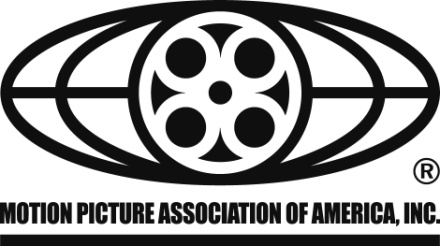
****

**Programa de segurança de conteúdos da MPAA**

**MELHORES PRÁTICAS PARA SEGURANÇA DE CONTEÚDOS**

**DIRETRIZES COMUNS**

[**http://www.mpaa.org/content-security-program/**](http://www.mpaa.org/content-security-program/)

Versão 3.0

2 de abril de 2015

Histórico do documento

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data** | **Descrição** | **Autor** |
| 1.0 | 31 de dezembro de 2009 | Lançamento público inicial | Deloitte & Touche LLP  MPAA  Empresas associadas da MPAA |
| 2.0 | 15 de maio de 2011 | Atualizações e revisões  Consolidação em Diretrizes comuns e complementares | PwC LLP  MPAA  Empresas associadas da MPAA |
| 2.1 | 1º de janeiro de 2013 | Atualizações e revisões | PwC LLP  MPAA  Empresas associadas da MPAA |
| 3.0 | 2 de abril de 2015 | Atualizações e revisões | MPAA  Empresas associadas da MPAA |

Índice

[Histórico do documento i](#_Toc427161836)

[I. Visão geral das melhores práticas 2](#_Toc427161837)

[II. Visão geral da unidade 3](#_Toc427161838)

[III. Gestão de risco 4](#_Toc427161839)

[IV. Formato de melhores práticas 6](#_Toc427161840)

[V. Diretrizes comuns das melhores práticas 7](#_Toc427161841)

[Anexo A – Glossário 84](#_Toc427161842)

[Anexo B — Definições de canal de distribuição e título da MPAA 88](#_Toc427161843)

[Anexo C — MAPEAMENTO PARA AS UNIDADES 90](#_Toc427161844)

[Anexo D — Mapeamento de controles para referências 102](#_Toc427161845)

[Anexo E — Perguntas mais frequentes 107](#_Toc427161846)

[Anexo F — Políticas e procedimentos sugeridos 108](#_Toc427161847)

[Anexo G — Outros recursos e referências 109](#_Toc427161848)

[Anexo H — Denúncia de pirataria para a MPAA 110](#_Toc427161849)

1. Visão geral das melhores práticas

**Introdução**

Por mais de três décadas, a Motion Picture Association of America, Inc. (MPAA) administrou avaliações de segurança de conteúdos em nome de suas Empresas associadas (Membros): Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Universal City Studios LLC; Twentieth Century Fox Film Corporation; Walt Disney Studios Motion Pictures e Warner Bros. Entertainment Inc.

A partir de 2007, estas análises foram realizadas utilizando um modelo de pesquisa, processo e modelo de relatório padronizados. Desde então, mais de 500 unidades foram entrevistadas em 32 países.

A MPAA está empenhada em proteger os direitos de quem cria conteúdo de entretenimento para o público em todo o mundo. Desde as artes criativas até a indústria de software, mais e mais pessoas em todo o mundo fazem sua vida com base na força de suas ideias. Isto significa que há uma participação crescente na proteção dos direitos de propriedade intelectual e reconhecimento de que estas salvaguardas são a pedra angular de uma economia de informação global saudável.

O objetivo do Programa de segurança de conteúdos da MPAA é reforçar o processo pelo qual o conteúdo dos membros é protegido durante a produção, pós-produção, comercialização e distribuição. Isso é realizado através do seguinte:

* publicação de um conjunto de melhores práticas através do serviço da unidade que descreve os controles padrão que ajudam a proteger o conteúdo dos membros;
* aferir e avaliar a segurança do conteúdo em parceiros externos com base nas melhores práticas publicadas;
* reforçar a importância de proteger o conteúdo dos membros; e
* fornecer um veículo de avaliação padrão para impulsionar as discussões individuais sobre questões de segurança de conteúdo entre os membros e seus parceiros de negócios.

**Objetivo e aplicabilidade**

O objetivo deste documento é fornecer aos fornecedores externos atuais e futuros contratados pelos membros um entendimento das expectativas gerais de segurança de conteúdo e das melhores práticas atuais da indústria. As decisões sobre o uso de fornecedores por qualquer membro específico são tomadas pelos membros exclusivamente de forma unilateral.

As práticas recomendadas de segurança de conteúdo são projetadas para levar em consideração os serviços que a unidade fornece, o tipo de conteúdo que a unidade controla, e em que janela de lançamento a unidade funciona.

As melhores práticas descritas neste documento estão sujeitas às leis e normas locais, estaduais, regionais, federais e do país.

As melhores práticas descritas neste documento, assim como os padrões da indústria e as referências da ISO aqui contidas, estão sujeitas a alterações periódicas.

**A conformidade com as melhores práticas é estritamente voluntária. Este não é um programa de acreditação.**

**Processo de exceção**

Sempre que não for viável cumprir uma melhor prática, as unidades devem documentar por que não podem cumprir a melhor prática e implementar medidas de compensação utilizadas em substituição da melhor prática. As exceções devem ser comunicadas diretamente ao Membro.

**Perguntas ou comentários**

Se você tiver quaisquer perguntas ou comentários sobre as melhores práticas, envie e-mail para contentsecurity@mpaa.org

1. Visão geral da unidade

A tabela a seguir descreve os serviços típicos oferecidos, o conteúdo controlado e a janela de lançamento envolvida em cada tipo de unidade.

| **N.º** | **Tipo de unidade** | **Serviços típicos da unidade** | **Tipo de conteúdo** | **Janela de lançamento** |
| --- | --- | --- | --- | --- |
| **1** | **Áudio, dublagem e legendagem** | * Dublagem no idioma original e estrangeiro * Legendagem * SFX * Pontuação * ADR/Foley | * Baixa resolução * Com marca d'água/estragado * Conteúdo completo/parcial * Masters de áudio | * Prévia de Cinema * Prévia de Home Vídeo |
| **2** | **Serviços de courier, entrega e remessa** | * Serviços de courier * Serviços de entrega * Empresas de remessa | * Variados | * Prévia de Cinema * Prévia de Home Vídeo * Catálogo |
| **3** | **Publicidade Criativa** | * Sem acabamento * Trailer * Propagandas de TV * Teasers * Imagens gráficas * Anúncios da Web | * Conteúdo completo/parcial estragado, com marca d'água * Imagens fixas * Clipes | * Prévia de Cinema * Prévia de Home Vídeo * Catálogo |
| **4** | **Serviços**  **Digital** | * Dominando o cinema digital * Replicação * Gerenciamento de chaves | * Alta resolução – conteúdo completo ou parcial * Principais distribuições de cinema digital * Pacotes de cinema digital | * Prévia de Cinema |
| **5** | **Serviços**  **Digitais** | * Intermediário digital * Varredura * Gravação de filme * Restauração de filmes | * Alta resolução – conteúdo completo ou parcial (fita de filme) | * Prévia de Cinema * Catálogo |
| **6** | **Distribuição** | * Distribuição * Execução * Bastidores/Depósito de filmes * DVD/ Reciclagem de fita | * Alta resolução * Imagem limpa | * Prévia de Cinema * Prévia de Home Vídeo * Catálogo |
| **7** | **DVD**  **DVD** | * Compressão * Criação * Codificação * Regionalização * Características especiais * Verificar disco CQ | * Limpeza – longa metragem | * Prévia de Home Vídeo |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N.º** | **Tipo de unidade** | **Serviços típicos da unidade** | **Tipo de conteúdo** | **Janela de lançamento** |
| **8** | **DVD**  **DVD** | * Compressão * Criação * Codificação * Regionalização * Características especiais * Verificar disco CQ | * Limpeza – longa metragem | * Prévia de Home * Vídeo |
| **9** | **Entretenimento de Voo (IFE) e**  **Serviços de hotelaria** | * Laboratório IFE * Integração IFE * Hotel * Companhia aérea * Navio de cruzeiro/Balsa * Bibliotecas * Hospitais * Prisões | * Alta resolução – conteúdo completo ou parcial * Estragado – conteúdo completo ou parcial | * Prévia de Cinema * Prévia de Home Vídeo * Catálogo |
| **10** | **Serviços de pós-produção** | * Telecinagem * Duplicação * Edição * Acabamento * CQ | * Alta resolução – conteúdo completo ou parcial | * Prévia de Cinema * Prévia de Home Vídeo * Catálogo |
| **11** | **Replicação** | * Premasterização * Masterização * Replicação * Verificação da Criação de disco | * Alta resolução * Imagem limpa | * Prévia de Home Vídeo |
| **12** | **Efeitos**  **visuais**  **(VFX)** | * Pós-produção digital * Imagens geradas por computador * Animação | * Alta resolução – parcial * Quadros, tomadas, sucessões e imagens fixas * Scripts * Storyboards | * Prévia de Cinema * Pós-cinema (2D e 3D) |
| **13** | **Aplicativo** | * Desenvolvimento de aplicativo | * Variados | * Variados |
| **14** | **Nuvem** | * Hospedagem * Centro de dados | * Variados | * Variados |

1. Gestão de risco

**Avaliação de risco**

Os riscos devem ser identificados por meio de uma avaliação de risco e controles apropriados devem ser implementados para diminuir o risco a um nível aceitável e garantir que os objetivos de negócios sejam atingidos.

A Organização Internacional para Padronização (ISO) 27000 define o risco como a "combinação da probabilidade de um evento e sua consequência." Por exemplo, qual é a probabilidade do conteúdo ser roubado da rede de uma unidade e liberado publicamente e qual é a consequência empresarial para uma organização e para o cliente se isso ocorrer (por exemplo, quebra contratual e/ou perda de receita para essa janela de lançamento).

A importância de um sistema de gestão robusto também é destaque na norma ISO 27001, que mostra como estabelecer um Sistema de gestão da segurança da informação (ISMS).

**Classificação de ativos**

Uma maneira de classificar os ativos em sua unidade é seguir um processo de quatro fases, o qual é resumido a seguir:

Monitorar e avaliar a eficácia

Determinar o controle de segurança mínimo definido

Implementar controles

Identificar e classificar ativos

Em consulta com o Membro (seu cliente), uma organização é responsável por determinar quais ativos de clientes exigem um maior nível de segurança. A tabela a seguir fornece um exemplo de como classificar o conteúdo:

| **Classificação** | **Descrição** | **Exemplos** |
| --- | --- | --- |
| **Conteúdo de alta segurança** | Qualquer conteúdo que a organização acredita que resultaria em perda financeira, reputação negativa da marca ou sérias penalidades caso o ativo seja roubado ou vazado | * Roubo de um filme de grande sucesso antes de seu primeiro lançamento mundial no cinema * Roubo de conteúdo de home vídeo antes de sua primeira data de lançamento em todo o mundo * Roubo de masters ou de visualizadores |

Informações adicionais sobre os riscos geralmente associados a cada tipo de unidade são também incluídas em cada melhor prática complementar.

**Controles de segurança**

O Instituto de governança de TI define controles como as "políticas, procedimentos, práticas e estruturas organizacionais destinadas a fornecer uma garantia aceitável de que os objetivos do negócio serão atingidos e eventos indesejáveis serão evitados ou detectados e corrigidos". Os controles de segurança são geralmente selecionados com base na classificação do ativo, de seu valor para a organização, e o risco de o ativo ser vazado ou roubado.

A fim de mitigar os riscos identificados, as organizações são encorajadas a implementar controles proporcionais a cada risco específico. Tais medidas também devem ser avaliadas periodicamente quanto a seu design e eficácia com base no ambiente de ameaça atual.



**Sistema de gestão**



**Organização e gestão**



**Segurança física**



**Transporte**



**Unidade**



**Segurança digital**



**Infraestrutura**



**IV. Organização do documento**



**MS-1 Conscientização/**

**Supervisão de segurança executiva p. 7**

**As melhores práticas são organizadas de acordo com o Modelo de segurança de conteúdos da MPAA, que fornece uma estrutura para avaliar a capacidade de uma unidade de proteger o conteúdo de um cliente. É composto de tópicos de segurança em três áreas: sistema de gestão, segurança física e segurança digital. Os componentes do Modelo de segurança de conteúdos da MPAA são extraídos de normas ISO (27001-27002), normas de segurança (ou seja, NIST, CSA, ISACA e SANS) e melhores práticas da indústria.**

**MS-2 Gestão de risco p. 7**

**MS-3 Organização de segurança p. 8**

**MS-4 Políticas e procedimentos p. 9**

**MS-5 Resposta a incidentes p. 12**

**MS-6 Continuidade de negócios e Recuperação de desastres p. 14**

**MS-7 Controle de alterações e Gestão de configuração p. 15**

**MS-8 Fluxo de trabalho p. 15**

**MS-9 Segregação de funções p. 16**

**MS-10 Verificações de antecedentes p. 17**

**MS-11 Acordos de confidencialidade p. 17**

**MS-12 Uso e triagens de terceiros p. 18**

**PS-1 Pontos de entrada/saída p. 20**

**PS-2 Entrada/Saída de visitante p. 21**

**PS-3 Identificação p. 22**

**PS-4 Segurança do perímetro p. 22**

**PS-5 Alarmes p. 23**

**PS-5 Autorização p. 25**

**PS-8 Chaves p. 26**

**PS-9 Câmeras p. 28**

**PS-7 Controle de acesso eletrônico p. 25**

**PS-10 Registro e monitoramento p. 29**

**PS-11 Revistas p. 30**

**Gestão de ativos**

**PS-12 Controle de inventário p. 33**

**PS-13 Contagens de inventário p. 34**

**PS-14 Rastreamento de mídia em branco/matérias-primas p. 35**

**PS-15 Ativos de clientes p. 35**

**PS-16 Descarte p. 36**

**PS-17 Expedição p. 38**

**PS-18 Recebimento p. 39**

**PS-19 Rotulagem p. 40**

**PS-20 Acondicionamento p. 40**

**PS-21 Veículos de transporte p. 41**

**DS-1 Firewall/WAN/**

**Segurança do perímetro p. 42**

**DS-2 Internet p. 46**

**DS-3 LAN/Rede interna p. 48**

**DS-4 Sem fio p. 51**

**DS-5 Segurança do dispositivo de I/O**

**p. 53**

**DS-6 Sistema de segurança p. 53**

**DS-7 Gestão de contas p. 56**

**DS-7.7-8.4 Autenticação p. 58-60**

**DS-9 Registro e monitoramento p. 61**

**Gerenciamento de conteúdos**

**DS-10 Segurança móvel p. 63**

**Transferência de conteúdos**

**DS-11 Técnicas de segurança p. 65**

**DS-12 Controle de conteúdo p. 67**

**DS-13 Sistemas de transferência p. 68**

**DS-14 Metodologia do dispositivo de transferência p. 68**

**DS-15 Portal do cliente p. 70**

1. Formato de melhores práticas

As melhores práticas são apresentadas para cada tópico de segurança listado no Modelo de segurança de conteúdos da MPAA usando o seguinte formato:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sistema de gestão | Segurança física | | | Segurança digital | | |
| Organização e gestão | Unidade | Gestão de ativos | Transporte | Infraestrutura | Gerenciamento de conteúdos | Transferência de conteúdos |

O gráfico na parte superior de todas as páginas destaca a área de segurança sendo tratada no Modelo geral de segurança de conteúdos da MPAA.

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| PS-9.0 | Chaves | Limitar a distribuição de **chaves mestras** para pessoal autorizado apenas (por exemplo, o proprietário, administração das unidades) | * Manter uma lista de **pessoal da empresa** que tem permissão para verificar **chaves mestras** * Atualizar a lista regularmente para remover todo o **pessoal da empresa**, que não precisa mais de acesso a **chaves mestras** |
| PS-9.1 | Implementar um processo de check-in/check-out para acompanhar e controlar a distribuição de **chaves mestras** | * Manter registros para rastrear as seguintes informações: * **Pessoal da empresa** em posse de cada **chave mestra** * Horário de check-out/check-in * Motivo para check-out |

P

**Glossário**

Todos os termos que estão incluídos no glossário são destacados em **negrito**e definidos no Anexo A.

**Orientações para implementação**

Considerações adicionais, etapas de implementação potenciais e exemplos são fornecidos para ajudar as organizações a implementar as melhores práticas.

**Melhores práticas**

As melhores práticas são apresentadas para cada Tópico de segurança.

**Tópico de segurança**

Cada área de capacidade é composta de um ou mais "Tópicos de segurança". Cada Tópico de segurança é abordado com uma ou mais das melhores práticas.

**N.º**

A cada melhor prática é atribuído um número de referência na forma de XX-Y.Z. XX para a área geral, Y para o Tópico de segurança, e Z para o controle específico.

