Comitê de Segurança da Informação

Daniela Barbetti

12/11/2020

Comitê de Segurança da Informação

➔ Histórico

- **2018 - Contratação da Gartner**
  - Objetivo: aconselhamento de boas práticas em assuntos de TI
  - Realizada pesquisa sobre o cenário de TI da Unicamp
  - Priorizado: Segurança da Informação

- **Orientações da Gartner:**
  - Criar um Comitê de Segurança da Informação
  - Objetivo: Implementar **estratégia** de Segurança da Informação apoiada por Política de Segurança, Normas e Procedimentos.

- **Em março de 2019** foi criado o Comitê de Segurança da Informação (CSI) através da **Portaria Interna CITIC/CGU n° 1/2019 de 09/04/2019**
  - Finalidades, Competências e Membros;
  - Representantes das áreas de negócio:
    - Administração Central (CCUEC, DAC, DGA e DGRH)
    - Área da Saúde (HC, Gastrocentro e CAISM)
    - Centros e Núcleos
    - Unidades de Ensino e Pesquisa
    - CSIRT Unicamp → apoio técnico

Comitê de Segurança da Informação

➔ Histórico

- **Membros:**

  - DGRH - **Christiane Zim Zapelini** e Leticia Meira Bisse (2019)
  - DGA - **Éderson Frasnelli Ribeiro** e Marco Antônio Pacheco Junior (1º sem 2019)
  - DAC - **Gilberto Rossi Savoini** e Cristiano Dalmaschio Ferreira
  - CCUEC - **Denis Clayton Alves Ramos** e **Marcos Aguinaldo Forquesato**
  - Unidades de Ensino e Pesquisa - **Danilo Figueiredo Rocha** (IC) e **Valcir Cabral Vargas** (IB)
  - Área de Saúde: **Daniel Cardoso da Conceição** (HC), Marcelo da Silva Primo (Gastrocentro - 2019) e Wagner Roberto Medeiros (CAISM - 2019)
  - Centros e Núcleos: Edelson Henrique Constantino (2019) e **Derivaldo Reis de Souza**

  Relatora: **Daniela Barbetti**

  Apoio Técnico: CSIRT Unicamp
  Adilson Paz da Silva, **Alexandre Berto Nogueira**, Marcelo da Silva Primo e **Vanderlei Busnardo Filho**.

Comitê de Segurança da Informação

➔ CSIRT Unicamp - Missão

- Registrar, acompanhar e responder os incidentes de segurança envolvendo os computadores da rede da Universidade;
- Apoiar os Órgãos da Universidade nas questões relacionadas à segurança dos recursos computacionais;
- Avaliar as condições de segurança dos computadores conectados da rede da Universidade;
- Orientar na identificação de comprometimento de computadores conectados na rede da Universidade;
- Orientar no reparo de danos causados por invasores;
- Disseminar informações sobre ações preventivas relativas à segurança dos recursos computacionais;
- Fomentar capacitação. Conscientização sobre Segurança da Informação;
- Dar suporte técnico ao Comitê de Segurança da Informação.

Comitê de Segurança da Informação

➔ Atividades realizadas pelo CSI em 2019

Atividades
Em março/2019: foi proposto pela Gartner, CGU e CITIC um cronograma com Plano de Ação a ser desenvolvido pelo Comitê.
Dificuldades encontradas: ○ Entendimento do escopo do trabalho a ser realizado; ○ Diferentes perfis técnicos de vários Órgãos; ○ Empenho em **estudar** os assuntos que, para a maioria, era novidade; ○ Acúmulo de responsabilidades: atividades diárias + atividades do Comitê; ○ Pensar a Universidade como um **TODO.**
Metodologia de trabalho adotada: ○ Reuniões semanais dos membros do Comitê - duração: 3 horas; ○ Estudo para elaboração das diretrizes de segurança da informação e divisão do trabalho em subgrupos com o objetivo de elaborar a Política de Segurança e Instruções Normativas.

Comitê de Segurança da Informação

➔ Atividades realizadas pelo CSI em 2019

Atividades
Divisão dos assuntos em eixos: ● Tratamento da informação (Classificação de dados e controle de acesso) ● Sistemas de informação (Desenvolvimento seguro) ● Infraestrutura computacional (Mapeamento físico e lógico das redes e gestão de hardware) ● Continuidade do negócio ● Comunicação da Política de Segurança da Informação ● Gestão operacional (gestão de logs, vulnerabilidades e incidentes)
Dentro de cada eixo proposto, os sub-grupos estudaram e definiram os processos e modelos que estão sendo utilizados para elaborar as políticas e normas. ● **Política de Segurança da Informação elaborada** ● Instruções Normativas elaboradas.

