SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

PUC Minas Virtual

PUC Minas
Virtual

UNIDADE II – IMPLEMENTAÇÃO DA SEGURANÇA NOS DADOS

PUC Minas
Virtual

2.3 – O MUNDO CLOUD E A SEGURANÇA DOS DADOS

PUC Minas
Virtual

2.3.1 – POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

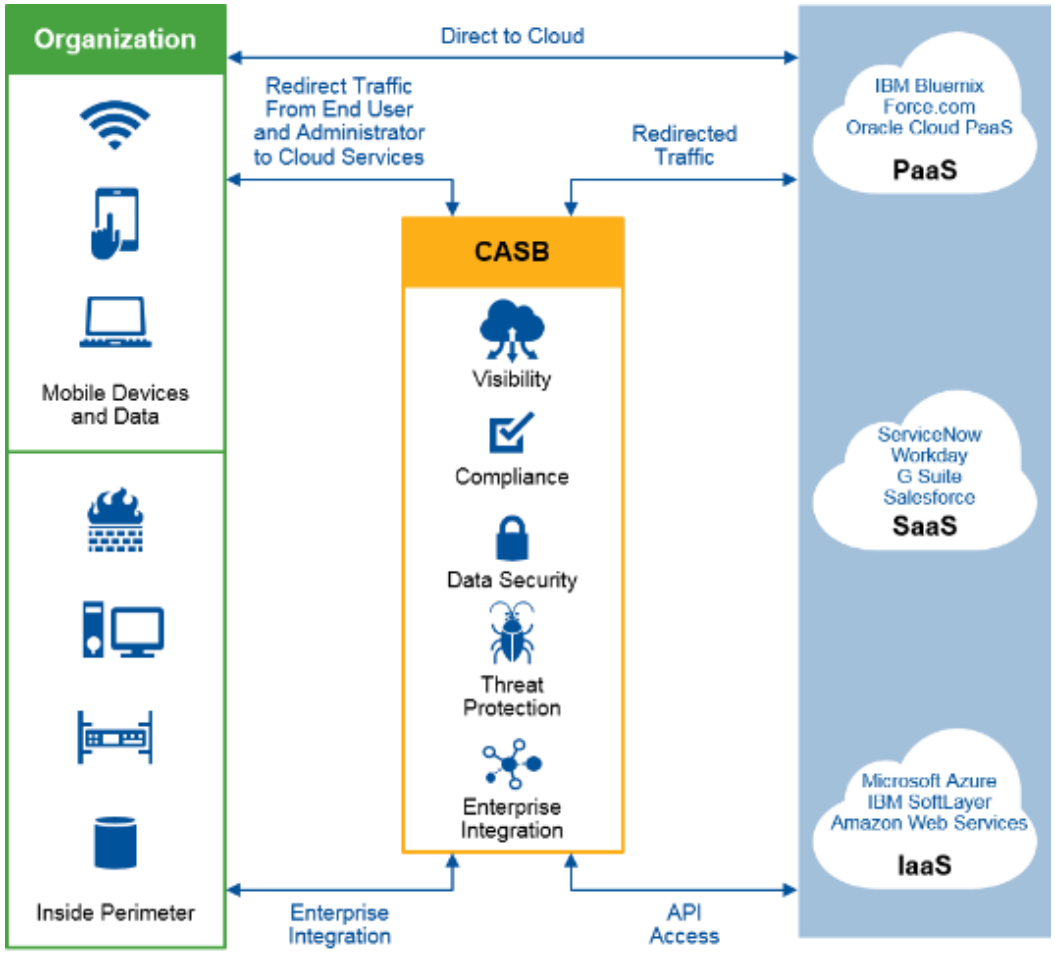
- **Trabalhar online muda todo o paradigma de segurança**.
- As organizações estão partindo para os **provimentos de serviços em nuvem.**
- As normas e regulamentações no nível de governo evoluíram para garantir **a privacidade** e principalmente garantir a **soberania** dos dados disponibilizados pelas pessoas às empresas.
- Porém, as informações confidenciais **se movem pela internet** aberta, entre aplicativos e entre dispositivos.

CASB

- De acordo como relatório do Gartner há a previsão que 60% das grandes empresas usarão um CASB para governar os serviços em nuvem até 2022.
- **Cloud Access Security Broker** (CASB): prove **segurança**, **visibilidade** e **controle** para aplicações nuvem.
- Através de componentes como estes é que conseguimos identificar **brechas de segurança**, que passaram a existir com a alta utilização de serviços de nuvem.

CASB

- É uma solução de software que fica entre o provedor de serviços em nuvem e o usuário do serviço em nuvem para impor controles de segurança.
- **O objetivo** é **monitorar a atividade** dos usuários nos aplicativos hospedados em nuvem e **tomar decisões** sobre o uso de aplicativos, acesso de usuários e etc.



