Prime

ISF – SEGURANÇA DA INFORMAÇÃO EM ATIVOS

Controle: Inventário de Informações e Outros Ativos Associados

Objetivo:

Identificar as informações da organização e outros ativos associados, a fim de preservar a segurança das informações e atribuir a propriedade apropriada.

Como seria este inventário?

- Preciso, atualizado, consistente e alinhado com outros inventários;
- Revisado regularmente;
- Atualizado automaticamente no processo de instalação, alteração ou remoção de um ativo;
- A granularidade deve estar em um nível adequado às necessidades;
- Cada ativo deve ser classificado de acordo com a classificação das informações;
- Informações e ativos devem ser atribuídas a um indivíduo ou grupo.

Gestão de Ativos

Para fazer a gestão dos ativos:

- Primeira coisa a se fazer é identificar as informações da organização:
  - ✓ Identificar o que se deseja preservar;
  - ✓ Atribuir a propriedade apropriada.
- Esse processo é chamado de inventário;
- Pode conter: informação, hardware, software, máquinas virtuais (VMs), instalações, pessoal, competência, capacidades e registros;
- Cada ativo deve ser classificado de acordo com a classificação das informações;
- A granularidade deve ser adequada;
- Deve ser atribuído um dono para o ativo inventariado.

Ativos de Negócios

As informações que são gravadas sobre os bens da empresa são:

- ✓ O tipo de ativo de negócio;
- ✓ Dono do ativo (dono do processo);
- ✓ Localização do ativo;
- ✓ O custo inicial;
- ✓ A idade;
- ✓ O custo estimado de reposição;
- ✓ O formato do ativo;
- ✓ A classificação;
- ✓ Valor do ativo para o negócio.

Gerenciamento de **Ativos de Negócios**

- Uma forma de controlar ou gerenciar riscos é exercer controle sobre as mudanças;
- Mudanças podem representar algum tipo de risco;
- Há vários modelos e métodos disponíveis que ajudam a exercer o controle, por exemplo, no COBIT, na ISO 20000 e na ITIL.

Esses modelos ajudam a:

- ✓ Lidar com os ativos;
- ✓ Entender como as mudanças acontecem;
- ✓ Quem inicia as mudanças e como são testadas.

Lidando e Usando **Ativos de Negócios**

Qual o objetivo de documentar a forma como lidamos com os ativos de negócio?

- Evitar erros que possam surgir pelo uso incorreto dos ativos;
- Evitar um dano desnecessário;
- Os procedimentos para lidar com os ativos devem ser desenvolvidos e implementados de acordo com o esquema de classificação de informação;
- Quanto mais complexo for o ativo, mais útil será definir instruções e direções claras.
- Exemplo: uma simples regra como não colocar papéis que contenham metal (clipes, grampos) em um triturador de papéis.

Qual o objetivo das regras para o uso de ativos de negócio?

- A implementação dessas regras está inclusa no escopo das medidas organizacionais;
- Normalmente providas em um manual;
- Exemplo: instruções de como usar equipamentos móveis quando fora da organização.

Controle: Uso Aceitável de Informações e Outros Ativos Associados

Objetivo:

Garantir que as informações e outros ativos associados sejam adequadamente protegidos, usados e manuseados.

Para quem é direcionado este controle?

- Serve para usuários externos que usam ou têm acesso às informações e ativos da organização;
- Eles devem ser responsáveis pelo uso de quaisquer recursos de processamento de informações.
- O uso de ativos de terceiros (nuvem) devem ser identificados e controlados por meio de acordos com provedores de serviços em nuvem;
- Cuidados também devem ser tomados quando um ambiente de trabalho colaborativo é usado.

Política de Uso Aceitável de Ativos e Informações

- **Uma política de Uso Aceitável deve indicar:**
  - ✓ Comportamentos esperados e inaceitáveis;
  - ✓ Uso permitido e proibido de informações e outros ativos associados;
  - ✓ Atividades de monitoramento que estão sendo realizadas pela organização.
- **Os seguintes itens devem ser considerados:**
  - ✓ Restrições de acesso para cada nível de classificação;
  - ✓ Manutenção de cadastro dos usuários autorizados;
  - ✓ Proteção de cópias temporárias ou permanentes de informações;
  - ✓ Armazenamento de ativos associados a informações;
  - ✓ Autorização de descarte de informações e outros ativos.