1. Diretrizes comuns das melhores práticas

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| MS-1.0 | Conscientização/Supervisão de segurança executiva | Estabelecer um sistema de gestão de segurança de informação que implementa uma estrutura de controle para segurança da informação, que é aprovado pelo(s) proprietário(s)/alta administração. | * por ex., estrutura de ISMS do ISO27001, NIST, CoBIT, etc. |
| MS-1.1 | Analisar as políticas e processos de gestão de segurança da informação pelo menos anualmente. |  |
| MS-1.2 | Treinar e envolver a gerência executiva/proprietário(s) nas responsabilidades do negócio para proteger os conteúdos pelo menos anualmente. |  |
| MS-1.3 | Criar um grupo de gestão de segurança da informação para estabelecer e analisar as políticas de gestão de segurança da informação. |  |
| MS-2.0 | Gestão de risco | Desenvolver um processo formal e documentado de avaliação de risco da segurança focado em fluxos de trabalho de conteúdos e em bens sensíveis, a fim de identificar e priorizar os riscos de roubo e de vazamento de conteúdos que sejam relevantes para a unidade. | * Definir uma margem clara para a **avaliação de risco de segurança e modificar conforme for necessário** * Incorporar uma abordagem sistemática que utiliza probabilidade de ocorrência de risco, impacto na proteção aos conteúdos/objetivos de negócio e classificação de ativos para atribuir prioridade * Consultar MS-6.0 quanto às melhores práticas relacionadas aos **fluxos de trabalho** documentados |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| MS-2.1 | Gestão de risco | Conduzir uma **avaliação de risco** interna anualmente e nas principais mudanças no fluxo de trabalho — baseadas no mínimo, nas Diretrizes comuns de melhores práticas da MPAA e nas Diretrizes complementares aplicáveis — e documentar e agir de acordo com os riscos identificados. | * Realizar reuniões com a administração e as principais partes interessadas, pelo menos trimestralmente, para identificar e documentar os riscos de roubo e vazamento de conteúdos * Conduzir varreduras de vulnerabilidade de rede externa e interna e testes de penetração externa trimestralmente, de acordo com DS-1.8 e DS-1.9 * Identificar os riscos-chave que refletem onde a unidade acredita que as perdas de conteúdos podem ocorrer * Implementar e documentar os controles para mitigar ou reduzir os riscos identificados * Monitorar e avaliar a eficácia dos esforços de remediação e controles implementados pelo menos trimestralmente * Documentar e executar o orçamento para as iniciativas de segurança, atualizações e manutenção |
| MS-3.0 | Organização de segurança | Identificar o(s) ponto(s)-chave de segurança de contato e formalmente definir papéis e responsabilidades de proteção de conteúdos e de ativos. | * Preparar organogramas e descrições de funções para facilitar a designação de papéis e responsabilidades no que se refere à segurança de conteúdos * Fornecer treinamento on-line ou presencial para preparar o pessoal de segurança em políticas e procedimentos que sejam relevantes para sua função |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| MS-4.0 | Políticas e procedimentos | Estabelecer políticas e procedimentos relativos à segurança de ativos e conteúdos; as políticas devem abordar os seguintes tópicos, no mínimo:   * Uso aceitável (por exemplo, redes sociais, Internet, telefone, dispositivos pessoais, dispositivos móveis, etc.) * Políticas de classificação e tratamento de ativos e conteúdos * Continuidade de negócios (backup, retenção e restauração) * Política de gestão de controle e configuração de alterações * Política de confidencialidade * Dispositivos digitais de gravação (por exemplo, smartphones, câmeras digitais, filmadoras) * Política de exceção (por exemplo, o processo de documentar os desvios da política) * Política de resposta a incidentes * Política de dispositivos móveis * Políticas de rede, internet e rede sem fio * Controles de senha (por exemplo, o tamanho mínimo da senha, proteção de tela) * Política de segurança * Política de visitantes * Política disciplinar/de sanções * Método anônimo interno para comunicar pirataria ou utilização incorreta de conteúdo (por ex., linha direta telefônica ou e-mail) | * Considerar fluxos de trabalho específicos da unidade/segmento no desenvolvimento de políticas e procedimentos. * Exigir que a administração assine todas as políticas e procedimentos antes de serem publicadas e liberadas * Comunicar medidas disciplinares em treinamento de orientação de novos contratados * Consultar o Anexo F para ter a lista de políticas e procedimentos a considerar |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| MS-4.1 | Políticas e procedimentos | Revisar e atualizar as políticas e procedimentos de segurança, pelo menos anualmente. | * Incorporar os seguintes fatores na revisão anual de gestão de políticas e procedimentos de segurança: * Tendências recentes de segurança * Feedback de pessoal da empresa * Novas ameaças e vulnerabilidades * Recomendações de órgãos reguladores (ou seja, FTC etc.) * Incidentes de segurança anteriores |
| MS-4.2 | Comunicar e exigir uma assinatura de todo o **pessoal da empresa** (por exemplo, funcionários, funcionários temporários, estagiários) e **funcionários terceirizados** (por exemplo, empreiteiros, profissionais liberais, agências de temporários) para todas as políticas, procedimentos e/ou requisitos de clientes. | * Distribuir cópias do manual da empresa contendo todas as políticas e procedimentos gerais após a contratação de novo **pessoal da empresa** e **funcionários terceirizados** * Avisar o **pessoal da empresa** e os **funcionários terceirizados** sobre atualizações das políticas, procedimentos e requisitos dos clientes * A administração deve manter a assinatura das políticas, procedimentos e requisitos dos clientes atuais para todo **pessoal da empresa** e **funcionários terceirizados** |
| MS-4.3 | Políticas e procedimentos | Desenvolver e atualizar regularmente um programa de conscientização sobre políticas e procedimentos de segurança e treinar o **pessoal da empresa** e **funcionários terceirizados** no ato da contratação e anualmente depois disso sobre políticas e procedimentos de segurança, tratando no mínimo das áreas seguintes:   * Políticas e procedimentos de segurança de TI * Segurança e tratamento de conteúdos/ativos em geral e requisitos específicos dos clientes * Relatórios e escalonamento de incidentes de segurança * Política disciplinar * Criptografia e gestão de chaves para todas as pessoas que lidam com conteúdo criptografado * Processos de descarte e destruição de ativos | * Comunicar mensagens de conscientização de segurança durante reuniões da administração/equipe * Implementar procedimentos para acompanhar quais **funcionários da empresa** concluíram o treinamento de segurança anual (por ex., repositório de dados, registros de participantes, certificados de conclusão) * Fornecer treinamento on-line ou presencial no ato da contratação para instruir o **pessoal da empresa** e **funcionários terceirizados** sobre incidentes comuns, riscos correspondentes e as responsabilidades deles para relatar incidentes detectados * Distribuir materiais de conscientização de segurança como cartazes, e-mails e boletins periódicos para incentivar a conscientização de segurança * Desenvolver mensagens adaptadas e treinamento com base nas responsabilidades de trabalho e interação com conteúdo sensível (por ex., pessoal de TI, produção) para mitigar problemas de pirataria * Considerar gravar as sessões de treinamento e disponibilizar as gravações para referência |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| MS-5.0 | Resposta a incidentes | Estabelecer um plano formal de resposta a incidentes que descreva as ações a serem tomadas quando um incidente de segurança for detectado e informado. | * Considerar a inclusão das seguintes seções no plano de **resposta a incidentes**: * Definição de incidente * Aviso da equipe de segurança * Escalada para a administração * Análise do impacto e prioridade * Contenção de impacto * Erradicação e recuperação * Informações de contatos importantes, incluindo informações de contato do estúdio do cliente * Notificação de parceiros de negócios e clientes afetados * Notificação dos oficiais da lei * Relatório de detalhes do incidente * Consultar NIST SP800-61 revisão 2 sobre o tratamento de incidentes de segurança informática |
| MS-5.1 | Identificar a equipe de resposta a incidentes de segurança, que será responsável por detectar, analisar e remediar incidentes de segurança. | * Incluir representantes de diferentes funções empresariais, a fim de tratar incidentes de segurança de todos os tipos; considerar o seguinte: * Administração * Segurança física * Segurança da informação * Equipe de rede * Recursos humanos * Jurídico * Oferecer treinamento para que os membros da equipe de **resposta a incidentes** entendam suas funções e responsabilidades ao lidar com incidentes |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| MS-5.2 | Resposta a incidentes | Estabelecer um processo de comunicação de incidentes de segurança para os indivíduos relatarem os incidentes detectados para a equipe de **resposta a incidentes** de segurança. | * Considerar a implementação de uma linha direta anônima ou site que possam ser usado para relatar atividade imprópria e/ou suspeita * Considerar a implementação de um e-mail do grupo para a comunicação de incidentes que informaria todos os membros da equipe de resposta a incidentes * Considerar aproveitar a linha direta de denúncias da MPAA para denúncias anônimas sobre atividades suspeitas – consultar as informações de contato da linha direta de denúncias 24 horas no Anexo H |
| MS-5.3 | Comunicar incidentes prontamente aos clientes, cujos conteúdos possam ter sido vazados, roubados ou comprometidos (por exemplo, ativos de clientes em falta), e realizar uma reunião de pós-mortem com a administração e o cliente. | * Implementar um processo de notificação de violação de segurança, incluindo o uso de formulários de notificação de violação * Envolver a equipe jurídica para determinar as ações corretas a tomar para relatar a perda de conteúdos para clientes afetados * Discutir as lições aprendidas com o incidente e identificar melhorias para o plano e processo de resposta a incidentes * Realizar análise de causa raiz para identificar vulnerabilidades de segurança que permitiram que o incidente ocorresse * Identificar e implementar controles remediadores para evitar que incidentes semelhantes ocorram novamente * Comunicar os resultados do pós-mortem, incluindo o plano de ação corretiva, para os clientes afetados |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| MS-6.0 | Continuidade de negócios e Recuperação de desastres | Estabelecer um plano formal que descreva as ações a serem tomadas para assegurar a continuidade de negócios. | * Considerar a inclusão das seções seguintes no plano de **continuidade de negócios**: * Ameaças a ativos e conteúdos cruciais, incluindo perda de energia e telecomunicações, falha de sistemas, desastres naturais, etc. * Procedimentos detalhados de backup de sistema de informações, conteúdo e metadados e documento de sistema de informações, incluindo a configuração de dispositivos cruciais de WAN e LAN/rede interna * Criptografia de backups (no mínimo, criptografia AES 128 bits) * Suprimento de energia de emergência para suportar pelo menos 15 minutos para o sistema CFTV e sistemas de informações cruciais, incluindo software para realizar desligamento seguro dos sistemas cruciais * Considerar um local reserva fora do local * Aviso da equipe de segurança * Escalada para a administração * Análise do impacto e prioridade * Contenção de impacto * Prioridades para a recuperação e procedimentos de recuperação detalhados, incluindo alternativas manuais e detalhes de configuração dos sistemas restaurados * Principais informações de contato * Notificação de parceiros de negócios e clientes afetados * Testes dos processos de continuidade de negócios e de recuperação de desastres pelo menos anualmente |
| MS-6.1 | Identificar a equipe de continuidade de negócios que será responsável por detectar, analisar e corrigir os incidentes de continuidade. | * Incluir funções e responsabilidades definidas * Fornecer treinamento, de modo que os membros da equipe de continuidade de negócios entendam suas funções e responsabilidades |
| MS-7.0 | Controle de alterações e Gestão de configuração | Estabelecer políticas e procedimentos para assegurar que novos dados, aplicativos, rede e componentes de sistemas foram aprovados previamente pela liderança de negócios. | * Incluir a documentação que descreve a instalação, configuração e uso dos dispositivos, serviços e recursos e atualizar a documentação conforme necessário * Documentar as políticas e procedimentos para lidar com problemas conhecidos * Incluir políticas e procedimentos para comunicação de bugs e vulnerabilidades de segurança * Restringir e monitorar a instalação de hardware ou software não autorizado * Gerenciar os riscos associados com alterações de dados, aplicativos, infraestrutura de rede e sistemas * Documentar e manter todas as solicitações de alteração, resultado de teste e aprovações de gestão |
| MS-8.0 | Fluxo de trabalho | Documentar **fluxos de trabalho** controlando conteúdo e pontos de verificação de autorização. Incluir os processos seguintes para conteúdo físico e digital:   * Entrega (recebimento/devolução) * Inserir * Movimento * Armazenamento * Remoção/destruição | * Usar diagramas de pista de oscilação para documentar **fluxos de trabalho** * Incluir ativos de processamento e tratamento da informação, quando aplicável * Avaliar cada ponto de contato quanto a riscos ao conteúdo * Implementar controles em torno de postos de controle de autorização * Identificar controles de aplicativos relacionados |
| MS-8.1 | Atualizar o **fluxo de trabalho** quando houver alterações no processo e analisar o processo do **fluxo de trabalho** pelo menos anualmente para identificar alterações. | * Seguir o **fluxo de trabalho** de conteúdos e os controles implementados para cada processo, a fim de determinar as áreas de vulnerabilidade |
| MS-9.0 | Segregação de funções | Segregar as funções no **fluxo de trabalho** de conteúdos. Implementar e documentar os controles de compensação quando a segregação não for prática. | * Documentar papéis e responsabilidades para eliminar a sobreposição de funções de cargo baseadas em papéis, tais como: * **Pessoal da câmara** e da sala de servidor/máquina * Pessoal de envio e recebimento * Movimento de ativos dentro da unidade (por exemplo, mensageiros) da **câmara** e área de conteúdos/produção * **Acesso à pasta de ativos digitais** (por exemplo, o argumentador de dados define o acesso para o produtor) * Transferência de pessoal de conteúdos do pessoal de produção * Segregar funções usando controles manuais (por exemplo, a aprovação do produtor antes de trabalhar no conteúdo) ou controles automáticos no sistema de ordenação de trabalho (por exemplo, a aprovação automática para cada etapa do **fluxo de trabalho**) * Implementar controles de compensação quando a segregação é inatingível, tais como: * Monitorar a atividade do pessoal da empresa e/ou de funcionários terceirizados * Manter e analisar os registros de auditoria * Implementar segregação física * Impor um controle de gestão |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| MS-10.0 | Verificações de antecedentes | Executar verificações de triagem de antecedentes em todos os **funcionários da empresa** e **funcionários terceirizados**. | * Realizar verificações de antecedentes de acordo com as leis, regulamentos, estatutos de sindicatos e considerações culturais pertinentes * Fazer triagem dos potenciais **funcionários da empresa** e **funcionários terceirizados** por meio de verificações de triagem de antecedentes que são proporcionais aos requisitos de negócio, à sensibilidade do conteúdo que será acessado, e possíveis riscos de roubo ou vazamento de conteúdos * Executar verificações de identidade, acadêmicas e de qualificação profissional quando necessário * Se as verificações de antecedentes não forem permitidas por lei, documentar como uma exceção e usar verificação de referências |
| MS-11.0 | Acordos de confidencialidade | Exigir que todos os **funcionários da empresa** assinem um acordo de confidencialidade (por exemplo, de não divulgação) na contratação e depois anualmente, que inclua requisitos de manipulação e proteção de conteúdos. | * Incluir orientações de não divulgação relacionadas à confidencialidade após a rescisão de seu contrato ou acordo de trabalho * Explicar a importância da confidencialidade/não divulgação em termos não jurídicos, conforme necessário * Garantir que todas as informações relevantes em equipamentos utilizados pelo **pessoal da empresa** para controlar o conteúdo sensível relacionado a negócios sejam transferidas para a organização e removidas do equipamento com segurança * A administração deve manter os acordos de confidencialidade assinados por todo o **pessoal da empresa** |
| MS-11.1 | Exigir que todos os **funcionários da empresa** devolvam todos os conteúdos e as informações do cliente em sua posse após a demissão ou rescisão de contrato. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| MS-12.0 | Uso e triagem de terceiros | Exigir que todos os **funcionários terceirizados** (por exemplo, freelancers) que lidam com conteúdo assinem acordos de confidencialidade (por exemplo, de não divulgação) na contratação. | * Incluir orientações de não divulgação nas políticas relacionadas à confidencialidade durante o período de seu contrato ou acordo de trabalho e após a sua rescisão * Explicar a importância da confidencialidade/não divulgação em termos não jurídicos, conforme necessário * Garantir que todas as informações relevantes em equipamentos utilizados pelos **funcionários terceirizados** para controlar o conteúdo sensível relacionado a negócios sejam transferidas para a organização e removidas do equipamento com segurança * A administração deve manter os acordos de confidencialidade assinados por todos os **funcionários terceirizados** * Incluir requisitos para manipulação e proteção de conteúdos |
| MS-12.1 | Exigir que todos os **funcionários terceirizados** devolvam todos os conteúdos e as informações do cliente em sua posse após a rescisão de seu contrato. |  |
| MS-12.2 | Incluir requisitos de segurança em contratos de terceiros. | * Exigir que os **funcionários terceirizados** cumpram os requisitos de segurança especificados nos contratos de terceiros e nos requisitos do cliente * Incluir uma cláusula de direito de auditoria para as atividades que envolvem o conteúdo sensível * Implementar um processo para monitorar a conformidade com os requisitos de segurança |
| MS-12.3 | Implementar um processo para recuperar **conteúdos** quando os vínculos laborais terminarem. | * Garantir que todos os **conteúdos** em equipamentos de terceiros sejam transferidos para a organização e removidos do equipamento com segurança |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| MS-12.4 | Uso e triagem de terceiros | Exigir que os **funcionários terceirizados** sejam vinculados e segurados quando necessário (por exemplo, serviço de courier). | * Exigir que os **funcionários terceirizados** mostrem a prova de seguros e mantenham um registro de sua empresa de seguros e o número da apólice * Exigir que um seguro de terceiros atenda a um determinado nível de cobertura * Exigir a atualização anual das informações quando os contratos forem renovados |
| MS-12.5 | Restringir o acesso de terceiros a áreas de conteúdos/produção a não ser que seja necessário para sua função laboral. | * Garantir que os **funcionários terceirizados** não tenham acesso eletrônico às áreas que abrigam conteúdo * Acompanhar **funcionários terceirizados** (por exemplo, equipes de limpeza) quando o acesso a áreas restritas (por exemplo, **caixa-forte**) for necessário |
| MS-12.6 | Notificar os clientes se **subcontratados** forem usados para manipular conteúdos ou o trabalho for transferido para outra empresa. | * Exigir assinatura/aprovação por escrito do cliente * Exigir que os subcontratados passem por atividades de **diligência devida** padrão * O trabalho transferido para outra empresa deve ser comunicado para os estúdios membros da MPAA e o questionário de fornecedor da MPAA deve ser respondido e fornecido aos estúdios membros para a diligência devida deles. |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| PS-1.0 | Pontos de entrada/saída | Sempre proteger todos os pontos de entrada/saída da unidade, incluindo as portas e janelas das docas de carga. | * Autorizar que os pontos de entrada/saída sejam desbloqueados durante o horário comercial, se a área de recepção for separada do resto da unidade com portas de acesso controlado |
| PS-1.1 | Controlar o acesso às áreas em que conteúdos são manipulados através da segregação da área de conteúdos de outras áreas da unidade (por exemplo, escritórios administrativos, salas de espera, docas de carga, áreas de coleta e entrega do courier, replicação e masterização). | * Permitir acesso a áreas de conteúdo/produção com base na necessidade de saber * Exigir que as salas utilizadas para fins de exibição sejam de acesso controlado (por exemplo, cabines de projeção). * Limitar o acesso a salas onde os participantes de **mídia** estejam presentes (por exemplo, Blu-ray, DVD) * Impor um modelo de segregação de funções que restrinja uma única pessoa de ter acesso tanto às salas de replicação quanto de masterização |
| PS-1.2 | Controlar o acesso onde houver empresas co-instaladas em uma unidade, o que inclui, entre outros, o seguinte:   * Segregação das áreas de trabalho * Implementação de entradas e saídas com acesso controlado que possam ser segmentadas por unidade de negócios * Registro e monitoramento de todas as entradas e saídas na unidade * Todos os inquilinos na unidade devem ser comunicados ao cliente antes da contratação |  |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| PS-2.0 | Entrada/Saída de visitante | Manter registro detalhado dos visitantes e incluir o seguinte:   * Nome * Empresa * Hora de entrada/Hora de saída * Pessoa/pessoas visitadas * Assinatura do visitante * Número de crachá atribuído | * Verificar a identidade de todos os visitante obrigando-os a apresentar documento de identificação com foto válido (por exemplo, carteira de motorista ou identificação emitida pelo governo) * Considerar esconder os nomes dos visitantes anteriores |
| PS-2.1 | Atribuir um **crachá de identificação** ou adesivo, que deve ficar visível em todos os momentos, para cada visitante e coletar os crachás na saída. | * Fazer crachás de visitantes facilmente distinguíveis de crachás do **pessoal da empresa** (por exemplo, crachás de plástico com código de cores) * Considerar uma rotatividade diária da cor dos crachás de papel ou das etiquetas * Considerar o uso de crachás que mudam de cor ao expirar * Registrar atribuições do crachá na entrada/saída * Os crachás de visitantes devem ser numerados sequencialmente e monitorados * Contabilizar os crachás diariamente |
| PS-2.2 | Não fornecer aos visitantes acesso com cartão chave às áreas de conteúdos/produção. |  |
| PS-2.3 | Exigir que os visitantes sejam acompanhados por funcionários autorizados, enquanto no local, ou nas áreas de conteúdos/produção. |  |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| PS-3.0 | Identificação | Fornecer ao **pessoal da empresa** e aos **funcionários terceirizados** de longo prazo (por exemplo, limpeza) **crachá de** **identificação** com foto e que deve ficar visível em todos os momentos. | * Emitir um **crachá de identificação** com foto para todo **pessoal da empresa** e **funcionários terceirizados** de longo prazo depois de uma verificação de antecedentes ser concluída * Estabelecer e implementar um processo para recuperar o **crachá de identificação** com foto imediatamente após a rescisão * Considerar a omissão da localização, nome da empresa, logotipo e outras informações específicas no **crachá de identificação** com foto * Considerar o uso do **crachá de identificação** com foto como o cartão chave de acesso, sempre que possível * Exigir que os funcionários comuniquem imediatamente a perda ou roubo dos **crachás de identificação com foto** * Fornecer um número de telefone ou site que funcione 24 horas, sete dias por semana, para informar a perda ou roubo dos **crachás de identificação com foto** * Treinar e incentivar os funcionários a contestarem pessoas sem identificação visível |
| PS-4.0 | Segurança do perímetro | Implementar controles de segurança do perímetro que tratam dos riscos aos quais a unidade pode ser exposta quando identificada pela **avaliação de risco** da organização. | * Implementar controles de segurança com base na localização e layout da unidade, tais como: * Restringir o acesso do perímetro com o uso de paredes, cercas e/ou portas que, pelo menos, sejam seguras após o expediente; paredes/cercas devem ter 2,40 m ou mais * Proteger e fechar, se necessário, áreas externas comuns, tais como as zonas de fumantes e varandas abertas * Fazer a cobertura da câmera externa suficiente em torno das áreas exteriores comuns (por exemplo, áreas de fumantes) e do estacionamento * Ter conhecimento do uso excessivo de placas de sinalização da empresa que possa criar pontos alvo * Usar alarmes em torno do perímetro, conforme necessário |
| PS-4.1 | Colocar guardas de segurança nas entradas do perímetro e em pontos de entrada/saída não-emergenciais. |  |
| PS-4.2 | Segurança do perímetro | Implementar um processo de patrulha diária de segurança com cronograma aleatório e documentar os resultados de patrulha em um registro. | * Exigir que os guardas de segurança patrulhem áreas externas e internas * Incluir uma análise das saídas de emergência, incluindo a verificação de vedações * Considerar o uso de um sistema de patrulhamento da guarda para acompanhar o patrulhamento (por exemplo, ponto de inspeção) e verificar fechaduras |
| PS-4.3 | Sempre trancar os portões do perímetro. | * Implementar uma cancela eletrônica, controlada por pessoal de segurança, para controlar o acesso de veículos à unidade * Distribuir licenças de estacionamento para o pessoal da empresa e de terceiros que tenham concluído a documentação necessária * Exigir que os veículos de visitantes apresentem documento de identificação e garantir que todos os visitantes tenham sido pré-autorizados a entrar nas unidades |
