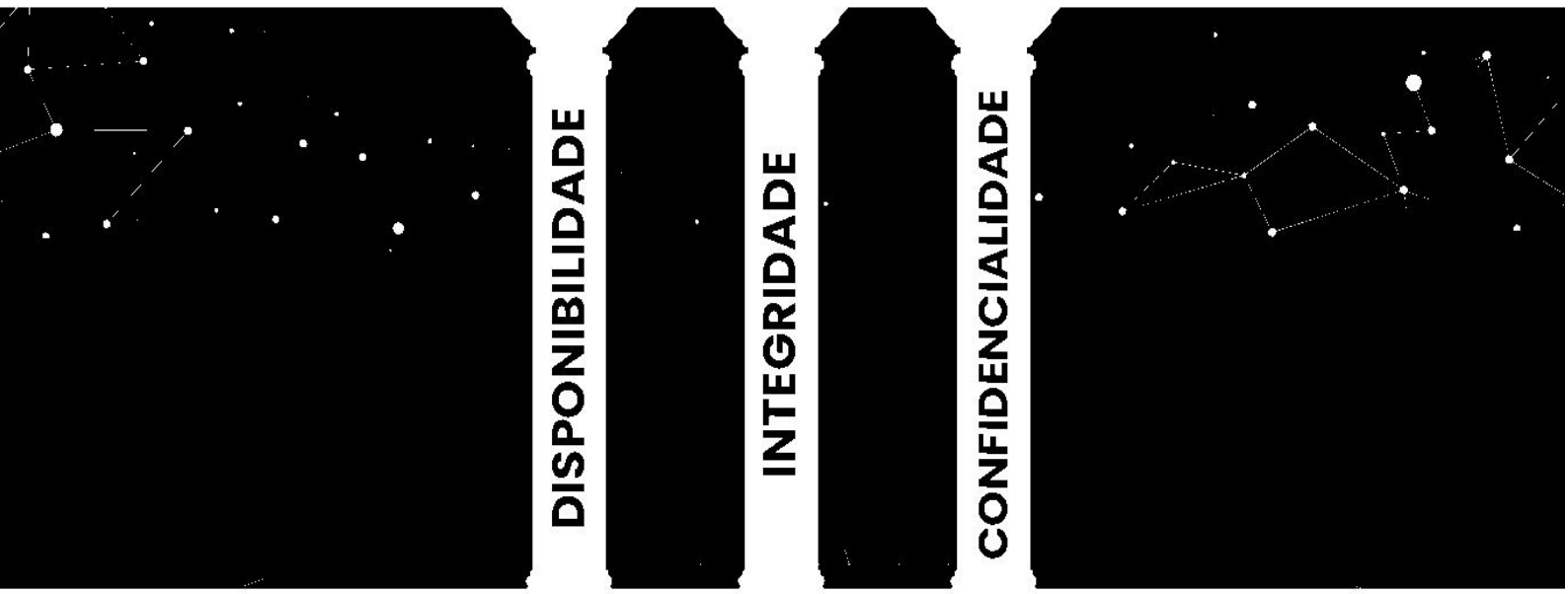
Resolução Caso (N1) - Gestão da Segurança da Informação



Aluno: Keslley Lima

Disciplina : Gestão SI

Email: keslleyls@outlook.com

Conteúdo

01 O propósito da gestão SI

A crescente digitalização dos processos empresariais, dados e informações geradas e a ampla utilização de sistemas de informação têm levado a uma maior exposição das empresas a riscos de segurança. Nesse contexto, a área de segurança da informação torna-se imprescindível para proteger os ativos de informação das organizações contra ameaças internas e externas. Além disso, a segurança da informação tem um papel fundamental na preservação da integridade, disponibilidade e confidencialidade das informações, evitando perdas financeiras, danos à reputação e outros prejuízos significativos.

Diante de todos estes desafios, nossa companhia titulada como Gênesis Tecnologia, empresa responsável pela manutenção e instalação do hardware e do software das urnas eletrônicas utilizadas nas eleições recentemente implementou algumas medidas de proteção contra as vulnerabilidades identificadas. Contudo, essas medidas se mostraram ineficientes e ineficazes. Sendo necessário, estruturação de um novo sistema de gestão da segurança da informação, no qual será descrito nas próximas páginas diferentes frentes estruturadas para esta área, que foi desenvolvida baseado em três principais pilares: 1) Disponibilidade, 2) Integridade e 3) Confidencialidade.

