Prime

ISF – PROCESSOS DE GERENCIAMENTO NA SEGURANÇA DA INFORMAÇÃO

Gerenciando a Configuração

Diz respeito às configurações de:

- Hardware;
- Software;
- Serviços;
- Redes.

As configurações devem ser registradas;

Um log deve ser mantido e mudanças devem ser registras e armazenadas em:

- Bancos de dados de configuração;
- Modelos de configuração.

Gerenciando a Configuração

As mudanças devem seguir o processo de gerenciamento de mudanças;

Os registros de configuração podem conter:

- Proprietário ou ponto de contato do ativo;
- Data da última mudança de configuração;
- Versão do modelo de configuração;
- Relação a configurações de outros ativos.

Controle: Gerenciamento de Configuração

Objetivo:

Garantir que hardware, software, serviços e redes funcionem corretamente com as configurações de segurança necessárias, e a configuração não seja modificada por alterações não autorizadas ou incorretas.

O que é definido neste processo?

- Configurações, incluindo as de segurança para hardware, software, serviços, redes, para sistemas recém-instalados, sistemas operacionais;
- Funções, responsabilidades e procedimentos para garantir o controle de mudanças;
- Modelos padrão para a configuração segura de hardware, software, serviços e redes;
- Orientação disponível, por exemplo, pré-definidos de fornecedores e de organizações de segurança;
- Nível de proteção necessário para determinar um nível de segurança suficiente;
- Apoiar a política de segurança da informação e políticas específicas de tópicos;
- Considerar a viabilidade e aplicabilidade das configurações de segurança;
- As configurações devem ser monitoradas por meio de ferramentas.

Gerenciando a Mudança

- Mudanças ocorrem a toda hora, controladas ou não;
- Novos sistemas e grandes mudanças nos sistemas existentes devem seguir regras e processos formais;
- Responsabilidades e procedimentos devem ser formalizados;
- Procedimentos de controle de mudanças buscam garantir a confidencialidade, integridade e disponibilidade das informações;
- Sempre que possível, os procedimentos de controle de mudanças para infraestrutura, projetos e desenvolvimento devem ser integrados.

Causas comuns sem o controle de mudanças:

- Falhas de sistema ou de segurança;
- Em mudanças do ambiente de desenvolvimento para o de produção;
- Podem afetar a integridade e a disponibilidade dos aplicativos.
- A mudança de software pode impactar o ambiente de produção e vice-versa.

Boas práticas no processo de gerenciamento de mudanças:

- Testar componentes;
- Segregar ambientes de produção e desenvolvimento.

Controle: Gerenciamento de Mudanças

Objetivo:

Preservar a segurança das informações ao executar as mudanças.

O que incluir nos procedimentos de controle de mudanças?

- **Planejamento e avaliação do impacto potencial das mudanças;**
- **Procedimentos de retorno, emergência e contingência;**
- **Autorização das mudanças;**
- **Comunicação às partes interessadas relevantes;**
- **Implementação das mudanças incluindo planos de implantação;**
- **Testes e aceitação das mudanças;**

Controle: Gerenciamento de Mudanças

Quais seriam os procedimentos de controle de mudanças?

Registros das mudanças;

Manter atualizados:

- ✓ **Documentação operacional;**
- ✓ **Procedimentos do usuário;**
- ✓ **Planos de continuidade de TIC;**
- ✓ **Procedimentos de resposta e recuperação.**

Controle: Gerenciamento de Vulnerabilidades Técnicas

Objetivo:

Evitar a exploração de vulnerabilidades técnicas.

Qual o pré-requisito para realizar um gerenciamento de vulnerabilidades?

- Inventário preciso de ativos;
- Funções e responsabilidades associadas ao gerenciamento de vulnerabilidade técnica, como:
  - ✓ Monitoramento de vulnerabilidade;
  - ✓ Avaliação de risco de vulnerabilidade;
  - ✓ Rastreamento de ativos.
- Lista de recursos que serão usados para identificar vulnerabilidades técnicas;
- Exigir que os fornecedores assegurem o reporte, manuseio e divulgação de vulnerabilidades em contratos.

Controle: Gerenciamento de Vulnerabilidades Técnicas

Com isso em mãos, quais os próximos passos?

