Segurança da Informação e Proteção ao Conhecimento

Aula 08 – Gerência de Operações e Comunicações

Prof. Dalton Martins
dmartins@gmail.com

Gestão da Informação
Faculdade de Informação e Comunicação
Universidade Federal de Goiás

Gerência de operações e comunicações

objetivos

Descrever responsabilidades, selecionar e aplicar controles e procedimentos da gerência de operações e comunicações.

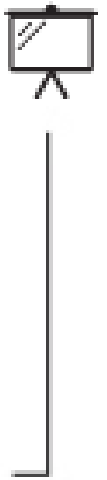
conceitos

Definição, procedimentos e responsabilidades da gerência de operações e comunicações e gerência de segurança de redes.

Objetivos

- Assegurar que as operações sejam realizadas de acordo com os requisitos de segurança.
- Gerenciar os serviços terceirizados.
- Proteger contra códigos maliciosos.
- Prover cópias de segurança.
- Gerenciar a segurança das redes.
- Controlar o manuseio de mídias.
- Controlar a transferência de informações e softwares.
- Garantir o monitoramento global de operações e comunicações.

Procedimentos e responsabilidades operacionais

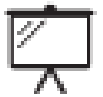


- Documentar procedimentos operacionais.
- Controlar mudanças operacionais.
- Estabelecer procedimentos para o gerenciamento de incidentes.
- Segregar responsabilidades.
- Separar facilidades de desenvolvimento, testes e operação.

Exemplo: Tratando responsabilidades operacionais:

- "Os usuários que operam os sistemas de TI da organização devem assinar um termo de responsabilidade antes de obter acesso a eles. A assinatura do termo representa que o usuário entende e concorda com as políticas e normas de segurança e tem conhecimento a respeito da legislação vigente e aplicável aos casos de não cumprimento."
- No exemplo, é apresentada uma regra que faz referência a um termo de responsabilidade que determina, por sua vez, todas as responsabilidades do usuário quanto à operação adequada dos sistemas de TI da organização, conforme as políticas e normas da segurança da informação vigentes e, ainda, determina a aplicação de legislação em caso de não cumprimento.

Proteção contra softwares maliciosos



São várias as possibilidades, como vírus, cavalos de troia, bombas lógicas etc. A proteção deve se basear na conscientização de segurança, controle de acesso e mudanças. Algumas práticas:

- Controle da conformidade com licenças.
- Controle de riscos associados a arquivos e softwares obtidos via rede.
- Instalação e atualização regular de antivírus.

Regras para a proteção contra códigos maliciosos:

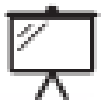
- Não abrir arquivos ou executar programas anexados a e-mails sem antes verificá-los com um programa de detecção de vírus.
- Não utilizar o formato executável em arquivos compactados, já que tal formato facilita a propagação de vírus.
- Utilizar programas de computadores licenciados para uso por parte da organização, de acordo com as disposições específicas estabelecidas em contrato.

Cópias de segurança

- Medida para assegurar a integridade e a disponibilidade de ativos.
- Geração e recuperação de cópias devem ser testadas.
- Práticas recomendadas:
  - Documentar procedimentos de recuperação.
  - Definir o modo e a frequência adequados ao negócio e à segurança da informação.
  - Armazenar cópias em locais remotos.
  - Testar mídias e procedimentos de recuperação.

Política de backups

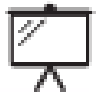
- Determinada segundo a importância dos sistemas e informações.
- Estratégias podem considerar uma combinação de métodos.
- Sistemas críticos devem manter duas cópias de segurança.
- Essencial ao plano de contingência da organização.



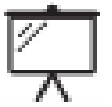
Exemplos

Regras para o tratamento de cópias de segurança:

- A cada funcionário cabe efetuar, regularmente, cópias de segurança dos seus dados.
- Manter registros das cópias de segurança geradas.
- Guardar as cópias de segurança em local seguro e distinto daquele onde se encontra a informação original.



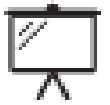
Tratamento de mídias e documentos



Deve-se usar procedimentos adequados para assegurar a segurança. Algumas práticas:

- Considerar a classificação da informação antes de sua manipulação.
- Controlar acessos.
- Descartar de modo seguro.
- Estabelecer regras para mídias em trânsito.

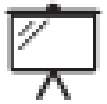
Gerência de segurança das redes



Deve-se aplicar medidas para garantir a segurança das redes. Algumas práticas:

- Segregar responsabilidades.
- Identificar os requisitos de gerenciamento de serviços de rede.
- Tratar acessos e equipamentos remotos.
- Aplicar medidas que assegurem a confidencialidade, a integridade e a disponibilidade dos recursos envolvidos.

Transferência de informações e softwares

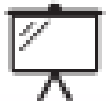


Deve-se proteger todos os recursos envolvidos com transferências internas e externas.

Algumas práticas:

- Proteção contra códigos maliciosos.
- Definir regras para o uso seguro de recursos eletrônicos.
- Estabelecer regras para transferências sem fio (wireless).
- Garantir conformidade com a legislação.
- Atribuir responsabilidades.

Monitoramento



Procedimento regular para a segurança da informação em termos de operações e comunicações.

Devem ser mantidos:

- Logs de operação.
- Logs de falhas.
- Logs de auditoria.

Exemplos de procedimentos com logs:

- "Não é permitido o acesso não autorizado ao e-mail de terceiros. As tentativas de acesso devem ser registradas em log, inclusive as originadas por administradores do sistema."
- "Deve ser possível reconstituir todas as atividades dos usuários a partir de logs. Os procedimentos usados para tal monitoramento devem considerar mecanismos de responsabilização claros e divulgados nos meios de comunicação internos da organização."

Atividade 6.1 – Segurança da informação na gerência de operações e comunicações

Você foi designado para desempenhar as funções de gerência de operações e comunicações. Abaixo são apresentadas algumas situações em que você deverá dizer o que deve ser feito e apresentar a sua justificativa:

No	Situação	Respostas/Procedimentos	Justificativa
01	Entrada de um novo funcionário na empresa, que será usuário do sistema de controle financeiro da organização.		
02	O banco de dados foi corrompido e não havia backup.		
03	Uma máquina servidora apresentou problemas e necessita ser encaminhada para manutenção fora do ambiente do datacenter.		
04	A Gerência de Recursos Humanos informou que adquiriu um novo sistema e determinou que este deve ser instalado no servidor de aplicações que lhe atende atualmente.		
05	A Gerência de Pesquisa e Desenvolvimento avisou que a administração do servidor de aplicações, do banco de dados e do controle de versões será feita pelo mesmo pesquisador.		
06	Num levantamento realizado por uma consultoria externa para levantamento da maturidade em segurança da informação, identificou-se que vários computadores de docentes estão sem antivírus instalados.		
07	Foi identificado na divisão financeira que houve uma alteração nos arquivos, mas não foi possível identificar quem executou tal alteração.		

Atividade 6.2 – Implementando a segurança da informação na gerência de operações e comunicações de sua organização

Você ainda é integrante do comitê de segurança da informação, e deverá apresentar propostas para a segurança da informação na gerência de operações e comunicações da sua organização. Elabore para cada um dos itens a seguir cinco tópicos que devem ser abordados em cada política:

a. Cópias de segurança.

b. Procedimentos contra software malicioso.

c. Tratamento de mídias.

d. Tratamento de documentos.

e. Segurança das redes.

f. Transferência de informações.