TRABALHO: SEGURANÇA DIGITAL

Atividade avaliativa deverá envolver tópicos abaixo mencionados. O conteúdo é amplo, acharão diversas informações, reportagens, dados de pesquisas, ilustrações, vídeos envolvendo o assunto, colaborando assim a enriquecer o trabalho.

• Pilares da informação

• Certificações de segurança:

• órgãos reguladores nacionais e internacionais: o CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil; o CSIRT – Computer Security Incident Response Team (Equipe de Resposta a Tratamento de Incidentes de Segurança)

• Certificado digital;

• Assinatura digital

**Pilares da segurança da informação**

**Introdução**

A importância da segurança da informação vem cada vez mais tomando relevância no cenário mundial, visto os grandes investimentos que empresas deste ramo vem recebendo. Este interesse todo se dá à crescente valorização dos dados que se torna muito valioso para diversas aplicações: seja uma informação confidencial de uma empresa, informações de usuários de uma plataforma, dados de serviços, entre muitos outros. A mera ideia de um vazamento já assusta estas companhias que veem milhões sendo desperdiçados em um mero ataque. O trabalho da segurança da informação é justamentediminuir perdas, criando barreiras com Processos, Tecnologia e Pessoas¹

**Os pilares**

A segurança da informação se divide em três pilares fundamentais em sua atuação. Os cinco pilares da segurança da informação são: integridade, confidencialidade, disponibilidade, autenticidade e legalidade.

O pilar da integridade garante a veracidade da informação, ou seja, que os dados não foram alterados sem autorização. Se houver a alteração, manipulação ou distorção de algum dado este pilar se rompe pois não há mais como saber se esta informação é verdadeira.

O pilar da confidencialidade assegura o acesso restrito a apenas pessoas autorizadas. Sendo assim, esta informação esta segura de acesso por pessoas não autorizadas que podem comprometer a veracidade da informação.

O pilar da disponibilidade afirma a disponibilidade dos dados do sistema poderão ser acessados por pessoa autorizadas à medida que estas informações são necessitadas.

O pilar da autenticidade confirma a legitimidade dos dados, uma vez confirma que não haja manipulação oi intervenções externas passando-se por um colaborador. Para assegurar essa etapa é necessário a documentação das ações dos usuários na e nos sistemas. Cabe a equipe da segurança da informação realizar mecanismos que assegurem isto.

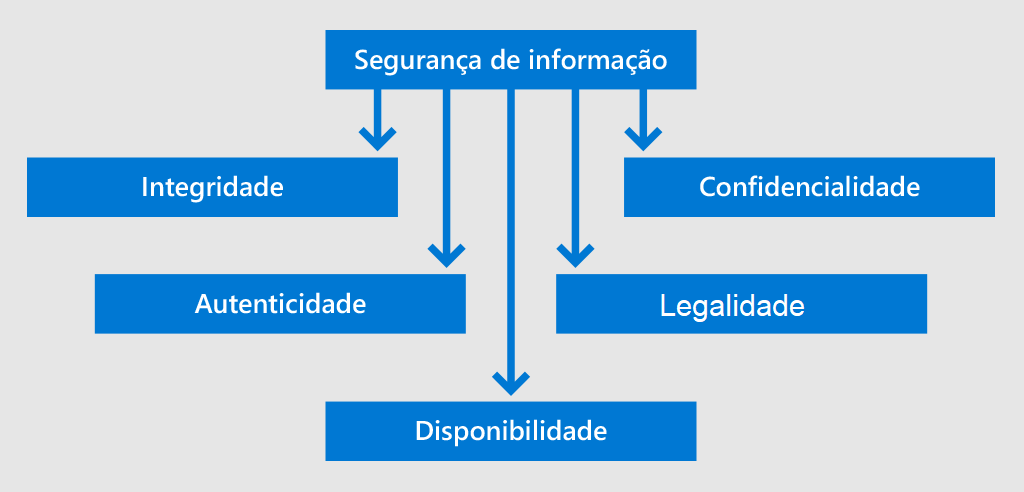
Finalmente o pilar da legalidade é necessário uma política de segurança para que os processos tangendo a informação estejam em conformidade com a lei. Evitando assim impedimentos operacionais, averiguações e auditorias de órgãos fiscalizadores.

Figura - pilares da segurança da informação

Portanto estes pilares servem para garantir que os dados não serão vazados para pessoas não autorizadas e que apenas pessoas reconhecidas e confirmadas terão acesso a ela.

**Certificações de segurança da informação**

**Introdução**

As certificações servem para valorizar o currículo do profissional que visa trabalhar com segurança da informação, atestando que ele possui experiência nos assuntos dentro do conteúdo da certificação obtida. Muito embora a obtenção de uma certificação não é um pré-requisito para a execução da atividade uma vez que muitos profissionais têm dificuldades em determinar quais certificações seriam apropriadas. ³

**Órgãos reguladores**

Há órgãos responsáveis, entre outras coisas, por regulamentar os certificados

No caso do Brasil existe o CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). Que Segundo o seu site oficial é:

um grupo de respostas a incidentes de segurança para a internet no Brasil, mantido pelo NIC.br do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil

Figura – LOGO CERT.br

Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.4

O CERT também atua no trabalho de conscientização sobre problemas de segurança no brasil analisando tendências e correlações entre eventos na internet brasileira. Este órgão também auxilia no estabelecimento de novos CSIRT no brasil.4

Os CSIRT (Computer Security Incident Response Team) nada mais são que times responsáveis por remediar incidentes relacionados a segurança em sistemas computacionais, estes times podem ser tanto de empresas terceiras ou times exclusivos para cada empresa

Figura – FIGURA CSIRI

**Certificado digital**

O certificado digital atua semelhante a uma carteira de identidade eletrônica para que pessoas ou empresas garantam a autenticidade sem que seja necessário a presença física ou de um representante.