| PS-5.0 | Alarmes | Instalar um sistema de alarme sonoro centralizado que abranja todos os pontos de entrada/saída (incluindo as saídas de emergência), janelas, docas de carga, saídas de incêndio e áreas restritas (por exemplo, **caixa-forte**, sala de servidor/máquina, etc.). | * Colocar alarmes em cada entrada para alertar o pessoal de segurança sobre entrada não autorizada na unidade * Ativar o alarme quando a unidade estiver sem supervisão |
| PS-5.1 | Instalar e posicionar de maneira eficaz detectores de movimento em áreas restritas (por exemplo, **caixa-forte**, sala de servidor/máquina etc.) e configurá-los para alertar o pessoal de segurança e outros funcionários apropriados (por exemplo, gerentes de projetos, produtor, editor-chefe, equipe de resposta a incidentes, etc.). | * Verificar se o sistema de alarme abrange áreas de armazenamento e **caixas-fortes** (por exemplo, através de sensores de movimento), após o horário comercial normal, como uma camada adicional de segurança |
| PS-5.2 | Instalar alarmes de suporte de porta em áreas restritas (por exemplo, caixa-forte, sala de servidor/máquina, etc.) para notificar quando pontos sensíveis de entrada/saída são abertos por mais tempo do que um período pré-determinado (por exemplo, 60 segundos). | * Configurar portas de acesso controlado para disparar alarmes e alertar o pessoal de segurança quando as portas forem mantidas abertas por um período de tempo prolongado |
| PS-5.3 | Alarmes | Configurar os alarmes para fornecer notificações de escalação diretamente ao pessoal encarregado pela segurança e outros funcionários (por exemplo, gerentes de projetos, produtor, editor-chefe, equipe de resposta a incidentes, etc.). | * Estabelecer e implementar procedimentos de escalonamento a serem seguidos se uma resposta oportuna não for recebida do pessoal de segurança após a notificação * Considerar a implementação de notificação automática de execução da lei em caso de violação * Implementar procedimentos de notificação nos finais de semana e após o horário comercial |
| PS-5.4 | Atribuir códigos de armar e desarmar exclusivos a cada pessoa que requeira o acesso ao sistema de alarme e restringir o acesso a todas as outras equipes de pessoal. | * Usar códigos de alarme exclusivos para controlar qual pessoal de segurança foi responsável por armar/desarmar o alarme * Atualizar os códigos de alarme atribuídos em um intervalo aprovado pela administração, a fim de reduzir o risco envolvido com o compartilhamento e perda de códigos |
| PS-5.5 | Analisar a lista de usuários que podem armar e desarmar os sistemas de alarmes trimestralmente ou depois de alteração de pessoal. | * Remover usuários que deixaram a empresa ou mudaram as funções de trabalho * Desativar os códigos de alarme que foram atribuídos aos usuários removidos |
| PS-5.6 | Testar o sistema de alarmes trimestralmente. | * Simular uma violação de segurança física e garantir o seguinte: * Sistema de alarme detecta a violação * O pessoal de segurança é alertado * O pessoal de segurança responde em tempo hábil de acordo com os procedimentos |
| PS-5.7 | Implementar medidas de segurança contra incêndio, de modo que no caso de uma falta de energia, as portas corta-fogo fiquem abertas e todas as outras fechadas para impedir o acesso não autorizado. |  |
| PS-6.0 | Autorização | Documentar e implementar um processo para gerenciar acesso à unidade e manter registros de todas as alterações aos **direitos de acesso**. | * Designar uma pessoa para autorizar o acesso à unidade * Notificar o pessoal adequado (por exemplo, gerência da unidade) sobre as mudanças no estatuto de funcionário * Criar um formulário físico ou eletrônico que deve ser preenchido por um supervisor para solicitar acesso à unidade para o **pessoal da empresa** e/ou **funcionários terceirizados** * Atribuir a responsabilidade de investigar e aprovar as solicitações de acesso |
| PS-6.1 | Restringir o acesso a sistemas de produção somente ao pessoal autorizado. |  |
| PS-6.2 | Revisar o acesso a áreas restritas (por exemplo, **caixa-forte**, sala de servidor/máquina) trimestralmente e quando os papéis ou situação de emprego do **pessoal da empresa** e/ou **funcionários terceirizados** forem alterados. | * Validar a situação de pessoal da empresa e dos funcionários terceirizados * Remover os direitos de acesso dos usuários com contrato rescindido * Verificar se o acesso continua a ser apropriado para a função associada aos usuários |
| PS-7.0 | Controle de acesso eletrônico | Implementar o acesso eletrônico em toda a unidade para cobrir todos os pontos de entrada/saída e todas as áreas onde o conteúdo é armazenado, transmitido ou processado. | * Atribuir o acesso eletrônico a áreas específicas da unidade com base na função e responsabilidades de trabalho * Atualizar o acesso eletrônico de acordo quando os papéis mudarem ou após a rescisão do pessoal da empresa e dos funcionários terceirizados * Manter um registro que mapeie o número de dispositivos de acesso eletrônico ao pessoal da empresa * Consultar Registro e monitoramento PS-10.0 * Analisar os momentos em que o acesso eletrônico não é necessário para as áreas comuns (por exemplo, elevadores públicos). |
| PS-7.1 | Controle de acesso eletrônico | Restringir a administração do sistema de acesso eletrônico ao pessoal apropriado. | * Restringir a administração do sistema eletrônico ao pessoal designado e não permitir que as pessoas que têm acesso ao conteúdo de produção executem tarefas administrativas de acesso eletrônico * Atribuir uma equipe independente para administrar e gerenciar o acesso eletrônico |
| PS-7.2 | Armazenar o estoque de cartões e os **dispositivos de acesso eletrônico** (por exemplo, cartões de acesso, chaves de segurança) em um armário fechado e garantir que os **dispositivos de acesso eletrônico** permaneçam desativados antes de serem atribuídos ao pessoal. Armazenar dispositivos de acesso eletrônico não atribuídos (por exemplo, cartões de acesso, chaves de segurança) em um armário fechado e garantir que permaneçam desativados antes de serem atribuídos ao pessoal. | * Limitar o acesso ao armário fechado à equipe de administração do sistema de **cartões de acesso**/**dispositivo de acesso eletrônico** * Exigir sign-out para a remoção de estoque |
| PS-7.3 | Desativar **dispositivos de acesso** eletrônico perdidos(por exemplo, cartões de acesso, chaves de segurança) no sistema antes de emitir um novo **dispositivo de acesso eletrônico**. | * Educar o **pessoal da empresa** e os **funcionários terceirizados** a relatar **dispositivos de acesso eletrônico** perdidos imediatamente para evitar o acesso não autorizado à unidade * Exigir a identificação antes de emitir **dispositivos de acesso eletrônicos** de substituição |
| PS-7.4 | Emitir **dispositivo de acesso eletrônico** para acesso de terceiros, com uma data de validade definida (por exemplo, 90 dias) com base em um calendário aprovado. | * Assegurar que os **dispositivos de acesso eletrônico** **de terceiros** sejam facilmente distinguíveis dos dispositivos de acesso eletrônico **do pessoal da empresa** * Certificar-se de que a data de validade é facilmente identificável nos **dispositivos de acesso eletrônico** * Atribuir o acesso aos dispositivos de acesso eletrônico de **terceiros** com base na necessidade de saber |
| PS-8.0 | Chaves | Limitar a distribuição de **chaves mestras** para pessoal autorizado apenas (por exemplo, o proprietário, administração das unidades). | * Manter uma lista de **pessoal da empresa** que tem permissão para verificar **chaves mestras** * Atualizar a lista regularmente para remover todo o **pessoal da empresa**, que não precisa mais de acesso a **chaves mestras** |
| PS-8.1 | Implementar um processo de check-in/check-out para acompanhar e controlar a distribuição de **chaves mestras** e/ou chaves para áreas restritas. | * Manter registros para rastrear as seguintes informações: * **Pessoal da empresa** em posse de cada chave mestra * Horário de check-out/check-in * Motivo para check-out * Exigir que **chaves mestras** sejam devolvidas dentro de um determinado período de tempo e investigar a localização de chaves que não foram devolvidas no prazo |
| PS-8.2 | Usar chaves que só possam ser copiadas por um chaveiro específico para pontos de entrada/saída exteriores. | * Usar chaves de alta segurança (cilindros), que oferecem um maior grau de resistência a quaisquer duas ou mais das seguintes ações: * Picagem * Moldagem * Duplicação de chave * Perfuração * Outras formas de entrada forçada |
| PS-8.3 | Inventariar **chaves mestras** e chaves para áreas restritas, incluindo pontos de entrada/saída da instalação, trimestralmente. | * Identificar, investigar e solucionar todas as chaves desaparecidas (perdidas/roubadas) * Analisar os registros para determinar quem fez check-out por último de uma chave cujo paradeiro se desconhece * Mudar as fechaduras quando **chaves mestras** ou chaves para áreas restritas estiverem faltando ou cujo paradeiro se desconhece |
| PS-8.4 | Obter todas as chaves de funcionários/terceiros com contrato rescindido ou aqueles que não precisarem mais de acesso. |  |
| PS-8.5 | Chaves | Implementar o controle de acesso eletrônico ou ou trocar as chaves de toda a unidade quando chaves-mestras ou chaves-mestras substitutas forem perdidas ou estiverem desaparecidas. |  |
| PS-9.0 | Câmeras | Instalar um sistema de **CFTV** que registra todos os pontos de entrada/saída da instalação e áreas restritas (por exemplo, sala de servidor/máquinas etc.). | * Cabos e fiação de câmeras devem ser discretamente escondidos e não ficar ao alcance * A unidade não deve presumir que o CFTV fornecido pelo prédio é adequado * Colocar as câmeras em todas as entradas da unidade * Garantir que as câmeras cubram as áreas de armazenamento e **caixas-forte** |
| PS-9.1 | Revisar o posicionamento das câmeras e registros para assegurar a cobertura, função, qualidade de imagem, condições de iluminação e taxa de quadros das imagens adequadas de vigilância, pelo menos diariamente. | * Analisar o posicionamento da câmera para garantir uma visão desobstruída de todos os pontos de entrada/saída e outras áreas sensíveis * Acomodar câmeras em áreas escuras (por exemplo, câmeras de baixa luminosidade ou infravermelho, luzes de detecção de movimento) * Analisar a qualidade de imagem para assegurar que a iluminação é adequada e que os rostos são distinguíveis * Analisar taxa de quadros para garantir que a atividade é gravada adequadamente * Posicionar as câmeras para evitar a captura de conteúdo em exibição * Gravar com resolução suficiente para ser possível identificar traços faciais * Gravar em uma taxa mínima de 7 quadros por segundo |
| PS-9.2 | Restringir o acesso físico e lógico ao **console** de **CFTV** e equipamentos de **CFTV** (por exemplo, DVRs) ao pessoal responsável pela administração/monitoramento do sistema. | * Colocar o equipamento de **CFTV** em um local de acesso controlado e seguro (por exemplo, sala de computador, armário fechado, gaiola) * Realizar revisões periódicas de acesso para garantir que somente os indivíduos apropriados tenham acesso a equipamentos de vigilância * Garantir que o console da Web para sistemas de **CFTV** baseados em IP seja restrito a pessoas autorizadas e que os controles de gestão de conta sólidos estejam em vigorando (por exemplo, a complexidade de senha, login de usuário individual, registro e monitoramento) |
| PS-9.3 | Câmeras | Certificar-se de que o registro de imagens da câmera inclui uma data precisa e marca de data/hora e retém imagens de vigilância de **CFTV** e dos registros de acesso eletrônico durante pelo menos 90 dias, ou o tempo máximo permitido por lei, em um local seguro. | * Gravar a hora e a data em **mídia** física relacionada à filmagem gravada em fita ou disco * Certificar-se de que marcas de data/hora precisas sejam mantidas no equipamento de gravação de imagens de câmera digital * Analisar dados e a marcação de hora quanto à precisão pelo menos semanalmente * Considerar armazenar os registros em um armário de telecomunicações de acesso controlado ou sala de informática * Determinar a quantidade típica de espaço necessário para um dia de registro e garantir que o tamanho do registro é grande o suficiente para manter os registros por pelo menos 90 dias, ou o período de retenção máximo permitido por lei * Considerar a retenção de imagens de vigilância de CFTV até a primeira data de lançamento da produção |
| PS-9.4 | Designar um funcionário ou grupo de funcionários para monitorar as imagens de vigilância durante o horário de funcionamento e investigar incidentes de segurança detectados imediatamente. | * Incorporar o processo de resposta a incidentes para lidar com incidentes de segurança * Considerar a adição de um monitor de vigilância na recepção ou no escritório de TI |
| PS-10.0 | Registro e monitoramento | Registrar e avaliar o acesso eletrônico a áreas restritas para eventos suspeitos pelo menos semanalmente. | * Identificar e documentar um conjunto de eventos que são considerados suspeitos * Considerar a implementação de um processo de comunicação automatizado que envia alertas em tempo real para o pessoal de segurança adequado quando atividade de acesso eletrônico suspeita for detectada * Mantes os registros por, no mínimo, um ano * Registrar e avaliar os seguintes eventos: * Tentativas repetidas de acesso com falha * Acesso em hora do dia incomum * Acesso sucessivo à porta em várias zonas |
| PS-10.1 | Registro e monitoramento | Registrar e analisar o acesso eletrônico, pelo menos diariamente, para as áreas seguintes:   * Caixa-forte de masters/marcadores * Premasterização * Sala de servidor/máquinas * Sala de sucata * Armações de alta segurança | * Identificar e documentar os eventos que são considerados incomuns * Considerar a implementação de um processo de comunicação automatizado que envia alertas em tempo real para o pessoal de segurança adequado quando atividade de acesso eletrônico suspeita for detectada. |
| PS-10.2 | Investigar atividades suspeitas de acesso eletrônico que forem detectadas. | * Identificar e comunicar os principais contatos que devem ser notificados após a detecção de atividade de acesso eletrônico incomum * Estabelecer e implementar procedimentos de escalação que devem ser seguidos se os contatos primários não responderem à notificação de eventos em tempo hábil |
| PS-10.3 | Manter um registro permanente de todos os incidentes de acesso eletrônico confirmados e incluir a documentação de todas as atividades de acompanhamento que foram tomadas. | * Aproveitar o formulário de relatório de **resposta a incidentes** para documentar incidentes confirmados com o **cartão de acesso/dispositivo de acesso eletrônico** * Analisar todos os incidentes recentes com o **cartão de acesso/ dispositivo de acesso eletrônico** periodicamente e realizar análise de causa raiz para identificar vulnerabilidades e correções apropriadas |
| PS-11.0 | Buscas | Estabelecer uma política, conforme permitido pelas leis locais, que permita que a segurança reviste aleatoriamente pessoas, bolsas, pacotes e itens pessoais para o conteúdo do cliente. | * Comunicar as políticas de revista a todos os **funcionários da empresa** e aos **funcionários terceirizados** * Realizar revistas periódicas ao **pessoal da empresa** e aos **funcionários terceirizados** para validar política |
| PS-11.1 | Buscas | Implementar um processo de revista à saída que seja aplicável a todo o pessoal da unidade e visitantes, incluindo:   * Remoção de todos os sobretudos, chapéus e cintos para inspeção * Remoção do conteúdo de todos os bolsos * Desempenho de uma autovarredura geral com a supervisão de segurança * Inspeção completa de todas as sacolas * Inspeção de bandeja de CD/DVD de notebooks * Varredura de indivíduos com um detector de metais portátil usado a cerca de sete centímetros do indivíduo revistado | * Instruir os guardas de segurança para procurarem itens que sejam proibidos de serem trazidos para o local (por exemplo, câmeras) ou materiais de filmes que não sejam permitidos de serem trazidos para a parte externa da unidade sem a devida autorização * Comunicar as políticas de revista de saída a todos os funcionários da empresa e aos funcionários de terceirizados * Escalonar mudanças de turno para evitar longas filas e tempos de espera longos |
| PS-11.2 | Proibir o pessoal de entrar/sair da unidade com dispositivos de gravação digital (por exemplo, unidades **USB**, câmeras digitais, telefones celulares) e incluir a busca desses dispositivos, como parte do processo de revista de saída. | * Confiscar quaisquer dispositivos de gravação digital detectados e armazená-los em armários seguros * Documentar quaisquer incidentes de tentativa de roubo de conteúdos * Tomar as medidas disciplinares necessárias para os indivíduos que tentam roubo de conteúdo * Implementar e aplicar uma política de proibição de dispositivos móveis/celulares com capacidade de gravação digital * Permitir telefones celulares com recurso de gravação digital se forem usados adesivos de lacre invioláveis |
| PS-11.3 | Reforçar o uso de sacos de plástico para alimentos e recipientes transparentes para qualquer alimento trazido para as áreas de produção. | * Considerar designar uma área para comer fora da área de produção |
| PS-11.4 | Implementar uma política de código de vestimenta que proíba o uso de roupas de grandes dimensões (por exemplo, calças largas, moletons muito grandes com capuz). |  |
| PS-11.5 | Usar etiquetas/hologramas numerados invioláveis para identificar dispositivos autorizados que podem entrar e sair da unidade. |  |
| PS-11.6 | Buscas | Implementar um processo para testar o procedimento de revista de saída. | * Realizar auditorias periódicas do processo de revista para assegurar que os guardas de segurança são meticulosos em suas revistas * Identificar formas de melhorar o processo de revista de saída * Documentar todas as auditorias e melhoramento do processo de revista |
| PS-11.7 | Realizar um processo de revista aleatória no veículo ao sair do estacionamento da unidade. |  |
| PS-11.8 | Segregar as linhas de replicação que processam conteúdo altamente sensível e realizar revistas ao sair de áreas segregadas. |  |
| PS-11.9 | Implementar controles adicionais para monitorar a atividade de guarda de segurança. | * Rever o processo de revista de saída para os guardas de segurança ao sair * Segregar responsabilidades de guardas de segurança para supervisionar áreas da unidade/produção a partir dos pontos de saída (por exemplo, processo de pesquisa) |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| PS-12.0 | Controle de estoque | Implementar um sistema de gestão de ativos de conteúdo para fornecer acompanhamento detalhado de ativos físicos (ou seja, recebido de cliente criado na unidade). | * Exigir um formulário de liberação ou ordem de serviço para confirmar que o conteúdo pode ser verificado por um indivíduo específico * Exigir que as pessoas apresentem a identificação para autenticação * Exigir uma etiqueta (por exemplo, código de barras, identificação única) para todos os ativos * Registrar todos os ativos que estão em check-in/check-out * Registrar a duração esperada de cada check-out * Considerar o uso de um alerta automatizado para fornecer notificações de ativos que não foram devolvidos no fim do dia útil ou do período de tempo autorizado * Rastrear e acompanhar indivíduos que têm com ativos em check-out pendentes * Registrar a localização de cada ativo * Registrar a data e hora de cada transação |
| PS-12.1 | Colocar código de barras ou atribuir identificadores de controle únicos nos ativos de clientes e mídias criadas (por exemplo, fitas, discos rígidos) após o recebimento e armazenar os ativos na caixa-forte quando não estiverem em uso. | * Aplicar códigos de barras duplos para rastrear os ativos (ou seja, código de barras, tanto no ativo como no recipiente/caixa). * Enviar os ativos diretamente para a **caixa-forte** depois de colocar o código de barras e devolver os ativos para a **caixa-forte** imediatamente quando não forem mais necessários |
| PS-12.2 | Reter os registros de transação de movimento do ativo por pelo menos um ano. | * Armazenar registros físicos ou digitais para todos os movimentos de ativos; os registros devem incluir: * Código de barras ou identificação exclusiva de ativo que fez check-in/check-out * Horário e data do check-in/check-out * Nome e ID exclusivo do indivíduo que fez check-out ao ativo * Motivo para check-out * Localização do ativo |
| PS-12.3 | Controle de estoque | Analisar registros do sistema de **gestão de ativos** de conteúdo pelo menos semanalmente e investigar anomalias. | * Identificar ativos que não foram devolvidos até a data de retorno esperada * Fazer acompanhamento de indivíduos que fizeram check-out por último de ativos que estão faltando * Implementar procedimentos disciplinares para os indivíduos que não seguem políticas de **gestão de ativos** * Considerar a implementação de notificação automática quando os ativos estiverem em check-out por longos períodos de tempo |
| PS-12.4 | Usar apelidos para o título do filme do estúdio quando aplicável nos ativos físicos e nos sistemas de rastreamento de ativos. | * Considerar a remoção do nome de estúdio em ativos físicos, quando apropriado |
| PS-12.5 | Implementar e analisar um relatório diário de vencimento para identificar ativos altamente sensíveis que forem retirados da **caixa-forte** com check-out e não tiverem o check-in registrado de volta. | * Fazer relatórios diários de vencimento manualmente ou através de um sistema de **gestão de ativos** * Investigar todas as exceções |
| PS-12.6 | Trancar e registrar bens que estão em atraso ou devolvidos se as remessas não puderem ser entregues a tempo. | * Estabelecer um procedimento para armazenar os ativos em uma área de acesso controlado * Manter a documentação que registra o armazenamento no local de ativos, incluindo a data e a razão para o armazenamento |
| PS-13.0 | Contagens de estoque | Efetuar uma contagem de estoque trimestral do(s) ativo(s) de cada cliente, reconciliar com os registros de **gestão de ativos** e comunicar imediatamente as variações para os clientes. |  |
| PS-13.1 | Segregar funções entre os funcionários da **caixa-forte** e as pessoas responsáveis por executar as contagens de estoque. | * Atribuir ao pessoal que não é da **caixa-forte** a execução de verificações aleatórias dos resultados da contagem |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| PS-14.0 | Rastreamento de mídia em branco/matérias-primas | Etiquetar estoque em branco/matérias-primas (por exemplo, código de barras, atribuir identificador exclusivo) por unidade quando recebido. | * Não permitir **mídia** em branco ou matérias-primas nas áreas de produção protegidas a menos que seja necessário para fins de produção |
| PS-14.1 | Estabelecer um processo para monitorar o consumo de matérias-primas (por exemplo, policarbonato) mensalmente. | * Reconciliar as matérias-primas existentes com ordens de trabalho para identificar as variações nos estoques * Estabelecer um limite de variação que desencadeia o processo de **resposta a incidentes**, quando ultrapassado * Considerar a realização de contagens físicas de matérias-primas, como parte do processo de rastreamento mensal |
| PS-14.2 | Armazenar **mídia** em branco/matérias-primas em um local protegido. | * Exigir controles de acesso (por exemplo, armário fechado, cofre) para evitar o acesso não autorizado * Restringir o acesso a **mídia** em branco/ matérias-primas ao pessoal responsável pela criação de produção * Exigir que as pessoas apresentem um pedido de ordem de serviço correto para fazer check-out na **mídia** em branco/matérias-primas |
| PS-15.0 | Ativos de clientes | Restringir o acesso a ativos de clientes acabados ao pessoal responsável por rastrear e gerenciar ativos. | * Restringir o acesso apenas a pessoal da **caixa-forte**, os quais poderão em seguida autorizar os indivíduos a fazer check-out nos ativos de clientes quando apresentados com um pedido válido de ordem de serviço * Segregar funções de modo que nenhum membro da equipe da **caixa-forte** manipule dados de produção para o processamento |
| PS-15.1 | Armazenar ativos de clientes em uma área restrita e segura (por exemplo, **caixa-forte**, cofre ou outro local de armazenamento seguro). | * Implementar um cofre adicional ou armação de alta segurança dentro da **caixa-forte** para os títulos altamente sensíveis * Fixar o cofre na parede ou piso parafusando-o à estrutura da sala |
| PS-15.2 | Solicitar dois **funcionários da empresa** com cartões de acesso separados para desbloquearem áreas altamente sensíveis (por exemplo, cofre, caixa forte de alta segurança) após o expediente. |  |
| PS-15.3 | Ativos de clientes | Usar um cofre à prova de fogo trancado para armazenar pacotes não entregues que forem mantidos na unidade durante a noite. | * Proteger o cofre parafusando-o em uma superfície imóvel (por exemplo, piso, parede) |
| PS-15.4 | Implementar uma área dedicada segura (por exemplo, câmara de segurança, sala de segurança) para o armazenamento de visualizadores não entregues que esteja trancada, de acesso controlado e monitorada com câmeras de vigilância e/ou guardas de segurança, | * Limitar o acesso ao pessoal que necessita de acesso para a sua função no trabalho * Certificar-se de que a área de armazenamento de visualizadores está completamente fechada, bloqueada e controlada em todas as ocasiões * Implementar um processo para rever imagens de vigilância regularmente |
| PS-16.0 | Descarte | Exigir que estoque rejeitado, danificado e obsoleto contendo ativos de clientes seja apagado, desmagnetizado, cortado em pedaços, ou fisicamente destruído antes do descarte. | * Implementar processos de inventário e reconciliar estoque, e em seguida reciclar ou destruir estoque rejeitado, danificado e obsoleto com segurança * Danificar a mídia irreparavelmente antes de colocá-la na lixeira de sucata * Considerar consultar o código 5220.22-M do Departamento de Defesa dos EUA quanto às normas de destruição e limpeza digital (consultar o anexo G) |