- Usar ferramentas de verificação de vulnerabilidade adequadas às tecnologias;
- Realizar testes de penetração planejados, documentados e repetíveis;
- Rastrear vulnerabilidades de bibliotecas de terceiros e código-fonte.

Considerações sobre o Gerenciamento de Vulnerabilidades Técnicas

Detectar a existência de vulnerabilidades em seus produtos e serviços e externos;	**Receber relatórios de vulnerabilidade de fontes internas ou externas.**
Estabelecer um ponto de contato público sobre divulgação de vulnerabilidades;	**Considerar programas de recompensas por descobertas de bugs;**
Um processo de atualização de software deve ser implementado para garantir que os patches aprovados mais atualizados sejam instalados;	**Se necessário, as modificações devem ser testadas e validadas;**

Considerações sobre o Gerenciamento de Vulnerabilidades Técnicas

- Para software adquirido, decida sobre usar atualização automática ou não;
- Um registro de auditoria deve ser mantido para todas as etapas do gerenciamento de vulnerabilidades técnicas;
- Alinhar com as atividades de gerenciamento de incidentes, para comunicar dados sobre vulnerabilidades;
- Responsabilidades pelo gerenciamento de vulnerabilidades para serviços em nuvem devem constar em contrato;

Lidando com Vulnerabilidades Técnicas

As seguintes orientações devem ser consideradas ao lidar com vulnerabilidades:

- Definir um cronograma para reagir a notificações de vulnerabilidades;
- Dependendo da urgência que precisa ser tratada, seguir com mudanças ou procedimentos de resposta a incidentes de segurança da informação;
- Utilizar apenas atualizações de fontes legítimas;
- Testar e avaliar as atualizações antes de serem instaladas;
- Abordar primeiro os sistemas de alto risco;
- Desenvolver remediação (normalmente atualizações ou patches de software);

Lidando com Vulnerabilidades Técnicas

As seguintes orientações devem ser consideradas ao lidar com vulnerabilidades:

- Testar para confirmar se a remediação ou mitigação é efetiva;
- Fornecer mecanismos para verificar a autenticidade da remediação;
- Se nenhuma atualização estiver disponível ou não puder ser instalada:
  - ✓ Aplique a solução alternativa sugerida pelo fornecedor ou de outras fontes;
  - ✓ Desligar serviços ou recursos relacionados à vulnerabilidade;
  - ✓ Adaptar ou adicionar controles de acesso, como firewalls;
  - ✓ Proteger sistemas, dispositivos ou aplicativos vulneráveis;
  - ✓ Aumentar o monitoramento para detectar ataques reais;
  - ✓ Aumentar a conscientização sobre a vulnerabilidade.

Como Gerenciar a Capacidade

Há duas formas de gerenciar a capacidade

1. Aumentando a Capacidade

- Contratando novos funcionários;
- Obtendo novas instalações ou espaço;
- Adquirindo sistemas, memória e armazenamento mais potentes;
- Migrando para a nuvem, por conta da elasticidade e escalabilidade.

2. Reduzindo a Demanda

- Excluindo dados obsoletos (espaço em disco);
- Descartando documentos impressos que tenham cumprido o prazo de retenção;
- Removendo aplicativos, sistemas, bancos de dados ou ambientes;
- Otimizando processos e batch;
- Eliminando desperdícios;
- Otimizando o código do aplicativo ou as consultas ao banco de dados;
- Negando ou restringindo largura de banda para serviços que não são críticos.

Controle: Gerenciamento de Capacidade

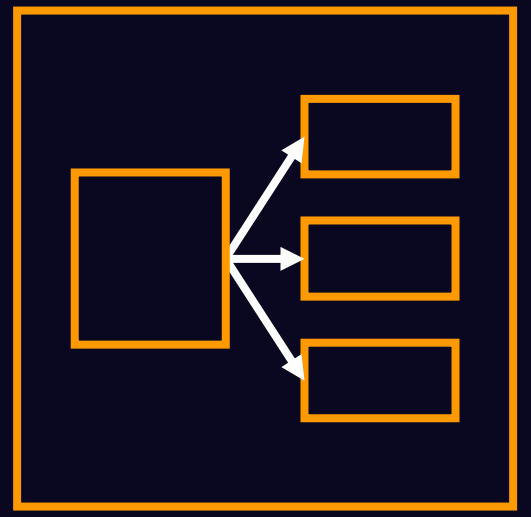
Objetivo:

Assegurar a capacidade necessária das instalações de processamento de informação, recursos humanos, escritórios e outras instalações.