Manuseio de Mídia

- "Mídia" refere-se a qualquer coisa em que dados possam ser gravados:
  - ✓ Papel, CDs, DVDs, pen drives, discos rígidos, fitas de backup etc.
- O propósito de ter diretrizes sobre como manusear mídias é:
  - ✓ Evitar que informações valiosas caiam em mãos erradas;
  - ✓ Prevenir publicação não autorizada;
  - ✓ Evitar mudanças, eliminação ou destruição de ativos;
  - ✓ Prevenir interrupção de atividades de negócio.
- A forma na qual a mídia deve ser manuseada é frequentemente ligada ao sigilo ou à classificação (categoria) e é documentada em procedimentos;
- Após o prazo de armazenamento ter expirado, devem ser destruídos, descartados ou esvaziados de forma segura, de preferência, por uma empresa especializada.

Controle: Devolução de Ativos

Objetivo:

Proteger os ativos da organização como parte do processo de mudança ou rescisão de emprego, contrato ou acordo.

O que acontece neste controle?

- O pessoal e outras partes interessadas devem devolver todos os ativos da organização em sua posse;
- Após a mudança ou rescisão, o pessoal deve devolver todos os ativos da organização;
- Esse controle tem o objetivo de proteger os ativos da organização;
- Faz parte do processo de mudança ou rescisão de trabalho, contrato ou acordo.

Devolução de Ativos

- Nos casos em que o pessoal compra o equipamento da organização ou usa seu próprio equipamento pessoal, os procedimentos devem ser seguidos para:
  - ✓ Garantir que todas as informações relevantes sejam rastreadas;
  - ✓ Transferidas para a organização;
  - ✓ Excluídas com segurança do equipamento.
- Durante o período de aviso prévio e posteriormente, a organização deve impedir a cópia não autorizada de informações relevantes;
- Identificar e documentar claramente o que deve ser devolvido:
  - ✓ Dispositivos terminais do usuário;
  - ✓ Dispositivos portáteis de armazenamento;
  - ✓ Equipamento especializado;
  - ✓ Hardware de autenticação (por exemplo, chaves, tokens e *smartcards*);
  - ✓ Cópias físicas das informações.

BYOD

- BYOD é Bring Your Own Device (BYOD), ou “traga o seu próprio dispositivo”;
- Possibilidade de usar os próprios dispositivos para trabalhar;
- São os ativos pessoais (um tablet, laptop ou telefone celular);
- Contém informações de negócio e essas informações devem ser protegidas;
- Deve haver uma política para BYOD na empresa;
- A empresa deve permitir apenas dispositivos que estejam em conformidade com a política BYOD;
- O uso desses dispositivos deve ser autorizado pela administração e deve ter controles, como:
  - ✓ Separação do uso pessoal e comercial dos dispositivos;
  - ✓ Acesso às informações comerciais somente após os usuários terem reconhecido seus deveres;
  - ✓ Políticas e procedimentos para evitar disputas sobre direitos de propriedade intelectual;
  - ✓ Acesso aos equipamentos durante uma investigação e controles de segurança;
  - ✓ Acordos de licenciamento de software.

Classificação da Informação

Designar é forma especial de categorização (exemplo: de acordo com um determinado assunto da organização ou um grupo de pessoas autorizadas)

Dono (responsável por um ativo de negócio)

Classificar é o ato de atribuir a classificação (como secreto, confidencial ou público)

Classificação é usada para definir diferentes níveis de sensibilidade na qual a informação deve ser estruturada

Controle: Classificação das Informações

Objetivo:

Assegurar a identificação e compreensão das necessidades de proteção da informação de acordo com sua importância para a organização.

Como é a Classificação?

- As informações devem ser classificadas de acordo com:
  - ✓ Seus requisitos legais;
  - ✓ Valor;
  - ✓ Importância;
  - ✓ Sensibilidade à divulgação ou modificação não autorizada.
- O Proprietário de um Ativo do Negócio atribui um nível adequado de acordo com uma lista de classificações.