Para esta finalidade, é essencial que o planejamento estratégico de negócio (PEN) e o planejamento estratégico de sistemas de informação (PESI) estão intimamente relacionados e devem ser alinhados para garantir que as estratégias de TI estejam alinhadas com as estratégias de negócio da empresa. O PESI envolve a análise dos sistemas de informação existentes e a identificação de oportunidades e ameaças relacionadas à tecnologia para garantir que os investimentos em TI atendam às necessidades reais da organização e permitam explorar oportunidades de negócio e vantagens competitivas [1]. O alinhamento entre o PEN e o PESI requer a colaboração das áreas de negócio e TI, e deve ser uma atividade contínua e adaptativa.

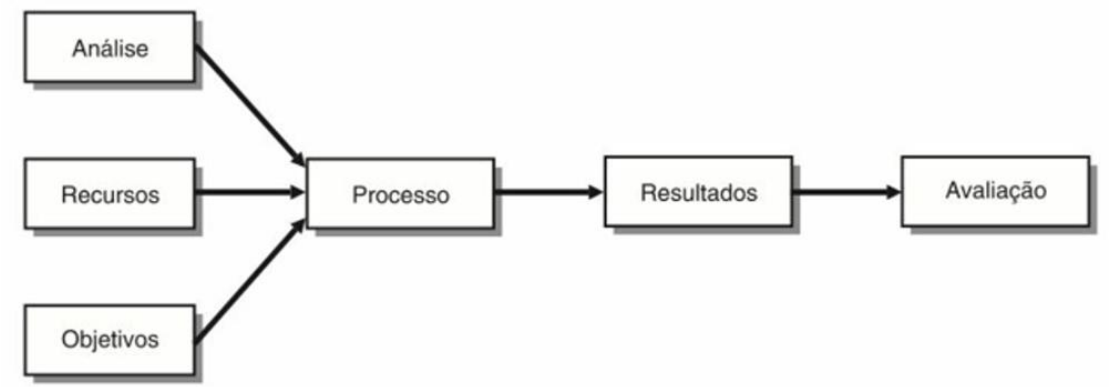


Figura 1: Modelo de PESI [2].

Conforme ilustrado na figura acima, o modelo de PESI envolve as seguintes etapas e atividades:

1. Análise do ambiente interno e externo: avaliação do ambiente de negócios da empresa

e dos sistemas de informação existentes;

2. Identificação de recursos: identificação das oportunidades e ameaças relacionadas à tecnologia e ao ambiente de negócios da empresa;
3. Definição de objetivos e metas: estabelecimento de objetivos e metas de TI alinhados com as estratégias de negócio da empresa. Bem como estruturação de processos para o estabelecimento de prioridades: determinação das prioridades para a alocação de recursos de TI;
4. Identificação de processo para definição de projetos e ações necessárias para alcançar os objetivos e metas estabelecidos. Além disso, alocação de recursos: identificação dos recursos necessários para a implementação dos projetos e ações;
5. Resultados: Implementação: execução das ações e projetos definidos no plano;
6. Avaliação: monitoramento dos resultados das ações e projetos e avaliação da eficácia do plano.

Baseado neste processo, nosso time de gestão da segurança da informação, propos e detalhou na sequencia as ações definidas e que após aprovação da gestão, serão adotadas para estruturação de um sistema de gestão da segurança da informação que atendam os 3 principais requisitos do PEN:

1. Requisitos e Políticas de Segurança;
2. Controle de acessos à informação;
3. Comprometimento com um ciclo de gestão da segurança da informação suportado por software.

Para o atendimento destes requisitos, estabelecementos frentes de ações baseados nos 3 pilares mencionados (Disponibilidade, Integridade e Confidencialidade)

Disponibilidade

Objetivo: garantir que os sistemas e recursos de TI estejam sempre disponíveis e acessíveis para os usuários autorizados, sem interrupções ou falhas, sendo essencial para a continuidade dos negócios e a satisfação dos clientes. Para garantir a disponibilidade, são necessárias medidas preventivas e corretivas, como redundância, backup, recuperação de desastres e monitoramento constante.