Como assegurar a capacidade?

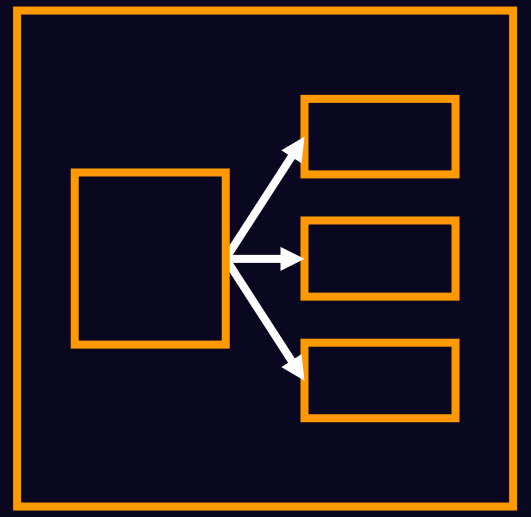
- Desenvolvendo um plano de gerenciamento de capacidade para sistemas de missão crítica;
- Identificando os requisitos de capacidade para instalações, recursos humanos e ativos;
- Monitorando o sistema e sua eficiência;
- Realizando testes de estresse de sistemas e serviços;
- Implementando controles de detecção para indicar problemas em tempo hábil;
- Projetando requisitos futuros de capacidade levando em conta requisitos de negócios e tendências;
- Especial atenção aos prazos de aquisição longos ou custos elevados.

Redundâncias



- Redundância é a duplicação de instalações em parte ou em sua totalidade;
- Pode ser com componentes sobressalentes ou duplicando tudo;
- As redundâncias são sempre ativadas em caso de emergência;
- Ativadas automaticamente ou manualmente;
- A redundância deve garantir o mesmo nível de segurança que os primários;
- Devem existir mecanismos para alertar sobre qualquer falha nas instalações.

Redundâncias



Existem alguns tipos de redundância para locais:

Cold Site: Funcionalidades básicas. Pode levar semanas para ativar e restaurar backups;

Hot Site: Espelha todos os equipamentos. Prontamente utilizado;

Warm Site: Intermediário ao Cold e Hot. Há constante atualização. Pode levar horas;

Mobile Site: Trailers ou caminhões. Mantém o essencial. Normalmente configurado como Cold ou Warm.

Controle: Redundância de Instalações de Processamento de Informações

Objetivo:

Assegurar o funcionamento contínuo das instalações de processamento de informação.

O que seguir ao implementar sistemas redundantes?

- Contratação de dois ou mais fornecedores de:
  - ✓ Serviços críticos;
  - ✓ Serviços de rede;
  - ✓ Provedores de serviços de internet.
- Utilização de redes redundantes;
- Usar dois data centers geograficamente separados com sistemas espelhados;
- Usar fontes de alimentação fisicamente redundantes.

Controle: Redundância de Instalações de Processamento de Informações

O que seguir ao implementar sistemas redundantes?

- Balanceamento de carga de múltiplas instâncias paralelas de componentes de software (entre instâncias no mesmo data center ou em data centers diferentes);
- Ter componentes duplicados em sistemas (por exemplo, CPU, discos rígidos, memórias) ou em redes (por exemplo, firewalls, roteadores, switches).
- Se possível, testar a redundância para garantir o failover para outro componente;

Consideração:

Medidas de redundância podem fazer parte das estratégias de continuidade de TIC.

Controle: Backup de Informações

Objetivo:

Habilitar a recuperação de perda de dados ou sistemas.

Dicas?

- Quanto mais antigo o backup, menores as consequências da perda de informação;
- Mais importante que o backup é o teste do Restore;
- Cuidado ao manejar os backups. São trancados? Onde são armazenados?

Controle: Backup de Informações

O que considerar em um Plano de Backup?

- Procedimentos precisos e completos de backup e restauração;
- Que reflitam os requisitos de negócios, segurança das informações e a criticidade;
- Definição se o backup será completo ou diferencial, assim como a frequência;
- Armazenamento dos backups em um local remoto, seguro e protegido;
- Proteção física e ambiental;
- Testes regulares da mídia de backup;
- Proteção dos backups por meio de criptografia de acordo com os riscos identificados;
- Consideração do período de retenção das cópias de arquivos;
- Após o período de retenção, consideração sobre uma exclusão segura.