Este instrumento é essencial para a realização de uma assinatura digital porque ela infere autenticidade a todas as transações.

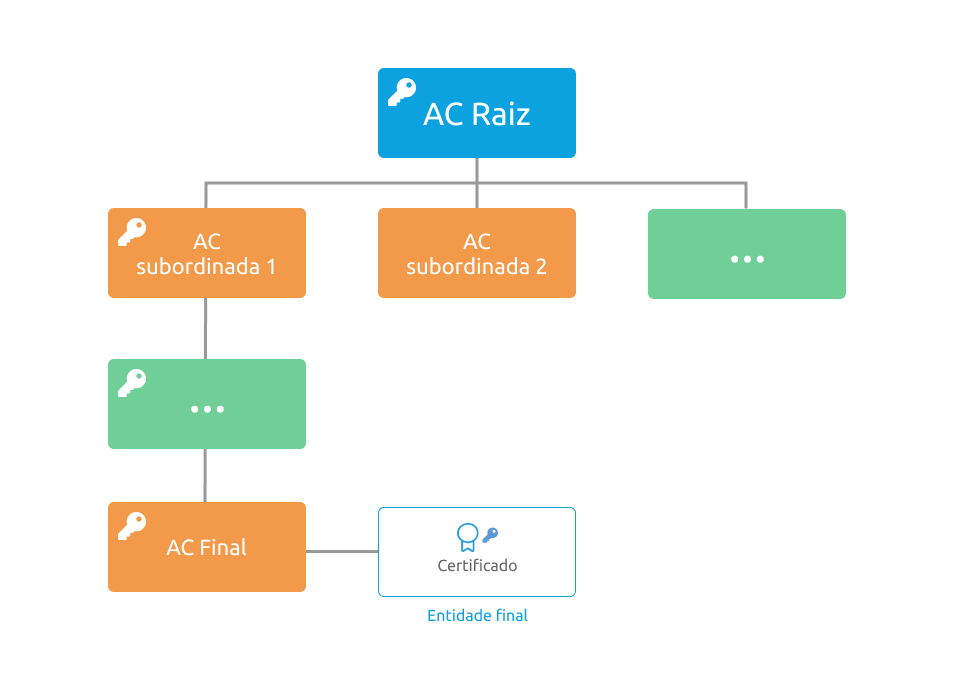
****Os certificados são emitidos por meio de autoridades certificadoras a mais importante do brasil é a Autoridade Certificadora raiz brasileira ou AC-raiz brasileira ela é o ponto máximo de confiança da infraestrutura é ela que autoriza que outras ACs secundárias funcionem. Como explicado na figura abaixo:

Figura - estrutura de certificados digitais fonte: BRyTecnologias6

**Assinatura digital**

A assinatura digital é uma técnica de criptografia que autêntica os documentos e garante a validade jurídica de um arquivo .PDF, .DOC ou outros formatos. Um certificado digital é obrigatório para fazer as assinaturas pois é ele que garante a credibilidade a todas as transações.

Desta forma as assinaturas digitais, em conjunto com os certificados, s ervem para agilizar os processos. No passo que não necessitam movimentar uma máquina analógica de autenticação com carimbos, assinaturas, impressões, deslocamento físico de arquivos. Ao enxugar o aparato acabam também barateando o custo destinados a estas áreas

Aqui vale destacar que **é impossível adulterar um documento assinado digitalmente sem invalidar a assinatura** e deixar “rastros” de que isso aconteceu. Todas as informações gravadas e criptografadas possuem traços únicos que não podem ser replicados em um contexto diferente daquele em que foram criadas.5

**Fontes:**

**[1] - ARTIGO os pilares da segurança da informação**, 19 jul. 2019. Disponível em: https://triplait.com/os-pilares-da-seguranca-da-informacao/. Acessado em: 23 set. 2020.

**[2] - ARTIGO os cinco pilares da segurança da informação**, 23 ago. 2019. Disponível: https://diferenciall.com.br/conheca-os-5-pilares-da-seguranca-da-informacao/. Acessado em: 23 set. 2020

**[3] - ARTIGO Certificações em segurança da informação**, 27 set 2017. Disponível: https://seginfo.com.br/certificacoes-em-seguranca-da-informacao/#:~:text=CISSP%20(Certified%20Information%20Systems%20Security%20Professional)&text=Um%20certificado%20CISSP%20%C3%A9%20um,a%20seguran%C3%A7a%20de%20ambientes%20corporativos. Acessado em: 23 set. 2020

**[4] – Sobre o CERT.BR,** 22 nov. 2019. Disponível em: https://www.cert.br/sobre/. Acessado em: 23 set. 2020

**[5] – ARTIGO diferença entre assinatura digital e certificado digital**. 15 out. 2019. Disponível em: https://www.bry.com.br/blog/certificado-digital-assinatura-digital/. Acessado em: 23 set. 2020

**[6] – ARTIGO O que é uma autoridade certificadora e quais são confiáveis**. 29 jun. 2018. Disponível em: https://www.bry.com.br/blog/o-que-e-uma-autoridade-certificadora/. Acessado em: 23 set. 2020