objetivo “Aspectos da gestão da continuidade do negócio, relativos à segurança da informação”

| Controle | Selecionado | Observações |
|---|---|---|
| Incluindo segurança da informação no processo de gestão da continuidade de negocio | Sim | Há identificação de todos os ativos e definição de quais atendem aos processos críticos. O entendimento dos riscos de parada do negócio é claro. |

| | | |
|---|---|---|
| Continuidade de negócios e avaliação de risco | Sim | Há monitoramento contínuo dos ativos usados por meio de registro de eventos, e verificações sistemáticas, para assegurar que o sistema como um todo está funcionando corretamente. |
| Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação | Sim | Há redundância de ativos para que não haja paradas no negócio. Há definição dos serviços críticos e os que aceitam certa indisponibilidade. |
| Estrutura do plano de continuidade do negócio | Não | Ainda não há estrutura de planos de continuidade documentada. No entanto, cada área tem suas responsabilidades definidas para tratamento de incidentes, para recuperação e reativação de ativos. |
| Testes, manutenção e reavaliação dos planos de continuidade do negócio | Não | Ainda não há testes de planos de continuidade. |

## 4.11 CONFORMIDADE

### 4.11.1 Conformidade com requisitos legais

Para que não ocorram violações legais de qualquer natureza, bem como de quaisquer requisitos de segurança da informação, recomenda-se especialistas em requisitos legais sejam procurados pela organização (NBR ISO/IEC 27002, 2005).

A Coordenação do Sistema Eletrônico de Votação conta com o apoio de áreas da Câmara dos Deputados especializadas em legislação. Por exemplo, quando da contratação de qualquer produto ou serviço, é criado processo formal que tramita em órgãos como a Comissão Permanente de Licitação, responsável pela elaboração de editais, e a Assessoria Técnica da Diretoria Geral, responsável por verificar a conformidade com os requisitos legais.

Quadro 38– Controles relacionados ao objetivo “Conformidade com requisitos legais”

| Controle | Selecionado | Observações |
|---|---|---|
| Identificação da legislação vigente | Sim | Há legislação interna que define, por exemplo, os dados mínimos que os registros de auditoria devem conter. |
| Direitos de propriedade intelectual | Sim | Não é permitido, por exemplo, o uso de qualquer programa de computador que não esteja de acordo com a licença definida por seu criador, ou ultrapassar o número máximo de usuários do banco de dados. |
| Proteção de registros organizacionais | Sim | Cópias de segurança dos dados são mantidas |

| | | |
|---|---|---|
| | | em local protegido e há períodos de retenção definidos. |
| Proteção de dados e privacidade da informação pessoal | Sim | Dados pessoais privados, como as minúcias das impressões digitais dos parlamentares, são guardados de forma segura e não são transferidos para o ambiente de homologação. |
| Prevenção de mau uso de recursos de processamento da informação | Sim | Os ativos ligados na rede do Sistema Eletrônico de Votação só podem ser utilizados para a atividade a que foram alocados. |
| Regulamentação de controles de criptografia | Não | Não há restrições quanto ao uso de criptografia. |

### 4.11.2 Conformidade com a política de segurança, normas e conformidade técnica

Recomenda-se que a segurança dos sistemas de informação seja analisada de forma crítica a intervalos regulares, para que se garanta a conformidade destes sistemas com as normas de segurança da informação da organização (NBR ISO/IEC 27002, 2005). Cada mudança que precisa ser feita nos componentes que integram o Sistema Eletrônico de Votação é pensada e analisada criticamente no que diz respeito à segurança. E, sempre que possível, desenvolve-se as mudanças para que os sistemas permaneçam seguros, independentemente das pessoas.

Quadro 39– Controles relacionados ao objetivo “Conformidade com a política de segurança, normas e conformidade técnica”

| Controle | Selecionado | Observações |
|---|---|---|
| Conformidade com as políticas e normas de segurança da informação | Sim | São observados os procedimentos de segurança durante as atividades operacionais, e ações corretivas necessárias são registradas. |
| Verificação da conformidade técnica | Não | Não estão documentados procedimentos para testes de invasão. |

### 4.11.3 Considerações quanto à auditoria de sistemas de informação

Para maximizar a eficácia e minimizar a interferência em processos de auditoria dos sistemas de informação, recomenda-se que existam controles para proteção dos sistemas operacionais e ferramentas de auditoria, protegendo a integridade da informação e evitando o uso indevido das ferramentas (NBR ISO/IEC 27002, 2005).