Registro e Monitoramento

- Com o aumento de ataques e mau comportamento, intencional ou não, é necessário ter a capacidade de registrar eventos e produzir evidências.
- Para esse propósito, é essencial ter um bom registro (logging).
- Registre e monitore, principalmente as evidências;
- Registre os eventos (log) de:


Atividades de sistema;


Atividades de usuários;


Exceções;


Falhas;


Eventos de segurança da informação.

- Caso não seja feita uma análise desses logs, a coleta será inútil;

- Mantenha os logs protegidos e em um local seguro;
- Antes de iniciar a coleta, garanta que os relógios do sistema estão sincronizados;
- Tenha em mente que arquivos de log contendo dados pessoais devem ser protegidos conforme as leis de privacidade.

Controle: Registro

Objetivo:

Registrar eventos, gerar evidências, garantir a integridade das informações de log, prevenir contra acesso não autorizado, identificar eventos de segurança da informação que possam levar a um incidente de segurança da informação e apoiar investigações.

O que considerar no controle de registro de eventos?

- Determine a finalidade e quais dados serão coletados e registrados;
- Os relógios devem estar sincronizados;
- Deve haver proteção dos registros, como hash ou acesso somente leitura;
- Verifique os requisitos de arquivamento e retenção dos logs de auditoria;
- Use mascaramento de dados para enviar logs para fornecedores;
- Analise os registros em busca de atividades incomuns ou anormais;
- Em ambientes na nuvem, as responsabilidades podem ser compartilhadas;
- Use a inteligência de ameaças disponível.

Logs de Eventos

O que incluir em cada log de evento?

- IDs de usuário;
- Atividades do sistema;
- Datas, horários e detalhes de eventos relevantes (por exemplo, login e logoff);
- Identificação do dispositivo, do sistema e localização;
- Endereços e protocolos de rede.

Eventos que devem ser considerados para registro:

- Tentativas de acesso ao sistema bem-sucedidas e rejeitadas;
- Alterações na configuração do sistema;
- Uso de privilégios;
- Uso de programas e aplicativos utilitários;

Logs de Eventos

Eventos que devem ser considerados para registro:

- Arquivos acessados e o tipo de acesso, incluindo exclusão de arquivos importantes;
- Alarmes disparados pelo sistema de controle de acesso;
- Ativação e desativação de antivírus e detecção de intrusão;
- Criação, modificação ou exclusão de identidades;
- Transações executadas por usuários em aplicativos.

Controle: Atividades de Monitoramento

Objetivo:

Detectar comportamentos anômalos e possíveis incidentes de segurança da informação.

O que é preciso fazer para detectar comportamentos anômalos?

- Os registros de monitoramento devem ser retidos por períodos definidos;
- Estabelecer uma linha de base de comportamento normal;
- Monitorar esta linha de base para anomalias e períodos de pico;
- Monitoramento contínuo por meio de uma ferramenta de monitoramento;
- Software de monitoramento automatizado configurado para gerar alertas;
- Eventos anormais devem ser comunicados às partes relevantes.

Monitorando Anomalias

O que podemos incluir no sistema de monitoramento?

- Entrada e saída do tráfego de rede, sistema e aplicativo;
- Acesso a sistemas, servidores, equipamentos de rede, aplicações críticas, etc.;
- Arquivos de configuração de rede e sistema de nível crítico;
- Logs de antivírus, IDS, sistema de prevenção de intrusão (IPS), filtros da web, firewalls, prevenção de vazamento de dados;
- Relacionados às atividade do sistema e da rede;
- Uso dos recursos, como CPU, discos rígidos, memória, largura de banda.

Monitorando Anomalias

Monitorar conforme linha de base:

- Utilização dos sistemas em períodos normais e de pico;
- Local, frequência e horário habitual de acesso;
- Encerramento não esperado de processos ou aplicativos;
- Atividade associada a malware, tráfego de endereços IP maliciosos ou botnet;
- Ataque conhecidos, como negação de serviço e estouro de buffer;
- Comportamentos incomuns como keystroke logging ou process injection;
- Gargalos e sobrecargas, como latência e network jitter;
- Acesso não autorizado (real ou tentativa) aos servidores DNS, portais da web etc.;
- Varredura não autorizada de aplicativos, sistemas e redes.