Integridade

Objetivo: refere à segurança e proteção das informações e dados que são processados, transmitidos ou armazenados por um sistema ou recurso de TI. Isso significa que a informação deve ser precisa, confiável e estar em sua forma original sem sofrer nenhuma alteração não autorizada.

Confidencialidade

Objetivo: proteção de informações sensíveis contra divulgação ou acesso não autorizado. É um dos principais pilares da segurança da informação, juntamente com a integridade e a disponibilidade. A garantia da confidencialidade é essencial para evitar perdas financeiras, danos à reputação e outras consequências negativas, as informações devem ser mantidas em sigilo e somente acessadas por usuários autorizados.

02 Garatia da Disponibilidade na TI

Para garantir a disponibilidade dos sistemas de TI, é necessário desenvolver um plano técnico que inclua medidas preventivas e de recuperação. Uma das ações que pode ser tomada é a implementação de um Plano de Continuidade de Negócios (PCN) por meio de um ambiente de recuperação de desastres (DR) na Oracle Cloud (OCI).

O PCN consiste em um conjunto de medidas e protocolos que têm como finalidade assegurar a continuidade das atividades de uma organização em circunstâncias de crise ou desastres, que podem ser causados por diversos fatores, como problemas de infraestrutura, ataques virtuais ou fenômenos naturais. O objetivo do PCN é mitigar os impactos dessas situações, minimizando o tempo de paralisação e os prejuízos financeiros.

A escolha deste plano foi priorizado devido criticidade da nossa operação que fornece instalação do hardware e do software das urnas eletrônicas, logo se faz necessário alta disponibilidade nos períodos de eleições, não podendo ter quebra do nosso SLA de disponibilidade, que é de 100% durante o período de votos e contagem da eleição. Outro fator considerado foi número crescente de casos no mercado brasileiro e internacional de desastres físicos e lógicos que causaram indisponibilidade de sistemas de TI, gerando impacto financeiro e operacional.

Um exemplo recente de desastre físico foi Incêndio destrói data center da OVH, maior hosting da Europa. A queda do serviço derrubou milhares de sites, incluindo alguns populares como os dos plug-ins WP Rocket e Imagify [3].

Para desenvolver um PCN eficiente, é necessário identificar as ameaças potenciais que podem afetar a organização e avaliar o impacto que elas podem causar. Com base nessas informações, são definidos os procedimentos de resposta a emergências, que incluem ações como evacuação do prédio, recuperação de sistemas, proteção de dados, entre outras. Também é importante que o PCN seja testado e atualizado regularmente para garantir que ele continue sendo eficiente diante das mudanças no ambiente de negócios e de TI.

Um exemplo de aplicação do PCN pode ser visto na biografia de Satya Nadella, CEO da Microsoft. Em 2014, poucos meses após assumir o cargo, Nadella foi confrontado com um problema de grande escala: um incêndio em um dos data centers da empresa em San Antonio, Texas. O incêndio causou a interrupção dos serviços de nuvem da Microsoft, afetando clientes como a Delta Airlines, a Xerox e a Chrysler. No entanto, graças ao PCN da empresa, foi possível restaurar os serviços em poucas horas e minimizar os impactos aos clientes afetados. Esse episódio demonstra a importância de ter um PCN eficiente e atualizado para garantir a continuidade dos negócios em situações de crise.

Já em relação aos desastres lógicos, um exemplo foi o ataque cibernético que atingiu o Tribunal Superior Eleitoral (TSE) durante as eleições municipais de 2020. O ataque, que teve início no dia da votação, causou a indisponibilidade do sistema de divulgação dos resultados por algumas

horas, mas não afetou a votação em si [4].

