Política de Segurança da Informação

Treinamento

Porto do Itaqui – EMAP

Governo do Maranhão – Governo de todos nós

CONTATOS DE EMERGÊNCIA

Ocorrências Internas

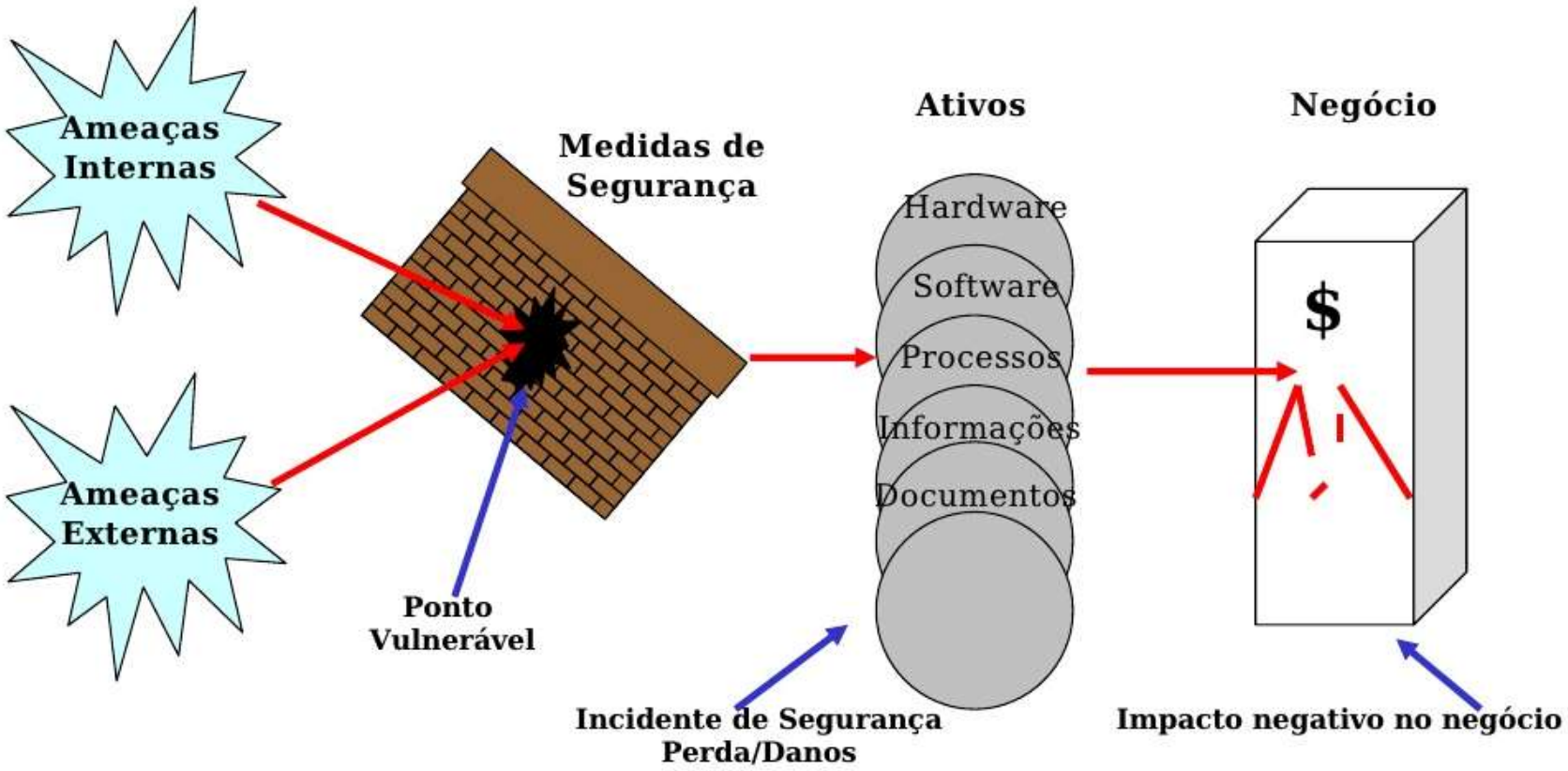
Fone:
3231.7444
98454.9662

Ramal:
5

Rádio:
Canal 1

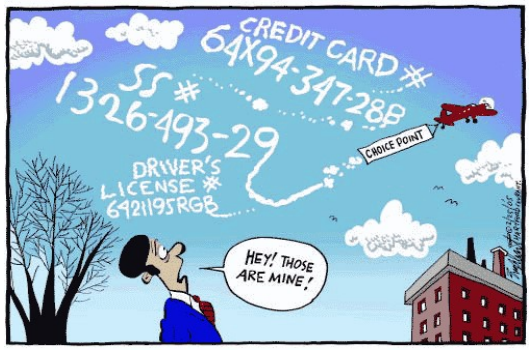
Política de Segurança da Informação

Ambiente nas Organizações



Principais Impactos

Quebra de Sigilo e Vazamento de Informações



Fraudes

Indisponibilidade dos serviços

Danos de imagem

Certificações
ISO 9001 : 2015
ISO 14001:2015

Segurança da Informação

O que é Segurança da Informação:

- Está relacionada com a proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou organização.
- Não está restrita somente aos sistemas computacionais, informações eletrônicas ou sistemas de armazenamento.
- **AS PESSOAS SÃO FUNDAMENTAIS PARA SEGURANÇA DA INFORMAÇÃO!!!!**

Características Básicas da segurança da informação:

- **Confidencialidade:** Garantia de que a informação é acessível somente por pessoas autorizadas a ter acesso à mesma.
- **Disponibilidade:** Garantia de acesso da informação aos usuários autorizados, sempre que necessário.
- **Integridade:** Garantia da inviolabilidade da informação durante seu ciclo de vida, preservando suas características e dados originais.

Sistema de Gestão da Segurança da Informação

Certificações
ISO 9001 : 2015
ISO 14001:2015

SGSI

Política do Sistema de Gestão da Segurança da Informação

- Comprometida com a segurança da informação, a EMAP mantém um Sistema de Gestão da Segurança da Informação com foco nos seguintes princípios:

➢ Garantir a **confidencialidade, integridade e disponibilidade das informações** de propriedade da EMAP ou sob sua custodia, com vistas a garantir a continuidade nos processos imprescindíveis, preservação e valores institucionais e qualidade na prestação dos seus serviços.

➢Garantir a **conformidade legal** e outros requisitos aplicáveis

➢Praticar a **melhoria contínua** do Sistema de Gestão da Segurança da Informação

➢ **É dever de todos os colaboradores e prestadores de serviços conhecer e cumprir esta política.**

Diretrizes do SGSI

A Segurança da Informação na Instituição estabelece os principais controles, denominados diretrizes:

- As **informações** da empresa, dos clientes e do público em geral **devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas**, evitando-se mau uso e exposição indevida.
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.
- O **acesso às informações** e recursos só deve ser feito se devidamente **autorizado**.
- Os **riscos às informações da empresa e incidentes de segurança da informação** devem ser reportados à Gerência de Tecnologia da Informação.
- As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas e todos devem entender e assegurar estas diretrizes.
- A **segurança da informação** deve ser considerada no **gerenciamento de projetos**, independentemente do tipo do projeto.

Diretrizes do SGSI

Tratamento da Informação:

- A informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação da EMAP
- **Toda e qualquer informação** produzida, recepcionada, classificada, utilizada, acessada, reproduzida, transportada, transmitida, distribuída, arquivada e armazenada **pelos empregados ou prestadores de serviços no exercício de suas funções públicas na empresa, são de propriedade da EMAP**
- As informações da empresa podem ser cedidas a terceiros por força da Lei de Acesso a Informação
- As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, conforme procedimento de Classificação da Informação

Incidentes de segurança da informação:

- Todo e qualquer **incidente de segurança da informação** deve ser obrigatoriamente **informado** pelos empregados e prestadores de serviços **à GETIN** no momento em que tomarem conhecimento do incidente

Diretrizes do SGSI

Gestão de Riscos:

- **Os riscos de segurança da informação são gerenciados pela GETIN** por meio de um processos para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Instituição, para que sejam recomendadas as proteções adequadas

Auditoria e Conformidade:

- **A EMAP possui direito legal de realizar o monitoramento, controle e registro de acesso às informações** que trafegam em sua rede interna e nos ativos de informação de propriedade da empresa.

Propriedade Intelectual:

- Tecnologias, marcas, metodologias e quaisquer informações que pertençam à EMAP **não podem ser utilizadas para fins particulares, nem repassadas a outrem**, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.