Os sistemas usados na rede do Sistema Eletrônico de Votação são desenvolvidos para gerar os registros de auditoria cabíveis. As auditorias podem ser realizadas em cópias dos dados disponibilizadas em outros ambientes, que não o de produção.

Quadro 40– Controles relacionados ao objetivo “Considerações quanto à auditoria de sistemas de informação”

| Controle | Selecionado | Observações |
|---|---|---|
| Controles de auditoria de sistemas de informação | Sim | Devem ser utilizadas cópias dos dados de produção, para realização das auditorias. |
| Proteção de ferramentas de auditoria de sistemas de informação | Sim | A auditoria deve ser realizada, sempre que possível, em cópias dos dados de produção. |

## 5 DISCUSSÃO

Observa-se que os princípios recomendados pela OCDE a serem seguidos pelos participantes estão presentes no dia a dia da Coordenação do Sistema Eletrônico de Votação, sendo alguns com maior intensidade do que outros. Dos princípios elencados, talvez o mais difícil de ser efetivamente posto em prática é o que se refere à conscientização dos participantes.

Quando se implantam controles de segurança, seja na colocação de grades em uma residência, seja na exigência de autenticação com biometria, cartão inteligente e senha, para execução de determinada atividade, observa-se degradação na usabilidade do ativo que está sendo controlado. Para o usuário qualquer queda de usabilidade pode significar perda de produtividade e, quando isso ocorre, começam a aparecer resistências ao uso dos controles de segurança, e, mais grave, questionamentos com relação à sua real importância que podem levar à remoção dos controles, pois o usuário não está efetivamente convencido de sua relevância.

Para que sejam evitados problemas de consciência, procura-se, no âmbito da Coordenação do Sistema Eletrônico de Votação, fazer com que a segurança dos sistemas de informação e da informação seja eficaz independentemente das pessoas envolvidas. O suporte a essa meta vem da criação e uso de normas internas, documentos como relatórios de versão de aplicações, documentos de autorização de mudanças, planos de testes, e finalmente, controles de acesso físico e lógico com separação de papéis.

Com base no levantamento efetuado, observa-se que, dos 133 controles recomendados pela norma (NBR ISO/IEC 27001, 2005), muitos já estão em uso pela Coordenação do Sistema Eletrônico de Votação, conforme resumido pela Tabela 1.

Tabela 1 - Resumo do uso dos controles recomendados

| Uso do controle | Quantidade | Percentual |
|---|---|---|
| Selecionado | 106 | 80 |
| Não selecionado | 12 | 9 |
| Não aplicável | 15 | 11 |

Foi elaborada uma política de segurança da informação que, apesar de não contemplar todos os controles recomendados pela norma, foi criada com base nas necessidades do negócio, buscando o que seria bom e exequível, para aprimorar a segurança da informação do Sistema Eletrônico de Votação, e não o que seria ótimo, mas ficaria apenas no papel. Também, conforme recomendação da norma, a política foi feita para que fosse implantada de forma paulatina e não de forma abrupta. Após a criação da política, foram realizadas revisões de forma a melhorá-la. Hoje, a política elaborada para o Sistema eletrônico de Votação está sendo usada como base para a elaboração da política de segurança da informação do Centro de Informática.

# 6 CONCLUSÕES

Votações de extrema importância para a nação ocorrem no Plenário Ulysses Guimarães da Câmara dos Deputados. São decisões que afetam a vida de todos os brasileiros. Quando um projeto chega ao plenário para ser votado, ele passou por diversas análises em várias partes da Casa. Debates foram feitos, consultas foram realizadas. Começa então uma longa maratona que objetiva costurar os acordos políticos necessários, para que o projeto seja apresentado ao plenário. Finalmente chega o momento em que o projeto é levado à votação.

Conforme exposto e com o objetivo de não introduzir maiores atrasos no processo, faz-se uso do Sistema Eletrônico de Votação, parte integrante da Coordenação do Sistema Eletrônico de votação do Centro de Informática da Câmara dos Deputados. É um momento muito sensível onde qualquer ruído pode fazer desmoronar todo o esforço empreendido até então. Não pode haver falhas. Não pode haver enganos. Uma falha no Sistema Eletrônico de Votação nesse instante é uma punição severa para quem depende do resultado da votação. É uma punição para a nação.