| PS-16.1 | Armazenar elementos direcionados para a reciclagem/destruição em um local/recipiente seguro para impedir a cópia e reutilização de ativos antes do descarte. | * Estabelecer e implementar políticas que limitem a duração (por exemplo, 30 dias) de armazenamento de estoque rejeitado, danificado e obsoleto antes de reciclar/destruir * Manter os ativos altamente sensíveis em áreas seguras (por exemplo, **caixa-forte**, cofre) antes da reciclagem/destruição * Assegurar que os depósitos de desperdícios sejam bloqueados |
| PS-16.2 | Manter um registro de descarte de ativos por pelo menos 12 meses. | * Integrar o registro de descarte de ativos no processo de **gestão de ativos** * Incluir um registro de descarte final para os bens descartados em registros de eliminação |
| PS-16.3 | Descarte | A destruição deve ser realizada no local. A destruição no local deve ser supervisionada e assinada por dois funcionários da empresa. Se uma empresa terceirizada de destruição for contratada, a destruição deve ser supervisionada e assinada por dois funcionários da empresa e os certificados da destruição devem ser mantidos. | * Considerar exigir as seguintes informações no certificado de destruição: * Data de destruição * Descrição do ativo destruído/descartado * Método de destruição * Nome da pessoa que destruiu os ativos |
| PS-16.4 | Usar a automação para transferir discos rejeitados de máquinas de replicação diretamente em caixas de sucata (sem manuseio do operador de máquina). | * Usar a segregação de funções (por exemplo, o pessoal que cria o disco de verificação é separado do pessoal que destrói o disco) onde a eliminação automática não for uma opção. * Manter um registro assinado da data e da hora em que o disco foi eliminado |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| PS-17.0 | Expedição | Exigir à unidade que gere uma ordem de serviço/expedição válida para autorizar as remessas de ativos para fora da unidade. | * Incluir a seguinte informação na ordem de serviço/expedição: * Número de ordem de serviço/expedição * Nome e empresa da pessoa que vai coletar o conteúdo * Data e hora da coleta * Contato da unidade * Criar um formulário para documentar ativos de saída que são transportados por meio de métodos incomuns |
| PS-17.1 | Acompanhar e registrar detalhes de remessa de ativos do cliente; no mínimo, incluir o seguinte:   * Hora da expedição * Nome do remetente e assinatura * Nome do destinatário * Endereço de destino * Número de rastreamento do courier * Referência à ordem de serviço correspondente | * Exigir assinatura do destinatário * Manter registros de expedição por um mínimo de um ano |
| PS-17.2 | Proteger os ativos de clientes que estão à espera de coleta. | * Trancar todas as portas e janelas nas áreas de envio e recebimento quando desacompanhado * Os ativos devem ser trancados até serem entregues ao fornecedor/courier |
| PS-17.3 | Validar ativos de cliente que deixarem a unidade, verificando uma ordem de serviço/expedição válida. | * Solicitar a identificação válida de couriers e pessoal de entrega para autenticar pessoas que coletam remessas para verificar a ordem de serviço correspondente * Confirmar que a contagem enviada corresponde à documentação de transporte * Informar quaisquer discrepâncias ou danos aos bens expedidos imediatamente |
| PS-17.4 | Expedição | Proibir couriers e pessoal de entrega de entrar em áreas de conteúdo/produção da unidade. | * Acompanhar pessoal de entrega se o acesso às áreas de conteúdo/produção for necessário |
| PS-17.5 | Documentar e manter um registro separado das informações sobre o motorista de caminhão. | * Manter um registro de todos os motoristas de caminhão e incluir as seguintes informações: * Nome * Etiquetas de licença para o trator e reboque * Empresa afiliada * Data e hora da coleta * Conteúdo manuseado |
| PS-17.6 | Acompanhar e monitorar o acondicionamento e vedação de reboques no local antes da expedição. | * Solicitar que o pessoal de segurança esteja presente em todos os momentos, enquanto os trailers são carregados e vedados |
| PS-17.7 | Registrar, monitorar e analisar os tempos de viagem, rotas e prazos de entrega para remessas entre unidades. | * Estabelecer uma linha de base para os prazos de entrega entre os pontos comuns de expedição e monitorar os tempos reais de variação * Investigar, denunciar e escalar grandes variações ao pessoal apropriado * Designar as paradas para descanso aprovadas * Considerar a implementação de um sistema de controle de GPS em tempo real para monitorar e alertar sobre atrasos não esperados |
| PS-17.8 | Proibir a transferência de elementos do filme, exceto para fins aprovados pelo estúdio do cliente. |  |
| PS-17.9 | Expedir cópias para as sessões de pré-estreias de cinema em segmentos (por exemplo, rolos pares ou ímpares). |  |
| PS-18.0 | Recebimento | Inspecionar os ativos do cliente entregues após o recebimento e comparar com os documentos de expedição (por exemplo, guia de remessa, registro). | * Identificar e registrar quaisquer discrepâncias (por exemplo, itens em falta, **mídia** danificada) * Informar discrepâncias para a administração, clientes e/ou o remetente imediatamente |
| PS-18.1 | Recebimento | Manter um registro de recebimento a ser preenchido por funcionários designados mediante o recebimento de entregas. | * Registrar as seguintes informações: * Nome e assinatura do courier/empresa de entrega * Nome e assinatura do destinatário * Data e hora da recepção * Detalhes do ativo recebido |
| PS-18.2 | Executar as seguintes ações imediatamente:   * Etiquetar (por exemplo, código de barras, atribuir identificador único) ativos recebidos * Introduzir o ativo no sistema de **gestão de ativos** * Mover o ativo para a área restrita (por exemplo, **caixa-forte**, cofre) | * Armazenar ativos recebidos que não podem ser imediatamente marcados e isolados em uma **área de montagem** segura (por exemplo, armação de alta segurança) |
| PS-18.3 | Implementar um método seguro para receber entregas durante a noite. | * Garantir que os horários para os itens esperados estarão disponíveis apenas para as pessoas que precisam vê-los |
| PS-19.0 | Rotulagem | Proibir a utilização de informação sobre títulos, incluindo nomes alternativos ("apelidos"), na parte exterior das embalagens, a menos que especificado de maneira diferente pelo cliente. |  |
| PS-20.0 | Acondicionamento | Enviar todos os ativos do cliente em recipientes fechados/selados e usar recipientes lacrados, dependendo do valor do ativo, ou se instruído pelo cliente. |  |
| PS-20.1 | Implementar pelo menos um dos seguintes controles:   * Fita inviolável * Embalagens invioláveis * Vedações invioláveis (por exemplo, na forma de hologramas) * Recipientes seguros (por exemplo, caixa Pelican com um cadeado com combinação) | * Estabelecer e comunicar um plano para como lidar com mercadorias que foram violadas * Comunicar todos os casos de violação para a equipe de resposta a incidentes (MS-5.0) |
| PS-20.2 | Acondicionamento | Aplicar celofane envolvendo todas as remessas e inspecionar a embalagem antes da expedição final para assegurar que ela esteja adequadamente acondicionada. | * Aplicar celofane envolvendo os ativos individuais (por exemplo, patins, paletes) ou por rolo se cargas a granel forem efetuadas |
| PS-21.0 | Veículos de transporte | Trancar automóveis e caminhões em todas as ocasiões e não colocar pacotes em áreas visíveis. | * Não deixar os pacotes desacompanhados |
| PS-21.1 | Incluir os seguintes recursos de segurança em veículos de transporte (por exemplo, reboques):   * Separação da cabine do condutor * Capacidade de bloquear e vedar portas da área de carga * GPS para remessas de alta segurança | * Usar veículos equipados com sistemas de rastreamento GPS para entrega de conteúdo sensível e ativos de alto valor |
| PS-21.2 | Aplicar selos numerados em portas de carga para as remessas de títulos altamente sensíveis. | * Exigir guardas de segurança para aplicar, registrar e monitorar os selos * Considerar medidas adicionais de segurança para pacotes altamente sensíveis (por exemplo, área de carga trancada/protegida, caixas pelicano lacradas). |
| PS-21.3 | Exigir escoltas de segurança a serem usadas quando houver a entrega de conteúdo altamente sensível em áreas de alto risco. | * Contratar pessoal de segurança capaz de proteger conteúdo altamente sensível de sequestros, assaltos e outras situações que possam resultar em roubo de conteúdos |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| DS-1.0 | Firewall/WAN/  Segurança do perímetro | Separar redes externas/WAN(s) de redes internas usando firewall(s) de inspeção com listas de controle de acesso que prevenir o acesso não autorizado a qualquer rede interna e com a capacidade de continuar o tráfego de upload e download. | * Configurar **firewalls** de **WAN** com Listas de Controle de Acesso que negam todo o tráfego a qualquer rede interna a não ser a dos hospedeiros explícitos que residem na **DMZ** * Configurar a rede **WAN** para proibir o acesso direto da rede à rede interna de conteúdo/produção * Incluir documentação detalhada de WAN que mostre com precisão e descreva o número de conexões para e de todos os dispositivos externos * As regras de firewall devem ser configuradas para gerar registros para todas as alterações de tráfego e de configuração, e os registros devem ser inspecionados pelo menos mensalmente * O firewall deve ter uma assinatura para atualizações de antivírus e detecção de intrusão, e atualizações devem ocorrer pelo menos uma vez por semana * Considerar incluir os itens seguintes na configuração do firewall: * Filtros antifalsificação * Bloquear endereços de IP não roteável * Bloquear endereços internos em portas externas * Bloquear solicitações de eco de UDP e ICMP * Bloquear portas e serviços não usados * Bloquear transferências da área DNS não autorizadas * Aplicar filtro de egresso, assim o tráfego de saída só pode vir de um endereço interno |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| DS-1.1 | Firewall/WAN/  Segurança do perímetro | Desenvolver um processo para revisar as Listas de Controle de Acesso (**ACL**s) para confirmar que as configurações são adequadas e exigidas pela empresa a cada 6 meses. | * Exportar as **ACLs** dos firewalls e/ou roteadores * Analisar as **ACLs** para confirmar que o acesso à rede está adequado * Exigir assinatura da administração da análise, bem como alterações de regras de firewall * Atualizar **ACLs** de acordo |
| DS-1.2 | Negar todos os protocolos por padrão e permitir apenas determinados protocolos seguros permitidos para acessar a WAN e firewall. | * Restringir todos os protocolos de comunicação sem criptografia, como **Telnet** e **FTP** * Substituir protocolos sem criptografia por versões criptografadas |
| DS-1.3 | Colocar servidores acessíveis externamente (por exemplo, servidores web) dentro da **DMZ**. | * Isolar os servidores na **DMZ** para fornecer apenas um tipo de serviço por servidor (por exemplo, servidor web etc.) * Implementar **ACLs** para restringir o acesso à rede interna da **DMZ** |
| DS-1.4 | Implementar um processo para corrigir dispositivos de infraestrutura de rede (por exemplo, firewalls, roteadores, switches, etc.), SAN/NAS (Storage Area Networks e Network Attached Storage) e servidores. | * Implementar um processo (por exemplo, mensalmente) para identificar, avaliar e testar os patches para dispositivos de infraestrutura de rede, SAN/NAS e servidores * Atualizar os dispositivos de infraestrutura de rede, SAN/NAS e servidores para os níveis de correção que solucionam as vulnerabilidades significativas de segurança * Tratar de patches cruciais em 48 horas * Considerar a implantação de um sistema de gestão de correções gerenciado centralmente |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| DS-1.5 | Firewall/WAN/  Segurança do perímetro | Proteger dispositivos de infraestrutura de rede, SAN/NAS, com base em padrões de configuração de segurança. Desativar o SNMP (Simple Network Management Protocol) se não estiver em uso ou usar apenas SNMPv3 ou superior e selecionar sequências da comunidade SNMP que sejam senhas fortes. | * Considerar as opções seguintes de proteção: * Desativar contas de convidados e compartilhamentos * Instalar antivírus/antimalware * Habilitar firewalls de software * Remover software não necessário * Desinstalar/desativar serviços desnecessários * Exigir que todos os usuários executem como usuários restritos * Usar uma **ACL** que restrinja o acesso ao dispositivo, de modo que apenas sistemas de gestão autorizados possam ser usados para conectar usando SNMP * Consultar os seguintes padrões de segurança para verificar proteção de dispositivos de infraestrutura de rede: * NIST * SANS * NSA |
| DS-1.6 | Não permitir a gestão remota do firewall a partir de qualquer interface externa. | * Em vez disso, usar autenticação de dois fatores e uma conexão **VPN** com Padrão de criptografia avançada (advanced encryption standard, AES) em 128 bits ou superior para realizar as funções de administração remota * Exigir que as pessoas forneçam dois dos seguintes itens para acesso remoto não administrativo: * Informação que o indivíduo saiba (por exemplo, nome de usuário, senha) * Um item físico exclusivo que o indivíduo possua (por exemplo, token, **cartão de acesso,** smartphone, certificado) * Uma qualidade física/biometria exclusiva do indivíduo (por exemplo, impressão digital, retina) |
| DS-1.7 | Firewall/WAN/  Segurança do perímetro | Colocar os backups de dispositivos de infraestrutura de rede/SAN/NAS e servidores em um servidor protegido centralmente na rede interna. | * Configurar dispositivos de infraestrutura de rede para armazenar backups de arquivos de configuração de maneira segura (por exemplo, criptografado) na rede interna * Garantir que apenas os administradores autorizados tenham acesso ao local de armazenamento e aos backups criptografados * Garantir que as restrições estão em vigor para reduzir ataques de força bruta e o acesso não autorizado aos arquivos de configuração se o Trivial File Transfer Protocol (TFTP) for usado para backups |
| DS-1.8 | Realizar varreduras de vulnerabilidade trimestralmente de todas as faixas de IP externas e hosts pelo menos e corrigir os problemas | * Corrigir problemas cruciais que forneçam acesso não autorizado ao conteúdo de maneira oportuna * Garantir que as ferramentas usadas para varredura/testes acomodem tecnologias de virtualização, se estiverem sendo usadas * Considerar a realização disso por um terceiro independente |
| DS-1.9 | Realizar testes de penetração anuais de todas as faixas de IP externo e hosts pelo menos e corrigir os problemas. | * Corrigir problemas cruciais que forneçam acesso não autorizado ao conteúdo de maneira oportuna * Garantir que as ferramentas usadas para varredura/testes acomodem tecnologias de virtualização, se estiverem sendo usadas * Considerar a realização disso por um terceiro independente |
| DS-1.10 | Proteger as conexões de ponto a ponto usando conexões dedicadas e privadas e usando criptografia. | * Usar padrão de criptografia avançada (AES) em 128 bits ou superior |
| DS-1.11 | Implementar um protocolo de serviço de tempo sincronizado (por exemplo, Network Time Protocol) para garantir que todos os sistemas têm uma referência de hora comum. | * Garantir que os sistemas tenham o horário correto e consistente * Assegurar que os dados de horário sejam protegidos * Garantir que as configurações de horário sejam recebidas de fontes de horário aceitas pela indústria |
| DS-1.12 | Firewall/WAN/  Segurança do perímetro | Estabelecer, documentar e implementar os requisitos de segurança da linha de base para os dispositivos e serviços de infraestrutura de rede WAN. | * Assegurar que os padrões do sistema que poderiam criar vulnerabilidades sejam modificados antes de serem colocados em produção * Considerar o monitoramento contínuo para comunicar a conformidade da infraestrutura em comparação às linhas de base de segurança |
| DS-2.0 | Internet | Proibir a rede de produção e todos os sistemas que processam ou armazenam conteúdo digital de acessar a internet diretamente, incluindo e-mail. Se um caso de negócios exigir acesso de internet da rede de produção ou dos sistemas que processam ou armazenam conteúdo digital, apenas métodos aprovados são permitidos por meio do uso de um aplicativo/sessão de desktop hospedado remotamente. | * Manipular exceções usando um sistema de portal de Internet (por exemplo, Citrix, Terminal Services, VNC etc.) com os seguintes controles: * O sistema é estritamente controlado onde a navegação na Internet é a única função do servidor * O acesso a sites restritos é proibido, inclusive sites de e-mail baseados na internet, sites peer-to-peer, compartimentos digitais e outros sites maliciosos conhecidos * Restringir que o conteúdo seja transferido para ou a partir do sistema * Usar patches e atualizar o sistema regularmente com as últimas definições de vírus * Rever a atividade do sistema regularmente * Bloquear o mapeamento de unidades locais, bloquear o armazenamento em massa em USB, bloquear o mapeamento de impressoras, bloquear as funções de copiar e colar e bloquear o download/upload do sistema de gateway de internet da rede de produção * Implementar **regras** de **firewall** para negar todo o tráfego de saída por padrão e permitir explicitamente sistemas específicos e portas que exigem transmissão de saída para redes internas designadas, como os servidores de definição de antivírus, servidores de aplicação de patches, servidores de licenciamento (apenas quando as licenças locais não estiverem disponíveis), etc. |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| DS-2.1 | Internet | Implementar software de filtragem de e-mail ou dispositivos que bloqueiem o seguinte nas redes de **não produção**:   * E-mails de phishing potencial * Anexos de arquivos proibidos (por exemplo, Visual Basic scripts, executáveis etc.) * Restrições de tamanho de arquivo limitadas a 10 MB * Domínios conhecidos que são fontes de malware ou vírus | * Identificar os tipos de conteúdo restritos para os anexos de e-mail e no corpo da mensagem de e-mail * Implementar uma solução de filtragem de e-mail e configurar com base em tipos de conteúdo restrito |
| DS-2.2 | Implementar o software de filtragem da internet ou dispositivos que restrinjam o acesso a sites conhecidos para comércio de arquivos peer-to-peer, vírus, pirataria ou outros sites maliciosos. | * Implementar software de filtragem de internet/servidor de proxy para detectar e impedir o acesso a sites maliciosos |
| DS-3.0 | LAN/Rede interna | Isolar a  **rede de conteúdo/produção** das **redes de não-produção** (por exemplo, rede de escritório, **DMZ**, a internet, etc.) por meio de segmentação da rede física ou lógica. | * Definir as Listas de Controle de Acesso que permitam explicitamente o acesso à **rede de conteúdo/produção** de hosts específicos que necessitam de acesso (por exemplo, servidor de antivírus, servidor de gerenciamento de patches, servidor de distribuição de conteúdo, etc.) * Incluir portas explicitamente definidas e serviços que devem permitir o acesso nas **Listas de Controle de Acesso** * Segmentar ou segregar redes baseadas em zonas de segurança definidas * Implementar **regras** de **firewall** para negar todo o tráfego de saída por padrão e permitir explicitamente sistemas específicos e portas que exijam transmissão de saída para redes internas designadas, como os servidores de definição de antivírus, servidores de aplicação de patches, servidores de licenciamento (apenas quando as licenças locais não estiverem disponíveis), etc. * Implementar as **regras de firewall** para negar todo o tráfego de entrada por padrão e explicitamente permitir sistemas específicos e portas que exijam a transmissão de entrada de servidores específicos de distribuição de conteúdo designados. * Consultar a DS-2.0 para obter orientação sobre o acesso à Internet no ambiente de produção * Atribuir **endereços** **IP estáticos** por meio do endereço MAC em **switches** * Desativar o **DHCP** na **rede de conteúdo/produção** * Proibir os sistemas de computador da produção de se conectar a mais de uma rede por vez * Proibir o uso ou armazenamento do conteúdo nas redes de não produção |
| DS-3.1 | Restringir o acesso a sistemas de conteúdo/produção somente ao pessoal autorizado. | * Considerar o uso de travas de cabo Ethernet físico para assegurar que um cabo de rede não seja conectado a um dispositivo alternativo/não autorizado |
| DS-3.2 | LAN/Rede interna | Restringir o acesso remoto à **rede de conteúdo/produção** somente ao pessoal aprovado que necessite de acesso para realizar suas responsabilidades de trabalho. | * Proibir o acesso remoto para a rede de conteúdo/produção * Manter uma lista de **pessoal da empresa** que tem permissão para acessar remotamente a **rede de conteúdo/produção** * Desenvolver processos para a administração analisar a atividade remota em sistemas que residam na **rede de conteúdo/produção** * Configurar sistemas de acesso remoto para usar contas individuais * Limitar o acesso remoto a um único método com Listas de controle de acesso * No caso de acesso remoto de emergência ser necessário, implementar o seguinte: * Usar autenticação de dois fatores e preferencialmente com base em certificado * Bloquear os protocolos de transferência de arquivo, incluindo FTP, SSH, IRC, IM * **A configuração da VPN** não deve permitir túnel dividido * Utilizar um modelo de barra inicial/bastion host como um intermediário para conectar à rede de produção |
| DS-3.3 | Usar switches/dispositivos de 3 camadas para gerenciar o tráfego de rede e desativar todas as portas de **switch** não utilizadas na **rede de conteúdo/produção** para evitar a detecção de pacotes por meio de dispositivos não autorizados. | * Exigir que os administradores de dispositivo usem autenticação sólida, incluindo: * Uso de protocolo criptografado * Hash com salt para a senha * Senha separada para comandos de execução * Conectar ao console do dispositivo e atualizar arquivos de configuração para desativar as portas de **switch** não utilizadas * Permitir o registro nos switches/dispositivos de 3 camadas |
| DS-3.4 | Restringir o uso de dispositivos sem switch, como hubs e repetidores na **rede de conteúdo/produção**. | * Substituir todos os hubs/repetidores por **switches** ou dispositivos de 3 camadas |
| DS-3.5 | LAN/Rede interna | Proibir ligação de rede dual-home (ponte na rede física) em sistemas de computadores dentro da **rede de conteúdo/produção**. | * Usar ponte de rede lógica na camada de rede (por exemplo, **roteadores**, **firewalls**, **switches**, etc.) em vez de utilizar várias placas de rede (**NIC**s) em um sistema de computador |
| DS-3.6 | Implementar uma detecção de intrusão baseada em rede/sistema de prevenção (**IDS/IPS**) na **rede de conteúdo/produção**. | * Configurar a detecção de intrusão baseada em rede/sistema de prevenção para alertar/evitar atividades suspeitas na rede * Assinar antivírus/antimalware para o **IDS/IPS** * Atualizar definições/políticas de assinatura de ataques e antivírus/antimalware no **IDS/IPS** pelo menos semanalmente * Registrar todas as atividades e alterações de configuração para o **IDS/IPS** * Implementar software de sistema de detecção de intrusão baseada em host em todas as estações de trabalho |
| DS-3.7 | Desativar o SNMP (Simple Network Management Protocol) se não estiver em uso ou usar apenas SNMPv3 ou superior e selecionar sequências da comunidade SNMP que sejam senhas fortes. | * Usar uma **ACL** que restrinja o acesso ao dispositivo, de modo que apenas sistemas de gestão autorizados possam ser usados para conectar usando SNMP |
| DS-3.8 | Proteger os sistemas antes de colocá-los na **LAN/Rede interna**. | * Consultar DS-1.5 para obter sugestões |
| DS-3.9 | Conduzir varreduras de vulnerabilidade de rede interna e corrigir os problemas, pelo menos anualmente. | * Garantir que as ferramentas usadas para varredura acomodem tecnologias de virtualização, se estiverem sendo usadas * Incluir o seguinte: * Redes de produção * Rede sem produção * Máquinas/dispositivos conectados * Máquinas/dispositivos não conectados |
| DS-3.10 | LAN/Rede interna | Colocar os backups de SAN/NAS de rede local, dispositivos, servidores e estações de trabalho em um servidor protegido centralmente na rede interna. | * Configurar dispositivos da rede local para armazenar backups de arquivos de configuração de maneira segura (por exemplo, criptografado) na rede interna * Garantir que apenas os administradores autorizados tenham acesso ao local de armazenamento e aos backups criptografados |
| DS-4.0 | Sem fio/WLAN | Proibir a rede sem fio e o uso de dispositivos sem fio na **rede de conteúdo/produção**. | * Restringir as redes sem fio para convidados somente ao acesso à Internet, e não à **rede de conteúdo/produção** * Remover ou desativar o acesso sem fio em estações de trabalho/notebooks que processam ou armazenam conteúdo da rede de conteúdo/produção |
| DS-4.1 | Sem fio/WLAN | Configurar redes sem fio **sem produção** (por exemplo, administrativa e convidado) com os controles de segurança a seguir:   * Desativar WEP/WLAN * Permitir apenas criptografia **AES**128 **(WPA2),** ou superior * Segregar redes de "convidados" de outras redes da empresa * Alterar as credenciais de logon de administrador padrão * Alterar o nome de rede padrão (**SSID**) | * Considerar os controles de segurança, tais como: * Usar nomes **SSID** não específicos da empresa * Ativar IEEE 802.1X ou IEEE 802.11i onde a opção estiver disponível * Usar RADIUS para autenticação, onde a opção estiver disponível * Ativar **filtragem de endereços MAC** * Colocar os endereços MAC sem fio das estações de trabalho e de dispositivos de produção na lista negra * Configurar o ponto/controlador de acesso sem fio para transmitir apenas dentro do intervalo necessário * Implementar uma estrutura 802.1X para redes sem fio, que inclui o seguinte: * Discagem de Acesso Remoto no Serviço de Usuário (RADIUS) para Autenticação, Autorização e Contabilização * Lightweight Directory Access Protocol (LDAP), como o Active Directory, para gerenciar contas de usuário * Infraestrutura de Chaves Públicas para gerar e gerenciar certificados de cliente e servidor * Implementar os controles seguintes se chaves pré-compartilhadas precisarem ser usadas: * Configurar WPA2 com **criptografia** CCMP (**AES-128**) ou superior * Definir uma senha complexa (Veja DS-8.1 para recomendações de complexidade e senha) * Mudar a senha pelo menos a cada 90 dias e quando o **pessoal da empresa** de área fundamental rescindir o contrato |