FONTE: WITEC,2022

CONTROLE E SEGURANÇA

- Antes da utilização deste tipo de ferramenta é necessário traçar os planos e definir uma **política de segurança da informação**.
- É um conjunto de regras contendo os princípios e diretrizes adotados pela organização, as quais devem ser seguidas por todos os colaboradores, clientes e fornecedores com foco em diminuir a probabilidade de ocorrências de violação de algum dos princípios da segurança da informação.

CONTROLE E SEGURANÇA

- A implementação das políticas de segurança da informação possibilitam as empresas fazer uma gestão eficaz protegendo a informação considerada **crítica**, **através da seleção e implementação de controles de segurança**.
- É uma forma de manter dados estratégicos longe de vazamentos promovendo a padronização de ações, de modo que todos saibam **o que fazer e evitar**.

CONTROLE E SEGURANÇA

- A implementação das políticas de segurança da informação possibilitam as empresas fazer uma gestão eficaz protegendo a informação considerada **crítica**, **através da seleção e implementação de controles de segurança**.
- É uma forma de manter dados estratégicos longe de vazamentos promovendo a padronização de ações, de modo que todos saibam **o que fazer e evitar**.

POLITICAS DE SEGURANÇA DA INFORMAÇÃO

- Diante de todo o cenário de modernização corporativa e da movimentação das cargas de trabalho para a nuvem de forma a viabilizar a utilização dos diversos dispositivos e meios de comunicação.
- Home office, serviços móveis, contratação de SaaS são algumas destas possibilidades.
- Existe uma norma que recomenda as melhores práticas em segurança da informação que é a **ISO/IEC 27001:2013** que tem como objetivo apontar o caminho para um ambiente seguro nas organizações.

POLITICAS DE SEGURANÇA DA INFORMAÇÃO

- Para criar uma política de segurança da informação podemos seguir alguns passos que são recomendados para possuirmos adesão corporativa:
  - ✓ Definir as pessoas ou equipes envolvidas na elaboração, implantação e manutenção da política;
  - ✓ Definir a responsabilidade dos colaboradores: imposição dos limites de uso, bem como as responsabilizações em caso de má utilização dos recursos de TI;

POLITICAS DE SEGURANÇA DA INFORMAÇÃO

- ✓ Definir tecnologias de defesa contra ataques: firewall, criptografia, controles de acesso, etc.;
- ✓ Definir responsabilidades da área de TI: configuração de equipamentos, instalação de softwares, implementação de controles para cumprir os requisitos de segurança definidos;

POLITICAS DE SEGURANÇA DA INFORMAÇÃO

- ✓ Definição de normas e procedimentos sobre os seguintes aspectos: **acessos externos, internos, físicos e lógicos**; **uso da internet**; uso e **instalação de softwares; política de uso de senhas**; **backups**, etc.;
- ✓ Definir **planos de recuperação**, **contingência** ou **continuidade do negócio**

POLITICAS DE SEGURANÇA DA INFORMAÇÃO

- **CASB** ou outras ferramentas de **monitoramento** pode lhe oferecer informações de **visibilidade sobre as ocorrências no ambiente** que fomentam a construção das políticas de segurança da informação.
- A partir desta visibilidade juntamente com as recomendações apontadas nas normas principalmente na ISO/IEC 27001:2013, conseguiremos implementar as melhores práticas com foco em melhorar a segurança dos negócios.

POLITICAS DE SEGURANÇA DA INFORMAÇÃO

- Possuímos então elementos para o início da proteção corporativa que deve mesmo se iniciar com a meta das **definições das formas de trabalho**.
- Isto evita **ações negligentes** por alta de orientação e assim, caso haja um vazamento de dados é possível **responsabilizar** quem o causou.
- Outro ponto importantíssimo é a construção do **Plano de Mitigação de Riscos de Segurança** que caminha junto com a execução dos **Testes de Vulnerabilidade.**

REFERENCIAS BIBLIOGRÁFICAS

WITEC,2022. Forcepoint CASB – Visibilidade, Segurança e Controle das Aplicações Nuvem. Disponível em: <https://witec.com.br/forcepoint-casb-visibilidade-seguranca-e-controle-das-aplicacoes-nuvem/>. Acesso em: 29 Set. 2022.

IT.EAM,2022. Hashing – O Que É e Como Funciona nas Criptomoedas?, 2020. Disponível em: < https://it-eam.com/computacao-em-nuvem-no-brasil/ >. Acesso em 05 Out. 2022.

STRINGFIXER, 2022. Função Hash. Disponível em:<https://stringfixer.com/pt/Hash_sum>.Acesso em: 27 Set. 2022.


PUC Minas
Virtual