Para garantir que nenhuma falha ocorra durante uma votação ou eleição, e que se assegure transparência ao processo de votação, a Coordenação do Sistema Eletrônico de Votação elaborou sua política de segurança da informação com a definição de regras para liberação de novas aplicações, uso de software de terceiros, controle de acesso físico às dependências do ambiente de produção, controle de acesso lógico aos sistemas e separação de papéis. Os documentos criados em parte colocaram no papel atitudes já consolidadas entre os integrantes da coordenação, e trouxeram muitas outras boas práticas em segurança da informação.

Os resultados apresentados neste trabalho mostram que muito foi feito na direção de se obter uma certificação ISO 27001 para o Sistema Eletrônico de Votação. Observa-se que, dos 133 controles recomendados pela norma NBR ISO 27001, estão em uso 106 controles que descreve um percentual de 80%. Dos 20% restantes, 11% foram considerados como não sendo aplicáveis na estrutura existente, ficando apenas 9% (12 controles) de fato não selecionados. Neste contexto é importante ressaltar que:

- Os controles “Gerenciamento de chaves” e “Identificação de equipamento em redes” serão implantados após a conclusão do projeto de modernização dos postos de votação a ser concluído ainda este ano;

- Os controles “Papéis e responsabilidades”, “Termos e condições de contratação” dependem da definição de uma política institucional que está em faze final de tramitação;
- Os controles “Regulamentação de controles de criptografia” e “Controles contra códigos móveis” talvez pudessem ter sido classificados como selecionados, já que não há restrições quanto ao uso de criptografia, e não há movimentação de códigos entre computadores que sejam executados automaticamente, como scripts em navegadores, por exemplo;

Ainda, dentre todos os controles não selecionados, vale considerar como prioridade para elaboração, a estrutura do plano de continuidade do negócio bem como sua reavaliação sistemática.

Com a adoção da norma, destacam-se especialmente dois benefícios compreendidos: um externo à coordenação, que é a ótima credibilidade que o Sistema Eletrônico de Votação tem perante a Casa; e um interno que é a confiança que as pessoas que trabalham diretamente com o Sistema Eletrônico de Votação têm, por estarem trabalhando em um ambiente crítico que considera fortemente as questões de segurança da informação.

Por se tratar de um sistema por meio do qual são sacramentadas decisões que afetam a todos os brasileiros, sugere-se que, com o amadurecimento devido, todas as informações não estritamente sigilosas, como códigos fontes dos sistemas e processos internos, sejam públicas, para que, cada vez mais, não haja dúvidas com relação à credibilidade do Sistema Eletrônico de Votação da Câmara dos Deputados.

# REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

CALDER, A.; WATKINS, S. **IT governance:** a manager's guide to data security and ISO 27001/ISO 27002. 4a. ed. London e Philadelphia: Kogan Page Limite, 2008.

CÂMARA DOS DEPUTADOS. Biblioteca Digital da Câmara dos Deputados, 1987. Disponivel em: <http://bd.camara.gov.br/bd/handle/bdcamara/7846>. Acesso em: 15 fev. 2012.

CÂMARA DOS DEPUTADOS. Gestão na Câmara dos Deputados, 2009. Disponivel em: <https://www2.camara.gov.br/a-camara/conheca/gestao-na-camara-dos-deputados/missao-visao-e-valores-da-camara-dos-deputados>. Acesso em: 17 fev. 2012.

CÂMARA DOS DEPUTADOS. Objetivos Estratégicos Corporativos, 2009b. Disponivel em: <https://www2.camara.gov.br/a-camara/conheca/gestao-na-camara-dos-deputados/objetivos-estrategicos-corporativos>. Acesso em: 23 fev. 2012.

CÂMARA DOS DEPUTADOS. **Regimento Interno da Câmara dos Deputados**. 8. ed. Brasília: Edições Câmara, 2011.

CRUZ, F. Projeto Política de Segurança da Informação. **Boletim da Estratégia**, Brasília, n. 22, ago. 2011.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD**: OECD Guidelines for the Security of Information: Towards a Culture of Security, 2002.

RAMPAZZO, L. **Metodologia Científica**. 3. ed. São Paulo: Edições Loyola, 2005.

REIS, L. G. **Produção de monografia - Da teoria à prática:** O método de educar pela pesquisa. 2. ed. Brasília: Senac-DF, 2008.

TRIBUNAL DE CONTAS DA UNIÃO. **Boas práticas em Segurança da Informação**. 2. ed. Brasília: Secretaria de Fiscalização de Tecnologia da Informação, 2007.