| DS-4.2 | Sem fio/WLAN | Implementar um processo para verificar pontos de acesso sem fio desonestos e corrigir quaisquer problemas validados. | * Implementar um processo a percorrer e analisar a unidade em busca de pontos de acesso sem fio desprotegidos trimestralmente * Configurar uma solução de acesso centralizado sem fio (ou seja, controlador sem fio) para alertar os administradores de pontos de acesso sem fio desonestos após a detecção, se possível |
| DS-5.0 | Segurança do dispositivo de I/O | Designar sistemas específicos a serem utilizados para a entrada/saída de conteúdo (I/O). | * Implementar **ACLs** para permitir o tráfego entre a **rede de conteúdo/produção** e sistemas utilizados para I/O para determinados **endereços IP** específicos de origem/destino |
| DS-5.1 | Bloquear dispositivos de entrada/saída (I/O), armazenamento em massa, armazenamento externo e de armazenamento móvel (por exemplo, **USB**, **FireWire**, Thunderbolt, SATA, **SCSI**, etc.) e gravadores de mídia (por exemplo DVD, Blu-Ray, CD, etc.) em todos os sistemas que controlam ou armazenam conteúdo, com exceção dos sistemas utilizados para conteúdo I/O. | * Considerar o seguinte para bloquear **dispositivos I/O**: * Alterar a configuração do registro para restringir o acesso de escrita a **dispositivos I/O** para sistemas baseados no MS Windows * Remover o arquivo de armazenamento em massa para controlar o acesso de escrita em estações de produção para sistemas baseados em Mac * Desativar **dispositivos I/O** usando política de grupo para sistemas que usam o Microsoft Active Directory ou Apple Open Directory * Usar software de monitoramento de porta I/O para detectar o uso da porta se o bloqueio de dispositivos de saída não for viável |
| DS-6.0 | Sistema de segurança | Instalar software antivírus e antimalware em todas as estações de trabalho, servidores e em qualquer dispositivo que se conecte aos sistemas SAN/NAS. | * Instalar uma solução corporativa de antivírus e antimalware com um console de gerenciamento centralizado * Considerar a instalação de proteção de ponto de extremidade |
| DS-6.1 | Atualizar todas as definições de antivírus e antimalware diariamente ou com mais frequência. | * Configurar o console de gerenciamento centralizado de antivírus e antimalware para baixar e enviar atualizações de definição, pelo menos uma vez por dia |
| DS-6.2 | Verificar todos os conteúdos em busca de vírus e malware antes de colocá-los na **rede de conteúdo/produção** | * Realizar varreduras em um sistema que não esteja conectado à **rede de conteúdo/produção** |
| DS-6.3 | Sistema de segurança | Realizar varreduras como segue:   * Permitir a verificação de vírus e malware regular e completa do sistema em todas as estações de trabalho * Permitir a verificação de vírus e malware regular e completa do sistema em todos os servidores e para sistemas que se conectam a SAN/NAS | * Configurar o software antivírus e antimalware para realizar uma verificação completa do sistema com base na estratégia de antivírus e antimalware * Configurar o software antivírus e antimalware para executar durante os períodos ociosos |
| DS-6.4 | Implementar um processo para atualizar regularmente os sistemas (por exemplo, sistemas de transferência de arquivos, sistemas operacionais, bancos de dados, aplicativos, dispositivos de rede) com patches/atualizações que remediem vulnerabilidades de segurança. | * Sempre que possível, implementar uma ferramenta de gestão de patch centralizada (por exemplo, WSUS, Shavlik, Altiris) para implantar automaticamente patches para todos os sistemas * Procurar patches de fornecedores e outros terceiros * Testar os patches antes da implantação * Implementar um processo de exceção e controles de compensação para casos em que haja um caso legítimo de negócios para sistemas sem patch |
| DS-6.5 | Proibir os usuários de serem administradores das próprias estações de trabalho, a menos que exigido pelo software (por exemplo, ProTools, Clipster e software de criação tais como Blu-Print, Scenarist e Toshiba). A documentação do fornecedor do software deve mencionar explicitamente quais direitos administrativos são necessários. | * Verificar se a conta de usuário utilizada para acessar a estação de trabalho não tem privilégios de administrador do sistema |
| DS-6.6 | Utilizar travas de cabo em dispositivos portáteis de computação que lidem com conteúdos (por exemplo, notebooks, tablets, torres), quando forem deixados sozinhos. | * Prender uma trava de cabo em uma superfície fixa (por exemplo, uma mesa) |
| DS-6.7 | Sistema de segurança | Implementar controles de segurança adicionais para notebooks e dispositivos de armazenamento portátil que contenham conteúdo ou informações sensíveis relacionadas aos projetos do cliente. Criptografar todos os notebooks. Usar dispositivos de armazenamento portáteis com hardware criptografado. Instalar software de eliminação remota em todos os notebooks/dispositivos móveis que lidem com conteúdo para permitir a limpeza remota de discos rígidos e outros dispositivos de armazenamento. | * Anexar telas de privacidade aos notebooks se precisarem ser usados em locais não seguros * Não conectar notebooks a locais de redes sem fio públicas * Desligar os notebooks quando não estiverem em uso e não fazer uso dos modos de suspensão ou hibernação |
| DS-6.8 | Restringir os privilégios de instalação de software à gestão de TI. | * Proibir a instalação e uso de software não aprovado incluindo softwares maliciosos (por exemplo, software ilegal ou malicioso) * Verificar todos os sistemas em busca de um inventário dos aplicativos instalados pelo menos trimestralmente |
| DS-6.9 | Implementar linhas de base de segurança e padrões para configurar sistemas (por exemplo, notebooks, estações de trabalho, servidores, SAN/NAS) que forem configurados internamente | * Desenvolver uma compilação padrão segura que é usada para todos os sistemas de imagem |
| DS-6.10 | Serviços e aplicativos desnecessários devem ser desinstalados dos servidores de transferência de conteúdo. | * Analisar a lista de serviços instalados (por exemplo, serviços. MSc) em todos os servidores de transferência de conteúdo e desinstalar ou desativar os não necessários * Revisar a lista de aplicativos instalados em todos os servidores de transferência de conteúdo e desinstale qualquer um que não seja necessário * Revisar a lista de aplicativos de inicialização para garantir que todos os aplicativos desnecessários não estão funcionando |
| DS-6.11 | Manter um inventário dos sistemas e componentes dos sistemas. | * Atualizar o inventário pelo menos mensalmente |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| DS-6.12 | Sistema de segurança | Documentar a topologia de rede e atualizar o diagrama anualmente ou quando alterações significativas forem feitas na infraestrutura. | * Incluir WAN, DMZ, LAN, WLAN (sem fio), VLAN, firewalls e topologia de servidor/rede |
| DS-7.0 | Gestão de contas | Estabelecer e implementar um processo de gestão de contas para contas de administrador, usuário e serviço para todos os **sistemas de informação** e aplicações que lidem com conteúdo. | * Documentar políticas e procedimentos para gerenciamento de contas que abordam o seguinte: * Novas solicitações de usuários * Modificações de acesso ao usuário * Desativação e ativação de contas de usuário * Rescisão de usuário * Expiração da conta * Folhas de ausência * Desautorizar o compartilhamento de contas de usuários por vários usuários * Restringir o uso de contas de serviço para apenas os aplicativos que os exigem * Habilitar o registro nos seguintes sistemas de infraestrutura e dispositivos, no mínimo: * Componentes de infraestrutura (por exemplo, **firewalls**, servidores de autenticação, sistemas operacionais de rede, mecanismos de acesso remoto incluindo **VPN**) * Sistemas de operação de produção * Componentes de gerenciamento de conteúdo (por exemplo, dispositivos de armazenamento, servidores de conteúdo, ferramentas de armazenamento de conteúdo, ferramentas de transporte de conteúdo) * Sistemas com acesso à Internet * Implementar um servidor para gerenciar registros em um repositório central (por exemplo, syslog/servidor de gerenciamento de registros, ferramenta de Gestão de Eventos e Informações de Segurança (ferramenta **SIEM**) |
| DS-7.1 | Gestão de contas | Manter evidência rastreável das atividades de gerenciamento de contas (por exemplo, e-mails de aprovação, formulários de solicitação de alteração). | * Guardar provas de aprovações gerenciais e ações associadas para todas as atividades de gerenciamento de conta, sempre que possível |
| DS-7.2 | Atribuir credenciais exclusivas com base na necessidade de saber usando os princípios de privilégio mínimo. | * Atribuir credenciais com base na necessidade de saber para os seguintes **sistemas de informação**, no mínimo: * Sistemas de produção * Ferramentas de gerenciamento de conteúdos * Ferramentas de **transferência de conteúdos** * Dispositivos de infraestrutura de rede * Sistemas de registro e monitoramento * Portal web do cliente * Sistemas de gestão de contas (por exemplo, Active Directory, Open Directory, LDAP) * **Permissões remotas de VPN** que só devem ser concedidas quando absolutamente necessário |
| DS-7.3 | Renomear as contas de administrador padrão e outras contas e limitar o uso dessas contas a situações especiais que requeiram essas credenciais (por exemplo, atualizações de sistemas operacionais, instalações de patches, atualizações de software). | * Consultar a documentação de todo o hardware e software para identificar todas as contas padrão * Mudar a senha de todas as contas padrão * Sempre que possível, mudar o nome de usuário de cada conta * Desativar contas de administrador quando não estiverem em uso |
| DS-7.4 | Segregar funções para assegurar que os indivíduos responsáveis pela atribuição de acesso a sistemas de informação não sejam eles próprios os usuários finais desses sistemas (isto é, o pessoal não deve ser capaz de atribuir acesso a eles próprios). | * Aproveitar uma equipe independente para garantir o acesso a sistemas de informação quando possível * Implementar controles de compensação quando a segregação é inatingível, tais como: * Monitorar a atividade dos funcionários da empresa e dos funcionários terceirizados * Manter e analisar os registros de auditoria * Implementar segregação física * Impor um controle de gestão |
| DS-7.5 | Gestão de contas | Monitorar e auditar atividades de conta de serviço e de administrador. | * Permitir controles de monitoramento para sistemas e aplicações que suportam registro * Configurar sistemas e aplicativos para registrar ações de administrador e registrar no mínimo, as seguintes informações: * Nome de usuário * Marcação de hora * Ação * Informações adicionais (parâmetros de ação) * Monitorar contas de serviço para garantir que elas sejam utilizadas apenas para os fins previstos (por exemplo, as consultas de banco de dados, a comunicação aplicativo-a-aplicativo) * Implementar um processo para analisar mensalmente a atividade da conta de serviço e do administrador para identificar um comportamento anormal ou suspeito e investigar possível abuso |
| DS-7.6 | Implementar um processo para revisar o acesso do usuário a todos os **sistemas de informação** que lidem com conteúdo e remover contas de usuário que já não necessitem de acesso trimestralmente. | * Remover os **direitos de acesso** aos **sistemas de informação** de usuários que já não necessitam de acesso devido a uma mudança no papel do trabalho ou rescisão de **pessoal da empresa** e/ou **funcionários terceirizados** * Remover ou desativar contas que não foram utilizadas em mais de 90 dias |
| DS-7.7 | Restringir o acesso do usuário ao conteúdo em uma base por projeto | * Remover os **direitos de acesso** aos **sistemas de informação** de usuários que já não necessitam de acesso devido à conclusão do projeto |
| DS-7.8 | Gestão de contas | Desativar ou remover contas locais em sistemas que controlam conteúdo onde tecnicamente for viável. | * Implementar um servidor centralizado de gerenciamento de contas (ou seja, o servidor de diretório como o LDAP ou Active Directory) para autenticar o acesso do usuário aos **sistemas de informação** * Para os dispositivos de infraestrutura de rede, implementar Autenticação, Autorização e Contabilização (AAA) para gerenciamento de contas * Desativar a conta de convidado * Se as contas locais tiverem de ser usadas, quando possível, alterar o nome de usuário e senha para cada conta padrão, desativar a capacidade de fazer logon ao sistema através da rede usando contas locais |
| DS-8.0 | Autenticação | Reforçar o uso de **nomes de usuário** e senhas exclusivos para acessar **sistemas de informação**. | * Reforçar o uso de **nomes de usuários** e senhas exclusivos para todos os **sistemas de informação** * Configurar os **sistemas de informação** para exigirem autenticação, usando **nomes de usuário e senhas exclusivos** a um nível mínimo |
| DS-8.1 | Adotar uma política de senha sólida para ter acesso aos **sistemas de informação**. | * Criar uma política de senha que consista no seguinte: * Extensão mínima de senha de 8 caracteres * Mínimo de três dos seguintes parâmetros: maiúsculas, minúsculas, números e caracteres especiais * Duração máxima da senha de 90 dias * Duração mínima da senha de 1 dia * Máximo de tentativas inválidas de login de entre 3 e 5 tentativas * As contas de usuário bloqueadas por tentativas de logon inválidas devem ser debloqueadas manualmente e não devem ser desbloqueadas automaticamente depois de um certo tempo ter passado * Histórico de senha de dez senhas anteriores |
| DS-8.2 | Autenticação | Implementar autenticação de dois fatores (por exemplo, nome de usuário/senha e hard token) para acesso remoto (por exemplo, **VPN**) para as redes. | * Exigir que as pessoas forneçam dois dos seguintes itens para acesso remoto: * Informação que o indivíduo saiba (por exemplo, nome de usuário, senha) * Um item físico exclusivo que o indivíduo possua (por exemplo, token, **cartão de acesso,** smartphone, certificado) * Uma qualidade física/biometria exclusiva do indivíduo (por exemplo, impressão digital, retina) * Usar autenticação de dois fatores e uma conexão **VPN** com Padrão de criptografia avançada (AES) em 128 bits ou superior para realizar as funções de administração remota |
| DS-8.3 | Implementar software de protetores de tela ou de bloqueio de tela protegidos por senha para servidores e estações de trabalho. | * Configurar servidores e estações de trabalho manualmente ou através de uma política (como políticas de grupo do Active Directory) para ativar um protetor de tela protegido por senha após um máximo de 10 minutos de inatividade |
| DS-8.4 | Considerar a implantação de mecanismos de autenticação adicional para fornecer uma estratégia de autenticação sobreposta para acesso à WAN e LAN/rede interna. | * Considerar a adição de um ou mais dos seguintes: * Multi-Factor Authentication * Identificar e acessar o sistema de gestão * Sistema de logon único * Identificar padrões da federação |
| DS-9.0 | Registro e monitoramento | Implementar sistemas de relatórios e registros em tempo real para registrar e relatar os eventos de segurança; reunir as seguintes informações, no mínimo:   * Quando (data e hora) * Onde (fonte) * Quem (nome de usuário) * O que (conteúdo) | * Habilitar o registro nos seguintes sistemas de infraestrutura e dispositivos, no mínimo: * Componentes de infraestrutura (por exemplo, **firewalls**, servidores de autenticação, sistemas operacionais de rede, mecanismos de acesso remoto [por exemplo, sistemas **VPN**]). * Sistemas de operação de produção * Componentes de gerenciamento de conteúdo (por exemplo, dispositivos de armazenamento, servidores de conteúdo, ferramentas de armazenamento de conteúdo, ferramentas de transporte de conteúdo) * Sistemas com acesso à Internet * Aplicativos |
| DS-9.1 | Implementar um servidor para gerenciar registros em um repositório central (por exemplo, syslog/servidor de gerenciamento de registros, ferramenta de Gestão de Eventos e Informações de Segurança (ferramenta **SIEM**). |  |
| DS-9.2 | Configurar os sistemas de registro para enviarem notificações automáticas quando forem detectados eventos de segurança, a fim de facilitar a resposta ativa aos incidentes. | * Definir eventos que exigem investigação e permitir mecanismos de notificação automática ao pessoal apropriado; considerar o seguinte: * Tentativas bem sucedidas e mal sucedidas de se conectar à **rede de conteúdo/produção** * Transporte de conteúdo com tamanho de arquivo e/ou hora do dia incomum * Repetidas tentativas de acesso a arquivos não autorizados * Tentativas de escalação de privilégio * Implementar um servidor para agregar registros em um repositório central (por exemplo, syslog/servidor de gerenciamento de registros, ferramenta de Gestão de Eventos e Informações de Segurança [**SIEM**]) |
| DS-9.3 | Investigar qualquer atividade incomum relatada pelos sistemas de registros e relatórios. | * Incorporar procedimentos de **resposta a incidentes** para controlar eventos de segurança detectados |
| DS-9.4 | Registro e monitoramento | Implementar mecanismos de registro em todos os sistemas utilizados para o seguinte:   * Geração de chaves * **Gerenciamento de chaves** * Gerenciamento de certificados do fornecedor | * Garantir que todas as chaves geradas e certificados adicionados são rastreáveis para um usuário único |
| DS-9.4 | Analisar todos os registros semanalmente e analisar todos os críticos e elevados diariamente. | * Investigar qualquer atividade incomum que possa indicar um incidente grave de segurança * Identificar quaisquer eventos adicionais incomuns que não estejam sendo alertados e configurar o sistema de registros e relatórios para enviar alertas sobre esses eventos * Correlacionar os registros de sistemas diferentes para identificar padrões de atividade incomum * Com base nas descobertas das análises de registro, atualizar as configurações de **SIEM** conforme apropriado |
| DS-9.5 | Ativar o registro de movimento e das transferências de conteúdo interno e externo e incluir no mínimo as seguintes informações:   * Nome de usuário * Marcação de data/hora * Nome do arquivo * **Endereço IP** de origem * **Endereço IP** de destino * Evento (por exemplo, download, visualização) |  |
| DS-9.6 | Registro e monitoramento | Manter os registros por pelo menos um ano. | * Procurar orientação de um consultor jurídico para determinar os requisitos regulamentares para a retenção de registros * Armazenar os registros de conteúdo em um servidor centralizado que possa ser acessado somente por usuários específicos e esteja seguro em uma sala de acesso controlado |
| DS-9.7 | Restringir o acesso do registro ao pessoal apropriado. | * Manter as Listas de Controle de Acesso para garantir que apenas o pessoal responsável pela monitoração de registro e revisão tem permissão para ver os registros * Segregar funções para assegurar que os indivíduos não sejam responsáveis por monitorar sua própria atividade * Proteger os registros de exclusão ou modificação não autorizada, aplicando **direitos de acesso** adequados em arquivos de registros |
| DS-10.0 | Segurança móvel | Desenvolver uma política Traga seu próprio dispositivo (Bring Your Own Device, BYOD) para dispositivos móveis que acessam ou armazenam conteúdo. | * Considerar a implementação de proteção antivírus/antimalware de dispositivo móvel, incluindo: * Atualizar as definições, incluindo * Realizar verificações diariamente |
| DS-10.1 | Desenvolver uma lista de aplicativos, lojas de aplicativos e plugins/extensões de aplicativos aprovados para dispositivos móveis que acessam ou armazenam conteúdo. | * Proibir a instalação de aplicativos não aprovados ou aplicativos aprovados que não forem obtidos através de uma loja de aplicativos pré-aprovada * Considerar um sistema de gestão de dispositivo móvel |
| DS-10.2 | Manter um inventário de todos os dispositivos móveis que acessam ou armazenam conteúdo. | * Incluir sistema de operação, níveis de patch, aplicativos instalados |
| DS-10.3 | Exigir criptografia para todo o dispositivo ou para áreas do dispositivo em que o conteúdo será manipulado ou armazenado. | * Considerar um sistema de gestão de dispositivo móvel |
| DS-10.4 | Prevenir a evasão de controles de segurança. | * Prevenir o uso de jailbreaking, rooting, etc. |
| DS-10.5 | Segurança móvel | Implementar um sistema para realizar um apagamento remoto de um dispositivo móvel, caso seja perdido /roubado/comprometido ou de outro modo necessário. | * Lembrar os funcionários que dados de fora da empresa podem ser perdidos no caso de um apagamento remoto de um dispositivo seja realizado |
| DS-10.6 | Implementar o travamento automático do dispositivo após 10 minutos de não utilização. |  |
| DS-10.7 | Gerenciar todos os patches do sistema operacional do dispositivo móvel e atualizações do aplicativo. | * Utilizar os patches/atualizações relacionados à segurança disponíveis mais recentes após a liberação geral pelo fabricante do dispositivo, transportadora ou desenvolvedor |
| DS-10.8 | Fazer cumprir as políticas de senha. | * Consultar DS-8.1 |
| DS-10.9 | Implementar um sistema para realizar backup e restauração de dispositivos móveis. | * Criptografar os backups e armazená-los em um local seguro |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| DS-11.0 | Técnicas de segurança | Assegurar que as técnicas de segurança (por exemplo, spoiling, **marca d'água** invisível/visível) estejam disponíveis para uso e sejam aplicadas quando instruído. |  |
| DS-11.1 | Criptografar conteúdo em discos rígidos usando um mínimo de **criptografia** **AES** de 128 bits ou superior, por meio de:   * **Criptografia** baseada em arquivo: (ou seja, criptografar o conteúdo em si) * **Criptografia** baseada em unidade: (ou seja, criptografar o disco rígido) | * Para discos rígidos externos, considerar a compra de unidades pré-criptografadas (por exemplo, Rocstor Rocsafe, LaCie Rugged Safe) * Criptografar todo o conteúdo em discos rígidos, incluindo: * SAN/NAS * Servidores * Estações de trabalho * Desktops * Notebooks * Dispositivos móveis * Unidades de armazenamento externo * Implementar um ou mais dos seguintes: * **Criptografia** baseada em arquivo como DMGs criptografados ou arquivos ZIP criptografados * **Criptografia** baseada em unidade usando software |
| DS-11.2 | Enviar chaves ou senhas de decodificação usando um protocolo de comunicação fora da unidade (ou seja, não na mesma **mídia** de armazenamento que o conteúdo em si). | * Enviar chaves ou senhas de decodificação utilizando um método diferente do que aquele que foi utilizado para a transferência do conteúdo * Verificar para garantir que os principais nomes e senhas não estejam relacionados ao projeto ou conteúdo |
| DS-11.3 | Técnicas de segurança | Implementar e documentar as políticas e procedimentos de políticas de gestão de chaves:   * Uso de protocolos de criptografia para a proteção de conteúdos ou dados sensíveis, independente de sua localização (por exemplo, servidores, banco de dados, estações de trabalho, notebooks, dispositivos móveis, dados em trânsito, e-mail) * Aprovação e revogação de dispositivos de confiança * Geração, renovação e revogação de chaves de conteúdo * Distribuição interna e externa de chaves de conteúdo * Ligar as chaves de criptografia à responsáveis identificáveis * Separar as funções para dissociar a gestão de chaves do uso das chaves * Procedimentos de armazenamento de chaves * Procedimentos de backup de chaves | * Considerar a criação de chaves de criptografia únicas por cliente e para ativos críticos * Impedir a substituição não autorizada das chaves criptográficas * Exigir que os custodiantes da chave criptográfica confirmem formalmente que entendem e aceitam suas responsabilidades de custodiante de chave |
| DS-11.4 | Criptografar conteúdo em descanso e em movimento, incluindo instâncias de servidor virtual, usando **criptografia** **AES** de no mínimo 128 bits ou superior. | * [http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1\_Dec2005.pdf](mailto:http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf) |
| DS-11.5 | Técnicas de segurança | Armazenar chaves secretas e privadas (não chaves públicas) usadas para criptografar dados/conteúdos em uma ou mais das formas seguintes sempre:   * Criptografado com uma chave de criptografia de chave que seja pelo menos tão forte quanto a chave de criptografia de dados e que seja armazenada separadamente da chave de criptografia de dados * Em um dispositivo criptográfico seguro (por exemplo, módulo de segurança de host (HSM) ou um dispositivo de ponto de interação de Segurança de transação do PIN (Pin Transaction Security, PTS)) * Ter pelo menos dois componentes da chave integrais ou partes de chave, de acordo com um método de segurança aceito pelo setor |  |
| DS-11.6 | Confirmar que os dispositivos na **Lista de dispositivos confiáveis (TDL)** são apropriados com base na aprovação dos proprietários de direitos. | * Exigir que os clientes forneçam uma lista de dispositivos confiáveis para a reprodução de conteúdo * Criar Mensagens de distribuição de chaves (KDMs) somente para dispositivos no **TDL** |
| DS-11.7 | Confirmar a validade das chaves de conteúdo e garantir que as datas de vencimento estejam em conformidade com as instruções do cliente. | * Exigir que os clientes forneçam as datas de vencimento das chaves de conteúdo * Especificar uma data final para quando as chaves expirarem para limitar a quantidade de tempo em que o conteúdo pode ser visualizado |
| DS-12.0 | Controle de conteúdo | Implementar um sistema de gestão de conteúdo digital para fornecer controle detalhado do conteúdo digital. | * Registrar todo conteúdo digital que fez check-in/check-out * Registrar a localização digital de todo conteúdo * Registrar a duração esperada de cada check-out * Registrar a data e hora de cada transação |
| DS-12.1 | Controle de conteúdo | Manter os registros de transação de movimento de conteúdo digital por um ano. | * Incluir o seguinte: * Horário e data do check-in/check-out * Nome e ID exclusivo do indivíduo que fez check-out ao ativo * Motivo para check-out * Localização do conteúdo |
| DS-12.2 | Analisar periodicamente registros do sistema de gestão de conteúdo digital e investigar anomalias. |  |
| DS-12.3 | Usar nomes alternativos do cliente (“apelidos”) quando aplicável nos sistemas de rastreamento de ativos. | * Restringir o conhecimento de nomes alternativos do cliente ao pessoal envolvido no processamento de ativos de clientes |