Diretrizes do SGSI

Controle de Acesso:

- O acesso, utilização e manuseio das informações e dos ativos de informação da EMAP por parte dos empregados e prestadores de serviço **são controlados e limitados ao cumprimento de suas atividades internas**
- **Os acessos podem ser rastreados**, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o empregado ou prestador de serviços, **para que seja responsabilizado por suas ações**.
- Os empregados e prestadores de serviço que utilizam ativos de informação e a rede interna da EMAP devem possuir uma **conta de acesso de usuário única e intransferível**

Monitoramento:

- **Todos os ativos de informação de propriedade da EMAP são monitorados** dentro dos limites da legislação vigente
- **Toda e qualquer pessoa que acessa as dependências da EMAP deve portar identificação física visível (pessoal e intransferível)** demonstrando qual sua função/atividade.

Diretrizes do SGSI

Uso de e-mail:

- O **correio eletrônico** disponibilizado da EMAP deve ser utilizado **somente para realização de atividades profissionais de interesse estritamente da Empresa**

Acesso à Internet:

- O **acesso à Internet** concedido aos empregados e prestadores de serviço que utilizam a rede interna da EMAP deve ser utilizado prioritariamente para os **interesses e negócios da Empresa**
- É vetado o acesso a sites de conteúdo de jogos, crimes, rádios, tvs, apostas, eróticos, pornográficos e blogs. A EMAP irá restringir os acessos a sites que, considerar alheios aos objetivos da Empresa, e monitorar consultas de usuários com o objetivo de garantir segurança e adequação no uso deste recurso.
- **Todos os acessos à internet serão armazenados em log, para posterior auditoria, se necessário**

Objetivos e Metas do Sistema de Gestão

Indicador	Necessidade da Informação	Medida	Fórmula / Pontuação	Meta	Frequência	Quem deve analisar	Arquivamento	Tipo (Gerencial/Técnico
Satisfação do Cliente	Avaliar o nível de satisfação dos clientes com relação aos atendimentos através da Central de Serviços da GETIN	Avaliações das pesquisas de satisfação com níveis Muito Bom e Excelente X Total de avaliações	Total de avaliações Muito bom e Excelente / Total de avaliações * 100	>= 80%	Mensal	GETIN	Servidor de Arquivos	Gerencial
Exposição aos Riscos	Avaliar a exposição dos ativos de informação da organização aos riscos de segurança da informação	Percentual de ações de minimização de riscos com avaliação de risco residual em "Risco Alto" e "Risco Extremo" no prazo	Total de ações com avaliação de risco residual em "Risco Alto" e "Risco Extremo" no prazo / Total de ações de minimização de riscos * 100	>= 80%	Semestral	GETIN	Servidor de Arquivos	Gerencial
Programa de auditoria interna	Realização do programa de auditoria interna	Quantidade de auditorias internas planejadas comparada à quantidade de auditorias planejadas	Quantidade Auditorias planejadas / Quantidade Auditorias planejadas * 100	100%	Anual	GETIN / GEQUA	Servidor de Arquivos	Gerencial
Acompanhamento das Ações de Melhoria e Ações Corretivas	Acompanhar o andamento das ações corretivas e ações de melhoria	Percentual de ações de melhoria e ações corretivas no prazo	a) Total de ações de melhoria no prazo / Total de ações de melhoria * 100 b) Total de ações corretivas prazo / Total de ações de corretivas * 100	>= 80%	Semestral	GETIN	Servidor de Arquivos	Gerencial
Engenharia Social	Avaliar se colaboradores estão preparados para agir apropriadamente no caso de ataques de engenharia social	Percentual dos colaboradores que reagem corretamente a um teste de engenharia social (envio de e-mail de phishing)	Quantidade de pessoas que não clicaram no link e/ou relataram o e-mail malicioso pelos canais apropriados / Total Participantes * 100	Verde: >= 90 Laranja: >= 60 Vermelho: < 60	Anual	GETIN	Servidor de Arquivos	Técnico
Gestão de Mudanças	Avaliar se o procedimento de gestão de mudanças está sendo respeitado	Percentual de novos sistemas / novas versões que respeitaram o procedimento de gestão de mudanças	Total de implantações de novos sistemas / novas versões dentro do procedimento / Total de implantações de novos sistemas / novas versões * 100	>= 90%	Semestral	GETIN	Servidor de Arquivos	Técnico