Com este intuito em mente, nosso time de segurança, detalha abaixo em alto nível (plano gerencial) nosta frente para construção do PCN:

1. Análise de riscos: é importante realizar uma análise de riscos para identificar as ameaças que podem afetar a disponibilidade dos sistemas de TI, como falhas de hardware, falhas de energia, desastres naturais, entre outros. Além disto, utilizar como base os incidentes e invasões recentes.
2. Definição de requisitos: com base na análise de riscos, é possível definir os requisitos necessários para garantir a disponibilidade dos sistemas de TI. No nosso caso, foi definido construção do ambiente redundante em outra estrutura (na OCI), sendo ativo-ativo e gerando alta disponibilidade dos serviços.
3. Escolha da solução: para garantir a disponibilidade dos sistemas de TI, vamos implementar um ambiente de recuperação de desastres na Oracle Cloud. Isso permite que os sistemas críticos sejam replicados em um ambiente remoto na nuvem, o que garante a continuidade do negócio em caso de desastre.
4. Implementação da solução: após a escolha da solução, é necessário implementá-la. Isso pode incluir a configuração de replicação de dados, a definição de políticas de backup e recuperação, e a realização de testes de validação.
5. Testes de validação: para garantir que a solução de recuperação de desastres funcione corretamente, é necessário realizar testes de validação. Isso pode incluir a simulação de desastres para avaliar a eficácia do plano de continuidade de negócios e a capacidade de recuperação.
6. Monitoramento contínuo: é importante monitorar continuamente o ambiente de recuperação de desastres para garantir que ele esteja sempre disponível e atualizado.

Com essas medidas, é possível garantir a disponibilidade dos sistemas de TI por meio de um ambiente de recuperação de desastres na Oracle Cloud, o que permite que a empresa mantenha seus serviços críticos em funcionamento mesmo em caso de desastre.

03 Integridade

Aliado as nossas ações detalhadas na frente de disponibilidade, temos neste plano elevação do nível de maturidade da nosso sistema de gestão de segurança da informação baseado no pilar de integridade. Para alcançarmos este objetivo, 4 frentes de trabalho foram estruturadas e propostas abaixo.

Políticas de segurança da informação: definir e comunicar claramente as políticas de segurança da informação para todos os funcionários da empresa, incluindo a importância da integridade dos dados [5]. Este documento formal estabelece diretrizes, regras e responsabilidades para garantir a segurança dos sistemas, dados e informações de uma organização. inclui objetivos, escopo, responsabilidades, classificação de informações, controles de acesso, proteção de dados, gerenciamento de incidentes, conformidade regulatória, treinamento e conscientização, e revisão e atualização. Para isto, estas políticas devem estar em conformidade com leis, para nosso plano, duas princiais: Lei Geral de Proteção de Dados (LGPD) descrita em [6] e a ISO 27001 [7].

Controle de acesso: implementar controles de acesso apropriados para limitar o acesso aos dados apenas para as pessoas autorizadas, incluindo autenticação forte, gestão de senhas e controle de privilégios. Para isto adotamos com solução de cofre de senhas ferramenta SenhaSegura [8], que consiste em um software que armazena de forma segura as senhas de acesso a diferentes sistemas e aplicativos utilizados em uma organização.
A solução permite que os usuários acessem os recursos necessários, senhas são criptografadas para garantir que não possam ser acessadas por usuários não autorizados. Além disto conta com processo de auditoria de acessos, registrando as atividades realizadas pelos usuários no cofre de senhas. A auditoria de acessos permite que os administradores da solução monitorem as atividades dos usuários e identifiquem possíveis violações de segurança.

Monitoramento de atividades: estabelecer um sistema de monitoramento de atividades de usuários, a fim de detectar possíveis anomalias ou comportamentos suspeitos. A solução adotada para monitoramento de segurança da informação utiliza Grafana [9] e Zabbix [10], no qual consiste em utilizar o Zabbix para coletar informações de segurança, como logs de firewall, logs de sistema, métricas de vulnerabilidade, entre outros. Em seguida, os dados coletados são exibidos em dashboards do Grafana, que permite visualizar as informações de forma clara e objetiva (melhor visibilidade).
Para implementar essa solução, é necessário configurar o Zabbix para coletar informações relevantes para a segurança da informação e definir gatilhos e alertas para notificar sobre eventos de segurança críticos. Além disso, é preciso configurar o Grafana para exibir esses dados de forma visualmente atraente e fácil de entender. Inicialmente pensamos em adotar seguintes métricas para nosso monitoramento: Número de tentativas de acesso não autorizadas ao sistema de TI, Taxa de tráfego de rede malicioso, volume de logs dos nosso sistemas de urnas eletronicas, quantidade de aertas de vulnerabilidades de segurança, desempenho de sistemas e aplicativos.