| N.º | Tópico de segurança | Melhores práticas | Orientações para implementação |
| --- | --- | --- | --- |
| DS-13.0 | Sistemas de transferência | Usar apenas **sistemas de transferência** aprovados pelo cliente que utilizem controles de acesso, **AES** de no mínimo 128 bits, ou superior, criptografia para conteúdo em repouso e para conteúdo em movimento e use autenticação forte para sessões de transferência de conteúdo. | * Permitir que apenas usuários autorizados tenham acesso ao sistema de transferência de conteúdo * Considerar a restrição do acesso também com base no projeto * Verificar com o cliente se os sistemas de transferência de conteúdo são aprovados, antes do uso |
| DS-13.1 | Implementar um processo de exceção, onde a aprovação prévia do cliente deve ser obtida por escrito, para resolver situações em que as **ferramentas de transferência** criptografadas não forem utilizadas. | * Usar nomes de usuários e senhas geradas aleatoriamente que são comunicadas de forma segura para a autenticação * Usar apenas ferramentas/aplicativo de transferência aprovados pelo cliente * Exigir que os clientes assinem as exceções onde as **ferramentas de transferência** não criptografadas precisem ser utilizadas * Documentar e arquivar todas as exceções |
| DS-14.0 | Metodologia do dispositivo de transferência | Implementar e utilizar sistemas exclusivos para transferências de conteúdo. | * Assegurar que as estações de edição e os servidores de armazenamento de conteúdo não sejam usados para transferir conteúdo diretamente * Desativar a **VPN**/acesso remoto para os sistemas de transferência ou para qualquer sistema usado para armazenar, transferir ou manipular conteúdo |
| DS-14.1 | Separar os sistemas de transferência de conteúdo das redes administrativas e de produção. | * Separar as redes física ou logicamente |
| DS-14.2 | Metodologia do dispositivo de transferência | Colocar os sistemas de transferência de conteúdo em uma **Zona Desmilitarizada** (**DMZ**) e não na **rede de conteúdo/produção**. | * Proteger os sistemas de transferência antes de colocá-los na **DMZ** (consultar DS-1.5 para ter sugestões) * Implementar **Listas de Controle de Acesso (ACLs)** que restringem todas as portas para além daquelas exigidas pela  **ferramenta de transferência** de conteúdo * Implementar **ACLs** para restringir o tráfego entre a rede interna e a **DMZ** para **endereços de IP** de origem/destino específicos * Desativar o acesso à internet dos sistemas usados para transferir conteúdo, exceto o acesso necessário para baixar conteúdo do cliente ou para acessar locais de transferência de conteúdo aprovados |
| DS-14.3 | Remover o conteúdo de dispositivos/sistemas de transferência de conteúdo logo após a transmissão/recepção bem sucedida. | * Exigir que os clientes forneçam a notificação mediante o recebimento de conteúdo * Implementar um processo para remover conteúdo dos dispositivos e sistemas de transferência, incluindo das lixeiras * Quando aplicável, remover o acesso de clientes às **ferramentas de transferência** imediatamente após a conclusão do projeto * Confirmar que a conexão está encerrada após o término da sessão |
| DS-14.4 | Enviar notificações automáticas para o coordenador ou coordenadores de produção sobre a transmissão de conteúdo de saída. | * Configurar o sistema de transferência de conteúdo para enviar uma notificação automática (por exemplo, um e-mail) ao coordenador ou coordenadores de produção sempre que um usuário enviar conteúdo para fora da rede |
| DS-15.0 | Portal do cliente | Restringir o acesso aos portais da internet que forem utilizados para transferência de conteúdo, streaming de conteúdo e distribuição de chaves para usuários autorizados. | * Implementar medidas de controle de acesso em torno de portais da internet que fazem a transferência de conteúdo, fazem streaming de conteúdo e distribuem chaves através da implementação de uma ou mais das seguintes ações: * Exigir credenciais de usuário * Integrar chaves de máquina e/ou de usuário para autenticação e autorização * Gerenciar as chaves de criptografia usando separação de funções adequada (por exemplo, uma pessoa deve criar as chaves e outra pessoa deve usar as chaves para criptografar o conteúdo) * Limitar o acesso do portal a redes específicas, **VLANs**, sub-redes, e/ou intervalos de **endereços IP** * Restringir a capacidade de upload/download como aplicável a partir do portal do cliente |
| DS-15.1 | Portal do cliente | Atribuir credenciais únicas (por exemplo, nome de usuário e senha) aos usuários do portal e distribuir as credenciais aos clientes de forma segura. | * Não incorporar nomes de usuário e senhas em links de conteúdo * Considerar a distribuição das credenciais do usuário e links de conteúdo em e-mails separados * Considerar a distribuição de credenciais do usuário através de telefone ou SMS * Considerar a distribuição das chaves de criptografia por meio de transferência fora de banda * Criar uma política de senha que consista no seguinte: * Extensão mínima de senha de 8 caracteres * Mínimo de três dos seguintes parâmetros: maiúsculas, minúsculas, números e caracteres especiais * Duração máxima da senha de 90 dias * Duração mínima da senha de 1 dia * Máximo de tentativas inválidas de login de entre 3 e 5 tentativas * As contas de usuário bloqueadas por tentativas de logon inválidas devem ser desbloqueadas manualmente e não devem ser desbloqueadas automaticamente depois de um certo tempo ter passado * Histórico de senha de dez senhas anteriores |
| DS-15.2 | Garantir que os usuários só tenham acesso aos seus próprios **ativos digitais** (ou seja, o cliente A não deve ter acesso ao conteúdo do cliente B). | * Implementar um processo de revisão de permissões de arquivo/diretório pelo menos trimestralmente * Garantir que o acesso esteja restrito a apenas aqueles que necessitam dele |
| DS-15.3 | Colocar o portal em um servidor dedicado na **DMZ** e limitar o acesso de/para **IPs** e protocolos específicos. | * Implementar **Listas de Controle de Acesso (ACLs)** que restringem todas as portas para além daquelas exigidas pelo portal do cliente * Implementar **ACLs** para restringir o tráfego entre a rede interna e a **DMZ** para **endereços de IP** de origem/destino específicos * Proteger os sistemas antes de colocá-los na **DMZ** (consultar DS-1.5 para ter sugestões) |
| DS-15.4 | Portal do cliente | Proibir o uso de software/sistemas/serviços de produção de terceiros que estejam hospedados em um servidor de internet a menos que aprovado pelo cliente antecipadamente. | * Considerar a adição de um ou mais dos seguintes: * Multi-Factor Authentication * Identificar e acessar o sistema de gestão * Sistema de logon único * Identificar padrões da federação * Usar uma conexão **VPN** com padrão de criptografia avançada (AES) em 128 bits ou superior |
| DS-15.5 | Usar **HTTPS** e impor o uso de um conjunto de criptografia sólida (por exemplo, TLS v1) para o portal de internet interno/externo. |  |
| DS-15.6 | Não utilizar cookies persistentes ou cookies que armazenem credenciais em texto simples. | * Analisar o uso de cookies por meio das aplicações existentes baseadas na internet e garantir que nenhum deles armazenará credenciais em texto simples * Se um aplicativo estiver armazenando credenciais em cookies de texto simples, então executar uma das seguintes ações: * Reconfigurar o aplicativo * Atualizar o aplicativo * Solicitar um patch de segurança do desenvolvedor do aplicativo |
| DS-15.7 | Definir o acesso a conteúdos em portais internos ou externos para expirar automaticamente em intervalos pré-definidos, onde for configurável. |  |
| DS-15.8 | Testar a vulnerabilidade de aplicativos da internet trimestralmente e corrigir os problemas confirmados. | * Usar as diretrizes de teste aceitas pela indústria, como as emitidas pela Open Web Application Security Project (OWASP) para identificar vulnerabilidades em aplicações Web comuns como Cross Site Scripting (XSS), SQL Injection e Cross Site Request Forgery (CSRF) * Os testes devem ser realizados por um terceiro independente * Consultar o Anexo G para ter mais informações |
| DS-15.9 | Portal do cliente | Realizar testes de penetração anual dos aplicativos de internet e corrigir os problemas confirmados. | * Usar as diretrizes de teste aceitas pela indústria, como as emitidas pela Open Web Application Security Project (OWASP) para identificar vulnerabilidades em aplicações Web comuns como Cross Site Scripting (XSS), SQL Injection e Cross Site Request Forgery (CSRF) * Os testes devem ser realizados por um terceiro independente * Consultar o Anexo G para ter mais informações |
| DS-15.10 | Permitir que apenas o pessoal autorizado solicite o estabelecimento de uma conexão com um prestador de serviços de telecomunicações. |  |
| DS-15.11 | Proibir a transmissão de conteúdo usando e-mail (incluindo webmail). | * Considerar o uso de servidores seguros de dispositivos de e-mail para criptografar e-mails e anexos (por exemplo, Cisco IronPort, Sophos E-Mail Security Appliance, Symantec PGP Universal Gateway Email) |
| DS-15.12 | Revisar o acesso ao portal do cliente, pelo menos trimestralmente. | * Remover **direitos de acesso** ao portal do cliente após os projetos serem concluídos * Remover todas as contas inativas * Considerar enviar notificações automáticas por e-mail para uma parte adequada para onde quer que os dados sejam transferidos |