Objetivos e Metas do Sistema de Gestão

Indicador	Necessidade da Informação	Medida	Fórmula / Pontuação	Meta	Frequência	Quem deve analisar	Arquivamento	Tipo (Gerencial/Técnico
Anti-Malware	Garantir medidas de proteção contra malwares	Percentual de estações de trabalho com EndPoint obsoletos desde a última avaliação	Total de estações de trabalho com EndPoint obsoleto / Total de estações de trabalho * 100	<= 5%	Mensal	GETIN	Servidor de Arquivos	Técnico
Disponibilidade Total	Medir disponibilidade dos serviços críticos de TI	Percentual de disponibilidade dos serviços críticos de TI: a) Datacenter b) Internet c) Telefonia fixa d) Rádio digital e) E-mail f) TOS+ g) TOTVS RM	Horas de indisponibilidade / total de horas avaliadas * 100	>= 95%	Mensal	GETIN	Servidor de Arquivos	Gerencial
Regras de Firewall	Avaliar desempenho dos firewalls	Contagem de regras de borda do firewall utilizadas 0 vezes no período	Contador do firewall	Zero	Semestral	GETIN	Servidor de Arquivos	Técnico
Configuração de Dispositivos	Garantir que os ativos de informação da empresa são continuamente configurados de forma segura de acordo PSI (Anti-malware em todas as estaçõs, ausência de softwares não compliance e estações no domínio)	Percentual de ativos de informação em conformidade com a PSI	Total de ativos de informação em conformidade com a política / Total de ativos de informação * 100	95%	Mensal	GETIN	Servidor de Arquivos	Técnico
Análise de Vulnerabilidades Técnicas	Avaliar se os sistemas que processam informações sensíveis (conformidade e integridade) são vulneráveis a ataques maliciosos	Percentual de sistemas críticos nos quais foram realizados análise de vulnerabilidades técnicas	Total de análises de vulnerabilidades de sistemas realizadas / Total previsto de análises de vulnerabilidades * 100	>= 80%	Anual	GETIN	Servidor de Arquivos	Técnico
Eficácia da Gestão de Requisições e Incidentes	Avaliar eficácia da gestão de requisições e incidentes de segurança da informação	Percentual de requisições e incidentes solucionados dentro do prazo (SLA)	Total de requisições e incidentes solucionados dentro do prazo / Total de requisições e incidentes no período * 100	>= 80%	Mensal	GETIN	Servidor de Arquivos	Técnico
Eficácia da Equipe de Tratamento de Requisições e Incidentes	Avaliar eficácia da equipe que trata as requisições e incidentes de segurança da informação	O percentual de requisições e incidentes pendentes de finalização (backlog)	Total de requisições e incidentes pendentes de finalização no período / Total de requisições e incidentes *100	<= 2%	Mensal	GETIN	Servidor de Arquivos	Técnico
Reporte de Eventos de Segurança da Informação	Medir se os eventos de segurança da informação são reportados e formalmente tratados	Total de incidentes reportados X Total de funcionários	Contador de incidentes da Central de serviços da GETIN	Ao menos 1 para cada 50 colaboradores	Anual	GETIN	Servidor de Arquivos	Técnico

PROAPI

Contribuição no desempenho do Sistema de Gestão de Segurança da Informação

- As pessoas que realizam trabalhos sob o controle da EMAP devem garantir o cumprimento dos seguintes itens:

a) Atender a legislações pertinentes às suas atividades

b) Comunicar à GETIN no caso de ocorrência de incidentes de segurança da informação

c) Cumprir a Política de Segurança da Informação da EMAP

d) Contribuir para o atendimento aos objetivos de segurança da informação da EMAP

e) Cumprir os procedimentos de controle operacional da segurança da informação aplicáveis às suas atividades

PROPAI

Procedimentos:

- Os procedimentos do Sistema de Gestão da Segurança da Informação podem ser acessados em:

- **http://www.emap.ma.gov.br/_files/arquivos/PSI.zip**

SE EU VEJO,

EU COMUNICO!

Como reportar incidentes?

- **Todos os incidentes de segurança da informação devem comunicados imediatamente para GETIN**

Telefone: 3216-6011

E-mail: suporte@emap.ma.gov.br

Certificações
ISO 9001 : 2015
ISO 14001:2015

Obrigado(a)!

Nome do Colaborador
Cargo, função ou Depto.
Tel.: +55 (98) XXXXX-XXXX
emaildocolaborador@emap.ma.gov.br

EMAP PORTO DO ITAQUI

GOVERNO DO MARANHÃO
GOVERNO DE TODOS NÓS

Empresa Maranhense de Administração Portuária - EMAP
Av. dos Portugueses s/nº, CEP 65.085-370, Porto do Itaqui
São Luís, Maranhão, Brasil. +55 98 3216-6000 | Fax: 3222-4807
comunicacao@emap.ma.gov.br | emap.ma.gov.br