Backup e recuperação: implementar um plano de backup e recuperação de dados para garantir que os dados possam ser recuperados em caso de perda ou corrupção. Para recuperação do ambiente já temos nosso ambiente de DR, por isto objetivo deste backup é ser imutável, visto que está cada vez mais comum empresas sofrerem ataques ransomware, no qual os dados são corrompidos. Para isto adotamos também uma solução da Oracle [11].

Para isto se faz necessário criar um compartimento (bucket) na Oracle Cloud Storage destinado a armazenar os backups imutáveis. Configurar uma política de retenção de dados para esse compartimento, definindo a duração mínima de retenção e a periodicidade de backups. Após isto, vamos configurar a opção de versão no compartimento, para que os backups sejam armazenados em diferentes versões e possam ser recuperados em caso de falhas. Definir a opção de criptografia e replicação geográfica dos dados de backup e por último realizar testes periódicos de recuperação de dados, para garantir que a solução de backup esteja funcionando corretamente.

04 Confidencialidade

Por último, para garantir confidencialidade da segurança da informação temos ações definidas para identificar quais são as informações confidenciais da organização, como dados pessoais de clientes, informações financeiras, estratégias de negócios, propriedade intelectual, entre outros. Na sequencia, classificar as informações confidenciais: Estabelecer uma hierarquia para as informações confidenciais, classificando-as em diferentes níveis de confidencialidade. E por último, além das medidas tomadas nas outras 2 frentes que fortalecem este pilar em questão, temos ações de sensibilizar e treinar os funcionários sobre a importância da confidencialidade da informação e sobre as medidas de segurança a serem adotadas para protegê-la. Isso inclui também orientações específicas sobre como manipular as informações confidenciais em suas rotinas diárias.

No trabalho apresentado, foi descrito um plano de gestão de segurança da informação baseado em três pilares: disponibilidade, integridade e confidencialidade. Foram apresentadas diversas ações para cada um desses pilares, incluindo a implementação de backup imutável, controle de acesso através de cofre de senhas, monitoramento de segurança através de ferramentas como Grafana e Zabbix, entre outras.

Além disso, foi descrita uma política de segurança da informação, que estabelece diretrizes, regras e responsabilidades para garantir a segurança dos sistemas, dados e informações de uma organização. Essa política inclui objetivos e escopo, responsabilidades, classificação de informações, controles de acesso, proteção de dados, gerenciamento de incidentes, conformidade regulatória, treinamento e conscientização e revisão e atualização.

Por fim, concluiu-se que a implementação de um plano de gestão de segurança da informação baseado nos pilares de disponibilidade, integridade e confidencialidade é fundamental para garantir a proteção dos dados e informações de uma organização. É necessário que as ações descritas sejam acompanhadas de perto e atualizadas constantemente para garantir a eficácia da segurança da informação da empresa.

Referências

1. Sistemas de Informação: Planejamento e Alinhamento Estratégico nas Organizações, Jorge Luis Nicolas Audy, 2003.
2. KING, W.R. How effective is your IS planning? Long Range Planning, London, v. 21, n.2, p. 103-112, 1988.
3. https://thehack.com.br/incendio-em-data-center-na-franca-interrompe-servidor-e-site-de-diversas-empresas-na-europa/
4. https://www.tse.jus.br/comunicacao/noticias/2020/Novembro/tentativas-de-ataques-de-hackers-ao-sistema-do-tse-nao-afetaram-resultados-das-eleicoes-afirma-barroso
5. https://www.docusign.com.br/blog/politica-de-seguranca-da-informacao-saiba-como-e-por-que-desenvolve-la
6. https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd
7. https://www.iso.org/standard/27001
8. https://senhasegura.com/
9. https://grafana.com/
10. https://www.zabbix.com/
11. https://blogs.oracle.com/oracle-brasil/post/protegendo-seus-ativos-mais-valiosos-contra-ransomware