Classificação

A classificação:

- Indica o nível de segurança necessário;
- Está de acordo com a maneira pela qual o bem da empresa é utilizado no negócio.
- O proprietário deve garantir que o ativo de negócio seja reclassificado se necessário;
- Só pode ser rebaixada pelo Proprietário;
- O Proprietário determina quem tem acesso aos Ativos do Negócio específicos;
- A classificação dada à informação é uma maneira rápida de determinar como esta informação será tratada e protegida;
- A classificação de um Ativo do Negócio também determina como ele pode ser armazenado fisicamente.

Controle: Rotulagem das Informações

Objetivo:

Facilitar a comunicação da classificação da informação e apoiar a automatização do processamento e gestão da informação.

O que é rotular?

- Procedimentos para “etiquetar” as informações;
- Deve ser desenvolvido e implementado de acordo com o esquema de classificação de informação adotado pela organização;
- Facilita a comunicação da classificação da informação;
- Apoia a automatização do processamento e gestão da informação.

Rotulagem

- Após classificado, é hora do ativo ser “etiquetado” ou rotulado;
- Se um ativo tem uma classificação, é dada uma marca ou etiqueta a ele;
- Isto pode ser colocado de forma física e visível;

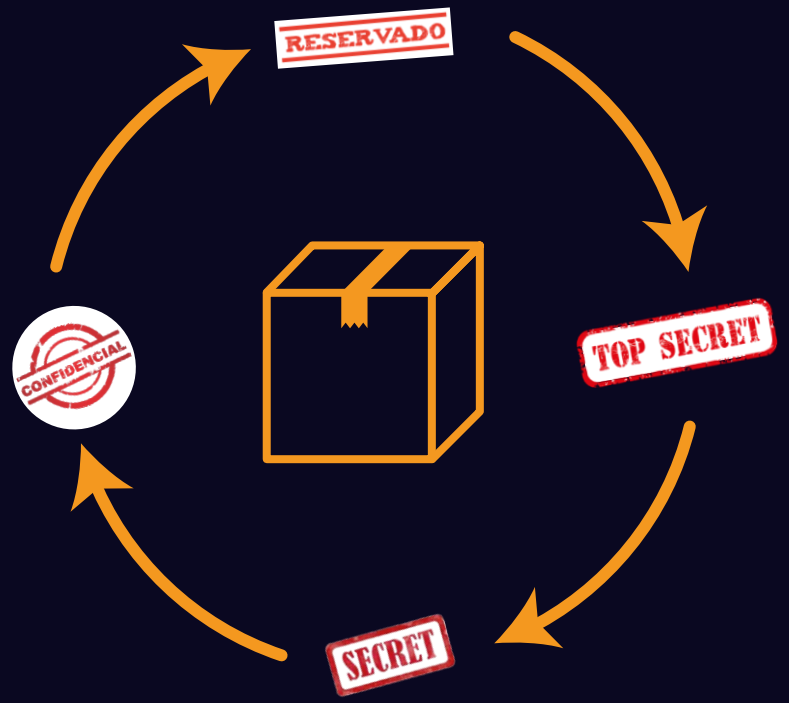
Considere os seguintes rótulos:

- Informações enviadas ou armazenadas em meio eletrônico ou físico;
- Cabeçalhos e rodapés de documentos e mensagens;
- Informações classificadas como sensíveis ou críticas;
- Marca d'água;
- Outros metadados úteis que podem ser anexados às informações;
- Carimbos.

Exemplos de **Classificação e Rótulos**

- Etiquetas físicas são uma forma comum de rotulagem;
- No entanto, documentos eletrônicos requerem um meio eletrônico de rotulagem, como, por exemplo, uma mensagem de notificação na tela.

Atenção: A falta de um rótulo "CONFIDENCIAL" não faz do ativo um ativo "PÚBLICO"



Controle: Transferência de Informação

Objetivo:

Manter a segurança das informações transferidas dentro de uma organização e com qualquer parte externa interessada.

Qual tipo de transferência?

- Para todos os tipos de transferências:
  - ✓ Verbal;
  - ✓ Eletrônica;
  - ✓ De mídia de armazenamento físico.

Como fazer?

- Estabeleça e comunique uma política sobre transferência de informações;
- As regras, procedimentos e acordos devem refletir a classificação;
- Deve incluir a autenticação do destinatário para proteção.

OBRIGADO

ISF – SEGURANÇA DA INFORMAÇÃO EM ATIVOS