Anexo A – Glossário

Este glossário de termos básicos e siglas é usado mais frequentemente e consultado por nós nesta publicação. Essas definições foram adotadas a partir de normas relevantes de ISO (27001/27002), normas de segurança (ou seja, NIST) e as melhores práticas da indústria. Nas orientações sobre boas práticas, todos os termos que estão incluídos neste glossário estão destacados em **negrito.**

| **Termo ou sigla** | **Descrição** |
| --- | --- |
| **Lista de Controle de Acesso (ACL)** | Mecanismo que implementa o controle de acesso de um recurso do sistema, listando as identidades das entidades do sistema que têm permissão para acessar o recurso. |
| **Direitos de acesso** | Permissão para usar/modificar um objeto ou sistema. |
| **Advanced Encryption Standard (AES) (Padrão de criptografia avançada)** | Um padrão de criptografia de chave simétrica NIST que utiliza blocos de 128 bits e extensões de chave de 128, 192 ou 256 bits. |
| **Gestão de ativos** | O sistema pelo qual os ativos são monitorados durante todo o fluxo de trabalho, desde a aquisição até o descarte. |
| **Circuito fechado de televisão (CFTV)** | Câmeras de vídeo usadas para transmitir um sinal para um local específico em um conjunto limitado de monitores. |
| **Console de CFTV** | Sistema central de interface de monitoramento do CFTV. |
| **Pessoal da empresa** | Qualquer indivíduo que trabalha diretamente para a unidade, incluindo empregados, funcionários temporários e estagiários. |
| **Rede de conteúdo/ produção** | Uma rede de computador que é usada para armazenar, transferir ou processar conteúdo de mídia. |
| **Ativo digital** | Qualquer forma de conteúdo e/ou mídia que foi formatada em uma fonte binária que inclui o direito de usá-lo. |
| **Diligência devida (Due Diligence)** | A pesquisa ou investigação de um funcionário ou trabalhador terceirizado potencial que é realizada antes da contratação para garantir boas condições. |
| **Dynamic Host Configuration Protocol (DHCP) (Protocolo de configuração de host dinâmico)** | Protocolo usado para atribuir automaticamente endereços IP para todos os nós da rede |
| **Zona Desmilitarizada (DMZ)** | Sub-rede física ou lógica que contém e expõe serviços externos de uma organização para uma rede maior não confiável, geralmente a Internet. |
| **Criptografia** | A conversão de dados para um formato, chamado de texto cifrado, o qual não pode ser facilmente entendido por pessoas não autorizadas. |
| **Fingerprinting (marca de impressão digital)** | Uma técnica na qual o software identifica, extrai e depois comprime componentes característicos de uma mídia, permitindo que a mídia seja identificada exclusivamente por sua forma comprimida resultante. |
| **Firewall** | Gateway que limita o acesso entre redes de acordo com a política de segurança local. |
| **Conjunto de regras de firewall** | Tabela de instruções que o firewall usa para determinar como os pacotes devem ser encaminhados entre origem e destino. |
| **FireWire** | A interface de alta velocidade que permite que os dados sejam transmitidos a partir de dispositivos externos ao computador. |
| **File Transfer Protocol (FTP) (Protocolo de transferência de arquivos)** | Protocolo TCP/IP que especifica a transferência de arquivos através da rede sem criptografia. |
| **HTTPS** | Um protocolo de comunicações para comunicação segurança em uma rede de computador, com ampla implantação especialmente na internet. |
| **Crachá de identificação** | Cartão utilizado para identificar indivíduos autorizados a acessar uma unidade (por exemplo, funcionários, fornecedores, visitantes). |
| **Detecção de intrusão/**  **Prevenção de intrusão (IDS/IPS)** | Um sistema de detecção de intrusão (intrusion detection system, IDS) é um dispositivo ou aplicativo de software que monitora as atividades da rede ou do sistema quanto a atividades maliciosas ou violações da política e produz relatórios para uma estação da gestão. Um sistema de prevenção de intrusão (IPS) realiza a mesma função e também tenta bloquear a atividade. |
| **Resposta a incidentes** | A detecção, análise e correção de incidentes de segurança. |
| **Sistemas de informação** | Qualquer sistema eletrônico ou baseado em computador, que é usado pela unidade para processar a informação. Os sistemas de informação incluem aplicativos, dispositivos de rede, servidores e estações de trabalho, entre outros. |
| **Dispositivo I/O** | Dispositivos usados para comunicação com e/ou entre computadores (por exemplo, unidades USB e FireWire). |
| **Endereço IP** | Uma identificação numérica (endereço lógico) que é atribuída a dispositivos que participam de uma rede de computadores. |
| **Gerenciamento de chaves** | A criação, distribuição, armazenamento e revogação de chaves de criptografia que são usadas para acessar o conteúdo criptografado. |
| **Cartão de acesso** | Cartão de plástico, o qual armazena uma assinatura digital que é utilizada com fechaduras eletrônicas de controlo de acesso. |
| **Rede de área local (LAN)** | Rede de computadores que abrange uma pequena área física (por exemplo, um escritório). |
| **Filtragem de endereços MAC** | Metodologia de controle de acesso de segurança utilizada para restringir o acesso a uma rede de computadores. |
| **Chave mestra** | Chaves que oferecem acesso a todas as portas (interiores e exteriores) em uma qualquer unidade. Chaves com acesso a todas as áreas de alta segurança são também consideradas chaves mestras. |
| **Mídia** | Dispositivos físicos ou superfícies de escrita, incluindo mas não limitado a fitas magnéticas, discos óticos, discos magnéticos, chips de memória LSI, impressões nos quais as informações são registradas, armazenadas ou impressas dentro de um sistema de informação. |
| **Protocolo de rede** | Convenção ou norma que controla ou permite a transferência, comunicação e conexão de dados entre terminais de computação. |
| **Cartão de interface de rede (NIC)** | Um componente de hardware de computador que conecta um computador a uma rede. |
| **Rede sem produção** | Todas as redes de computadores que não são utilizadas para o processamento ou a transferência de conteúdo de mídia. As redes sem produção podem incluir o escritório ou rede administrativa e a rede do cliente. |
| **Avaliação de risco** | A identificação e priorização de riscos que é realizada para identificar possíveis ameaças a uma empresa. |
| **Gestão de risco** | A identificação, análise e mitigação de riscos por meio de avaliação de riscos e implementação de controles de segurança. |
| **Roteador** | Dispositivo cujo software e hardware são adaptados para as tarefas de direcionamento e encaminhamento de informações. |
| **Gestão de eventos e informações de segurança (Security information and event management, SIEM)** | Um termo para produtos e serviços de software combinando gestão de informações de segurança (security information management, SIM) e gestão de eventos de segurança (security event management, SEM). A tecnologia SIEM fornece análise em tempo real dos alertas de segurança gerados pelo hardware de rede e pelos aplicativos |
| **Segregação de funções** | Um princípio de segurança pelo qual nenhuma pessoa deve ter a capacidade de concluir uma tarefa por conta própria; um princípio pelo qual nenhuma pessoa deve ser responsável por mais de uma função relacionada. |
| **Identificador do conjunto de serviços (Service Set Identifier, SSID)** | Um identificador único para uma LAN sem fio que frequentemente é uma sequência legível e, assim, é normalmente chamada de "nome da rede". |
| **Pequena interface de sistema de computação (SCSI)** | Normas para conectar fisicamente e transferir dados entre computadores e dispositivos periféricos. |
| **Área de montagem** | Uma área onde o conteúdo é armazenado antes de ser coletado (por exemplo, para entrega ou inserção). |
| **IP estático** | Configuração em que um computador usa o mesmo endereço IP sempre que é ligado. |
| **Switch** | Dispositivo de computador de rede que conecta vários computadores dentro de uma rede e canaliza o tráfego para destinos específicos. |
| **Telnet** | Protocolo de rede utilizado na Internet ou rede de área local para acessar máquinas remotas. |
| **Funcionário terceirizado** | Qualquer indivíduo que trabalha para uma empresa externa, mas é contratado pela unidade para prestação de serviços. Funcionários terceirizados incluem empreiteiros, freelancers e agências temporárias. |
| **Mecanismos de rastreamento** | Ferramentas, processos e/ou métodos usados para rastrear ativos em todo o processo de produção, incluindo o registro de ativos, rastreamento de movimentos de ativos (por exemplo, mover um ativo da caixa-forte para baias de edição), expedição e destruição de ativos. |
| **Ferramentas de transferência** | Ferramentas usadas para a transmissão eletrônica de ativos digitais através de uma rede, geralmente com mecanismos de autenticação e criptografia aceitáveis. |
| **Protocolo de transferência** | O procedimento envolvido na transmissão de arquivos através de uma rede de computadores ou a Internet. |
| **Lista de dispositivos de confiança (TDL)** | Uma lista de dispositivos digitais específicos que são aprovados para reproduzir conteúdo. |
| **Nome de usuário exclusivo** | Identificação de login distinguível. |
| **Universal Serial Bus (USB)** | Padrão de barramento serial para conectar dispositivos a um computador host. |
| **Gestão de acesso do usuário** | O processo de criar, alterar direitos de acesso e remover contas de usuário de um sistema ou aplicativo. |
| **Caixa-forte** | Uma área que é dedicada a armazenar mídias físicas com conteúdo. |
| **Virtual Local Area Network (VLAN) (Rede virtual de área local)** | Rede de computador que tem os atributos de uma LAN/Rede interna, mas não se limita a localização física. |
| **Rede virtual privada (VPN)** | Rede de computadores que permite aos usuários acessar outra rede maior. |
| **Rede de área ampla (WAN)** | Rede de computadores que abrange uma área ampla (por exemplo, uma empresa). |
| **Watermarking (execução de marca d'água)** | O processo de incorporar de forma irreversível (possivelmente) as informações em um ativo digital. |
| **Trabalho em andamento (WIP)** | Qualquer bem que não é considerado como um produto final. |
| **Fluxo de trabalho** | A sequência de passos que uma empresa executa no conteúdo. |