Comitê de Segurança da Informação

➔ Histórico

- **Em outubro de 2020** foi criado o Comitê de Segurança da Informação (CSI) através da **Resolução GR-102/2020, de 06/10/2020**
  - Subordinado à CITIC e de natureza permanente;
  - **Artigos 1º e 2º - Finalidades**

    1) Propor, definir e orientar a implementação da **estratégia** de Segurança da Informação apoiada por Política de Segurança, Normas e Procedimentos;

    2) Acompanhar a efetividade da implantação da estratégia de Segurança de forma a promover a **melhoria contínua**.

  - **Artigo 3º - Competências**

    I - Debater, propor e definir a Diretriz Corporativa de Segurança da Informação no âmbito da Universidade Estadual de Campinas;

    II - Definir o catálogo de processos que detalhe as práticas de Segurança da Informação;

    III - Identificar as principais iniciativas para a melhoria contínua das medidas de proteção das informações e levantar os recursos necessários;

    IV – Propor e definir alterações na Política de Segurança da Informação e em normas e procedimentos vigentes;

Comitê de Segurança da Informação

➔ Histórico

- **Artigo 3º - Competências**

  V - Propor e acompanhar estratégias, metas e ações de Segurança da Informação, bem como apresentar resultados decorrentes da implementação;
  VI - Apoiar a implantação de soluções para eliminar ou minimizar os riscos da Segurança da Informação;

  VII - Propor ações corretivas cabíveis no caso de quebra de Segurança;

  VIII - Estabelecer uma relação consistente das políticas e estratégias institucionais e da tecnologia da informação com os aspectos de segurança;

  IX – Manifestar-se em ações de segurança da informação.

- **Definição de membros por Portaria Interna CITIC sendo:**
  - 02 Representantes DGRH
  - 02 Representantes DGA
  - 01 Representante DAC
  - 03 Representantes CCUEC
  - 02 Representantes Unidades de Ensino e Pesquisa
  - 02 Representantes Área de Saúde
  - 01 Representante Centros e Núcleos
    CSIRT Unicamp → apoio técnico

Comitê de Segurança da Informação

➔ Atividades realizadas pelo CSI em 2020

Atividades
Política de Segurança revisada conforme orientações da Gartner e aprovada na reunião do CONSU de agosto de 2020 → **Por que?**
Instruções Normativas elaboradas, revisadas, aprovadas pela CITIC e aguardando publicação: → **O que?** • IN-CITIC-001/2020 - Comunicação da Política de Segurança da Informação • IN-CITIC-002/2020 - Desenvolvimento seguro de sistemas de informação • IN-CITIC-003/2020 - Mapeamento físico e lógico das redes de dados • IN-CITIC 004/2020 - Gestão de incidentes • IN-CITIC-005/2020 - Gestão de vulnerabilidades • IN-CITIC-006/2020 - Gestão de registros (logs) de auditoria
Aplicação das INs dentro de cada Órgão → **Como?**
Documentos indicando melhorias de segurança no ambiente computacional da Universidade elaborados, aprovados e encaminhados para o CCUEC: • Adoção de DNSSEC na zona unicamp.br • Adoção de RPKI nos roteadores do backbone • Adoção de IPv6 na Nuvem Unicamp • Necessidade de registro de logs das autenticações dos usuários (Autenticação Central e SiSe) • Implementar segundo fator de autenticação (2FA) nos serviços de autenticação de usuários
Finalizar a revisão das Instruções Normativas que já estão elaboradas, solicitar aprovação e publicar.

Comitê de Segurança da Informação

➔ Planejamento para 2021

Atividades
Elaborar novas Instruções Normativas
Elaborar novos documentos indicando melhorias de segurança no ambiente computacional da Universidade
Elaborar documentos de boas práticas
Acompanhar o andamento das solicitações encaminhadas pela CITIC/CSI

Comitê de Segurança da Informação

➔ O que priorizar para 2021? (Fonte: CERT.br)

Invista no básico:

→ Mantenha os sistemas atualizados

- Acompanhe os fabricantes e aplique patches, patches, patches ...
- Atualize **TODOS** os sistemas e aplicações (mesmo que sejam só internos).
- Defina regras para priorizar a aplicação de correções de segurança com severidade de maior impacto.

Urgências:

→ Múltiplos fatores de autenticação:

- Impede sucesso de ataques de força bruta de senhas (nº 1 no 1º semestre de 2020);
- Reduz impacto de comprometimento de credenciais;
- Implementar em serviços Web, *login* remoto, elementos de rede, dentre outros.

→ Adote protocolos mais modernos:

- Criptografia forte: HTTPS mandatório;
- Segurança de DNS: DNSSEC;
- Segurança em roteamento: RPKI;
- Protocolo IP: IPv6 é o atual. IPv4 é legado e já acabou. Novas redes só terão IPv6.

Sempre: **Conscientização em segurança da informação.**

“Nenhum grupo ou estrutura única conseguirá fazer sozinho a segurança ou a resposta a incidentes.” **(Fonte: CERT.br)**

Dúvidas?

Contato: csi@unicamp.br