Controle: Sincronização do Relógio

Objetivo:

Permitir a correlação e análise de eventos relacionados à segurança e outros dados registrados e apoiar investigações sobre incidentes de segurança da informação.

Qual a importância de sincronizar relógio?

- Garante precisão dos logs de eventos;
- Necessários para investigações ou como prova em casos legais e disciplinares;
- Essenciais para registros de auditoria, pois evita prejudicar a credibilidade.

Controle: Sincronização do Relógio

Considerações

- Um tempo de referência padrão para uso dentro da organização deve ser definido;
- Um relógio atômico ou sistema de posicionamento global (GPS) deve ser usado;
- Usar NTP (Network Time Protocol) and PTP (Precision Time Protocol);
- Usar duas fontes externas de tempo ao mesmo tempo para melhorar a confiabilidade dos relógios e gerenciar adequadamente qualquer variação;
- Diferenças devem ser registradas para mitigar riscos decorrentes de discrepâncias.

Controle: Prevenção de Vazamento de Dados

Objetivo:

Detectar e impedir a divulgação e extração não autorizadas de informações por indivíduos ou sistemas.

O que fazer para reduzir o risco de vazamento de dados?

- **Identificar e classificar informações para proteger contra vazamentos;**
- **Monitorar canais como e-mail, transferências de arquivos, dispositivos móveis e de armazenamento;**
- **Evitar o vazamento de informações, como e-mails de quarentena contendo informações confidenciais.**

Controle: Prevenção de Vazamento de Dados

As ferramentas de prevenção e vazamento de dados devem ser usadas para:

- Identificar e monitorar informações confidenciais;
- Detectar a divulgação de informações confidenciais, como aquelas carregadas em serviços de nuvem de terceiros ou enviadas por e-mail;
- Bloquear ações dos usuários ou transmissões de rede que exponham informações confidenciais, por exemplo, cópia de entradas de banco de dados em uma planilha.

Prevenindo o Vazamento de Dados

A organização precisa avaliar as seguintes necessidades:

- De um usuário copiar e colar um conteúdo;
- Fazer upload de dados para dispositivos e mídia de armazenamento;
- Usuários visualizarem e manipularem dados mantidos remotamente;
- Exportação de dados;
- Captura de telas ou fotografias da tela.

Considere ações que confundam o adversário:

- Substituindo informações autênticas por informações falsas;
- Engenharia social reversa;
- Usando honeypots para atrair invasores.

Controle: Exclusão de Informações

Objetivo:

Evitar a exposição desnecessária de informações confidenciais e cumprir os requisitos legais, estatutários, regulamentares e contratuais para exclusão de informações.

O que levar em consideração na hora de excluir informações?

- O método de exclusão;
- Evidências do resultado da exclusão;
- Se utilizar fornecedores, obter evidências de exclusão de informações deles.

Controle: Exclusão de Informações

Quando e o que excluir?

- Quando não forem mais necessárias, conforme período definido na política;
- Por solicitação do titular;
- Versões obsoletas, cópias e arquivos temporários onde quer que estejam;

Considerações

- Usar software que garanta a exclusão permanentemente;
- Usar fornecedores aprovados e certificados para serviços de descarte seguro;
- Usar mecanismos de descarte apropriados como desmagnetização de discos rígidos e outros meios de armazenamento magnético.

Controle: Proteção de Sistemas de Informação Durante Testes de Auditoria

Objetivo:

Minimizar o impacto da auditoria e outras atividades de garantia em sistemas operacionais e processos de negócios.

Quais orientações devem ser observadas durante uma auditoria?

- Acordar a solicitação de acesso aos sistemas e dados para auditoria;
- Acordar e controlar o escopo dos testes de auditoria;
- Limitar os testes de auditoria ao acesso somente leitura a software e dados;
- Se necessário outras permissões, executar o teste por um administrador em nome do auditor;
- Verificar requisitos de segurança dos dispositivos usados para acesso;
- Excluir cópias quando a auditoria for concluída ou proteção adequada se houver a obrigação;
- Executar testes de auditoria que possam afetar a disponibilidade do sistema fora do horário comercial;
- Monitorar e registrar todos os acessos para fins de auditoria e teste.

OBRIGADO

ISF – PROCESSOS DE GERENCIAMENTO NA SEGURANÇA DA INFORMAÇÃO