Anexo B — Definições de canal de distribuição e título da MPAA

**Tipos de título**

| **Tipos de título** | **Descrição** |
| --- | --- |
| **Filme** | Tipo de trabalho lançado nos cinemas ou direto para o vídeo doméstico ou para a Internet que inclui os seguintes tipos:   |  |  | | --- | --- | | **Tipo de filme** | **Descrição** | | Longa-metragem | Um filme de extensão completa. | | Curta | Um filme mais curto do que seria considerado um filme de longa-metragem. | | Outro tipo de formato longo | Outras obras, por exemplo, um documentário. | |
| **Episódio de TV** | Um tipo de trabalho que está relacionado com a TV, a internet ou dispositivo móvel e inclui episódios de uma temporada ou minissérie. Um piloto é também um episódio como são outras sequências específicas (tais como "webisódio" ou "mobisódio"). |
| **Feitos para a TV** | Um tipo de trabalho que está relacionado com a TV, a internet ou dispositivo móvel, mas não tem episódios (por exemplo, filmes feitos para a televisão, eventos esportivos ou programas de notícias). |
| **Promoção/Publicidade** | Um tipo de trabalho que inclui:   * + "Promoção" –– Qualquer material promocional associado à mídia. Isso inclui teasers, trailers, pacotes eletrônicos para imprensa e outros materiais. A promoção é um caso especial de 'Anúncio'. |
| **Anúncio** | Qualquer forma de publicidade, incluindo comerciais de TV, infomerciais, anúncios de serviço público e promoções não abordadas pelo termo "Promoção". Isto não inclui trailers e teasers de filmes embora possam ser veiculados como um comercial de TV. |
| **Música** | Um tipo de trabalho que inclui ringtones, vídeos de música e outras músicas. |
| **Outro** | Um tipo de trabalho que inclui:   |  |  | | --- | --- | | **Tipo** | **Descrição** | | Excerto | Um ativo que consiste principalmente de parte ou partes de outra obra ou obras. | | Complementar | Material concebido para complementar uma outra obra. Por exemplo, um adicional associado a um DVD. | | Coleção | Uma coleção de ativos que não cai em outra categoria. Por exemplo, uma coleção de filmes. | | Franquia | Uma coleção ou combinação de outros tipos, por exemplo, uma franquia pode incluir múltiplos programas de TV, ou programas de TV e filmes. | |

**Canais de distribuição**

| **Canal de distribuição** | **Descrição** |
| --- | --- |
| **Cinema** | Um filme que é lançado exclusivamente nos cinemas. |
| **Não para cinema** | Um filme que é lançado publicamente em qualquer outra forma diferente da televisão, home vídeo ou cinema. Isto inclui a exibição de um filme (i) em aviões, trens, navios e outros veículos comuns, (ii) em escolas, faculdades e outras instituições de ensino, bibliotecas, agências governamentais, empresas e organizações de serviços e clubes, igrejas e outros grupos orientados para religião, museus e cineclubes (incluindo a transmissão da exposição por circuito fechado dentro da área imediata da origem de tal exposição), e (iii) em instalações militares permanentes ou temporárias, instituições fechadas, presídios, centros de aposentadoria, instalações de perfuração offshore, acampamentos madeireiros e acampamentos remotos florestais e de construção (incluindo a transmissão da exposição por circuito fechado dentro da área imediata da origem de tais exposições). |
| **Home Video** | Um filme lançado para a venda direta e as vendas para locação de produtos embalados em nível de atacado, por exemplo, em DVD ou Blu-Ray. |
| **Televisão gratuita** | Um filme que é lançado para o público em ondas de radiodifusão gratuita, geralmente conforme estabelecido no acordo de licença com redes, estações de televisão ou redes básicas de cabo. |
| **Televisão por assinatura** | Um filme que é lançado para o público de uma forma que exige o pagamento de pelo menos um participante da cadeia de transmissão, tais como vídeo sob demanda, satélite, cabo e pay-per-view. |
| **Internet** | Um filme que é lançado em qualquer um dos seguintes canais de distribuição on-line:   |  |  | | --- | --- | | **Tipo** | **Descrição** | | Venda eletrônica (EST) ou Download para Posse (DTO) | Cópias digitais permanentes vendidas on-line. | | Aluguel on-line ou vídeo sob demanda (VOD) | Locação paga on-line para visualização temporária. | | Assinatura de vídeo sob demanda (SVOD) | Aluguel por assinatura on-line para visualização on-line. | | Vídeo sob demanda grátis on-line (FVOD) | Transmissão grátis on-line de visualização normalmente suportada por receitas de publicidade. | | Outro | Mídia nova e on-line, como celular ou TV de Protocolo de Internet. | |

Anexo C — MAPEAMENTO PARA AS UNIDADES

As unidades devem analisar a legenda seguinte para identificar quais os tipos correspondem aos serviços que a unidade proporciona e implementar os controles apropriados com base em uma avaliação de risco.

|  |  |  |  |
| --- | --- | --- | --- |
| **Legenda** | | | |
| ADS | Áudio, dublagem e legendagem | FL | Laboratórios de filmes |
| CA | Publicidade Criativa | IFE | IFE (entretenimento de voo) e serviços de hotelaria |
| CDF | Serviços de courier, entrega e remessa | PP | Pós-produção |
| D | Distribuição | R | Replicação |
| DC | Cinema digital | VFX | Efeitos visuais |
| DS | Serviços digitais | AS | Segurança de aplicativos |
| DVD | Criação de DVD | CS | Segurança na nuvem |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| MS-1.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-1.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-1.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-1.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-2.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-2.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-3.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-4.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-4.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-4.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-4.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| MS-5.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-5.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-5.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-5.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-6.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-6.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-7.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-8.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-8.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-9.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-10.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-11.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-11.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.5 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.6 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-1.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-1.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-1.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-2.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-2.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-2.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-2.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-3.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-4.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-4.1 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-4.2 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-4.3 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-5.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.5 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.6 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.7 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-6.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-6.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-6.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.5 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-10.0 | X | X | X | X | X | X | X | X | X | X |  | X | X | X |
| PS-10.1 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| PS-10.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-10.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-11.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-11.1 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.2 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.3 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.4 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.5 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.6 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.7 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.8 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| PS-11.9 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-12.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-12.1 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.2 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.3 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.4 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.5 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.6 |  |  | X | X |  |  |  |  |  |  |  |  |  |  |
| PS-13.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-13.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-14.0 | X | X |  | X | X | X | X | X | X | X | X | X |  |  |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-14.1 | X | X | CDF | X | X | X | X | X | X | X | X | X | AS | CS |
| PS-14.2 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| PS-15.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-15.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-15.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-15.3 |  |  | X |  |  |  |  |  |  |  |  |  |  |  |
| PS-15.4 |  |  | X |  |  |  |  |  |  |  |  |  |  |  |
| PS-16.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-16.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-16.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-16.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-16.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.5 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-17.6 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-17.7 |  |  | X | X |  |  |  | X |  |  | X |  |  |  |
| PS-17.8 |  |  |  |  |  |  |  | X |  |  | X |  |  |  |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-17.9 |  |  |  |  |  |  |  | X |  |  |  |  |  |  |
| PS-18.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-18.1 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| PS-18.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-18.3 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-19.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-20.0 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-20.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-20.2 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-21.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-21.1 |  |  | X | X |  |  |  | X |  |  | X |  |  |  |
| PS-21.2 |  |  | X | X |  |  |  | X |  |  | X |  |  |  |
| PS-21.3 |  |  | X | X |  |  |  | X |  |  | X |  |  |  |
| DS-1.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-1.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.10 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.11 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.12 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-2.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-2.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-2.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.10 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-4.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-4.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-4.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-5.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-5.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.10 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.11 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.12 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-7.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-10.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.6 |  |  |  |  | X |  |  |  |  |  |  |  |  |  |
| DS-11.7 |  |  |  |  | X |  |  |  |  |  |  |  |  |  |
| DS-12.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-12.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-12.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-12.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-13.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-13.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-14.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-14.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-14.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-14.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-14.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.10 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.11 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.12 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |

Anexo D — Mapeamento de controles para referências

A tabela a seguir fornece um mapeamento geral das melhores práticas para as normas da ISO 27001/27002 e NIST 800-53. Estas normas podem ser consultadas para obter mais informações sobre a implementação dos controles de segurança fornecidos.

| **N.º** | **Tópico de segurança** | **Referência ISO 27002 -2013** | **Referência NIST 800-53 rev. 4** |
| --- | --- | --- | --- |
| **MS-1.0** | Conscientização/Supervisão de segurança executiva | 6.1.1 | PM-1, PM-2 |
| **MS-1.1** | 6.1.1 | AT-2, AT-3, PM-1, PM-2 |
| **MS-1.2** | 5.1.2, 6.1.1 | PM-1, PM-6, AT-3 |
| **MS-1.3** | 5.1.2, 6.1.1 | PM-1, PM-6, AT-3 |
| **MS-2.0** | Gestão de risco | 6.1.1 | CA-1, RA-1 |
| **MS-2.1** | 5.1.2 | RA-2 |
| **MS-3.0** | Organização de segurança | 6.1.3 | PM-2 |
| **MS-4.0** | Políticas e procedimentos | 5.1.1, 6.1.1 | PL-1 |
| **MS-4.1** | 5.1.2 | PL-1 |
| **MS-4.2** | 8.1.3 | PL-1, PS-7 |
| **MS-4.3** | 8.2.2, 8.1.3 | AT-1, AT-2, AT-3, AT-4 |
| **MS-5.0** | Resposta a incidentes | 16.1.1 | IR-1, IR-8 |
| **MS-5.1** |  | IR-2 |
| **MS-5.2** | 16.1.2 | IR-6, IR-7 |
| **MS-5.3** | 16.1.2 | IR-4, IR-5 |
| **MS-6.0** | Continuidade de negócios e Recuperação de desastres | 17.1.1 | CP |
| **MS-6.1** | 17.1.1 | CP |
| **MS-7.0** | Controle de alterações e Gestão de configuração | 14.2.2 | CM |
| **MS-8.0** | Fluxo de trabalho | 11.1 |  |
| **MS-8.1** | 11.1 |  |
| **MS-9.0** | Segregação de funções | 6.1.2 | AC-5 |
| **MS-10.0** | Verificações de antecedentes | 7.1.1 | PS-3 |
| **MS-11.0** | Acordos de confidencialidade | 7.1.2 | PL-4, PS-6, SA-9 |
| **MS-11.1** | 8.1.4 | PS-4, PS-8 |
| **MS-12.0** | Uso e triagem de terceiros | 7.1.2 | PL-4, PS-6, SA-9 |
| **MS-12.1** | 8.1.4 | PS-7, SA-9 |
| **MS-12.2** | 7.2.1 | PS-4 |
| **MS-12.3** | 8.14 |  |
| **MS-12.4** | 7.1.2 | PS-7 |
| **MS-12.5** | 11.1.2 | PL-4, PS-6, SA-9 |
| **MS-12.6** | 7.1.1 |  |
| **PS-1.0** | Pontos de entrada/saída | 11.1 | PE-3 |
| **PS-1.1** | 11.1 | PE-3, PE-6 |
| **PS-1.2** | 11.1 | PE-1, PE-2, PE-3 |
| **PS-2.0** | Entrada/Saída de visitante | 11.1 | PE-8 |
| **PS-2.1** | 11.1 | PE-7, PE-2, PE-3 |
| **PS-2.2** | 11.1 | PE-3 |
| **PS-2.3** | 11.1 | PE-7, PE-2, PE-3 |
| **PS-3.0** | Identificação | 11.1.2 | PE-3 |
| **PS-4.0** | Segurança do perímetro | 11.1.1 | PE-3 |
| **PS-4.1** | 11.1.1 | PE-3 |
| **PS-4.2** | 11.1.1 | PE-3 |
| **PS-4.3** | 11.1.1 | PE-3 |
| **PS-5.0** | Alarmes | 11.1.1 | PE-3, PE-6 |
| **PS-5.1** |  | PE-6 |
| **PS-5.2** | 11.1.1 | AC-6 |
| **PS-5.3** | 11.1.1 |  |
| **PS-5.4** | 11.1.1 | PE-3, PE-6 |
| **PS-5.5** | 11.1.1 | PE-3 |
| **PS-5.6** | 11.1.1 | PE-6 |
| **PS-5.7** | 11.1.1 | PE-9, PE-10, PE-11, PE-13 |
| **PS-6.0** | Autorização | 11.1 | PE-1, PE-2, PE-3 |
| **PS-6.1** | 11.1 | PE-2, |
| **PS-6.2** | 11.1 | PE-2, PS-4, PS-5 |
| **PS-7.0** | Controle de acesso eletrônico | 11.1 | PE-2, PE-3 |
| **PS-7.1** | 11.1 | PE-2, PE-3 |
| **PS-7.2** | 11.1 | PE-2, PE-3 |
| **PS-7.3** | 11.1 | PE-2, PE-3 |
| **PS-7.4** | 11.1 | PE-2, PE-3 |
| **PS-8.0** | Chaves | 11.1 | PE-2, PE-3 |
| **PS-8.1** | 11.1 | PE-2, PE-3 |
| **PS-8.2** | 11.1 | PE-2, PE-3 |
| **PS-8.3** | 11.1 | CM-8 |
| **PS-8.4** | 9.2.6 | CM-5, CM-8 |
| **PS-8.5** | 9.2.6 | CM-5, CM-8 |
| **PS-9.0** | Câmeras |  | PE-6 |
| **PS-9.1** | 11.1 | PE-6 |
| **PS-9.2** | 11.1 | PE-2, PE-3 |
| **PS-9.3** | 11.1 | AU-6, PE-6 |
| **PS-9.4** | 11.1 | PE-6 |
| **PS-10.0** | Registro e monitoramento | 12.4 | AU-3, AU-6  AU-9, AU-11 |
| **PS-10.1** | 12.4 | AU-6 |
| **PS-10.2** | 12.4 | AU-6 |
| **PS-11.0** | Buscas | 11.1 |  |
| **PS-11.1** |  |  |
| **PS-11.2** |  |  |
| **PS-11.3** |  |  |
| **PS-11.4** |  |  |
| **PS-11.5** |  |  |
| **PS-11.6** | 11.1 |  |
| **PS-11.7** |  |  |
| **PS-11.8** |  |  |
| **PS-11.9** |  |  |
| **PS-12.0** | Controle de estoque | 8.1 | CM-8 |
| **PS-12.1** | 8.2.2 | MP-3 |
| **PS-12.2** | 8.2.3 | AU-9, AU-11 |
| **PS-12.3** |  | AU-6, CM-8 |
| **PS-12.4** |  |  |
| **PS-12.5** | 8.2.3 | AU-1, AU-3, AU-6 |
| **PS-12.6** | 8.2.3 |  |
| **PS-13.0** | Contagens de estoque | 8.1.1 | AU-6, CM-8 |
| **PS-13.1** | 6.1.2 | AC-5 |
| **PS-14.0** | Rastreamento de mídia em branco/matérias-primas | 8.2.2 | MP-4 |
| **PS-14.1** | 8.1.1 | MP-4, PE-2, PE-3 |
| **PS-14.2** |  |  |
| **PS-15.0** | Ativos de clientes | 8.2.3 | MP-4, PE-2, PE-3 |
| **PS-15.1** | 8.2.3 | MP-2, MP-4 |
| **PS-15.2** |  |  |  |
| **PS-15.3** |  |  |  |
| **PS-15.4** |  |  |  |
| **PS-16.0** | Descarte | 8.3.2 | MP-6 |
| **PS-16.1** | 8.3.2 | MP-6 |
| **PS-16.2** |  | MP-6 |
| **PS-16.3** |  | MP-6 |
| **PS-16.4** |  |  |
| **PS-17.0** | Expedição | 8.3.3 | MP-5 |
| **PS-17.1** | 8.3.3 | AU-11, PE-16, MP-5 |
| **PS-17.2** | 8.2.3 | MP-5 |
| **PS-17.3** | 8.3.3 | PE-3, PE-7 |
| **PS-17.4** | 8.3.3 | PE-3, PE-7 |
| **PS-17.5** |  |  |
| **PS-17.6** |  |  |
| **PS-17.7** |  |  |
| **PS-17.8** |  |  |
| **PS-17.9** |  |  |
| **PS-18.0** | Recebimento | 8.2.3 | PE-16 |
| **PS-18.1** |  | MP-5 |
| **PS-18.2** | 8.2.2 | MP-3, MP-4 |
| **PS-18.3** | 8.2.3 | MP-3, MP-5 |
| **PS-19.0** | Rotulagem | 8.2.2 | MP-3 |
| **PS-20.0** | Acondicionamento | 8.3.3 | MP-5 |
| **PS-20.1** | 8.3.3 |  |
| **PS-20.2** |  |  |
| **PS-21.0** | Veículos de transporte |  | MP-5 |
| **PS-21.1** |  |  |
| **PS-21.2** |  |  |
| **PS-21.3** |  |  |
| **DS-1.0** | Rede externa/WAN | 13.1 | AC-4, SC-7 |
| **DS-1.1** | 9.1, 13.1, 13.2 | AC-3, AC-4 |
| **DS-1.2** | 10.1, 13.2 | CM-7 |
| **DS-1.3** | 13.2 | AC-20, CA-3, SC-7 |
| **DS-1.4** | 12.6 | CM-6, SI-2 |
| **DS-1.5** |  | CM-6, CM-7 |
| **DS-1.6** | 9.4, 10.1 | AC-6, AC-17 |
| **DS-1.7** | 12.3, 17.1 |  |
| **DS-1.8** | 12.6, 13.1 | RA-5, SC-7 |
| **DS-1.9** | 12.6 | RA-5, SC-7 |
| **DS-1.10** | 10.1, 13.1 | SC-7, SC-12, SC-33 |
| **DS-1.11** | 12.4 | SC-7, SC-12, SC-33 |
| **DS-1.12** | 12.2, 16.1 | SC-7, SC-12, SC-33 |
| **DS-2.0** | Internet | 12.1, 13.1 | CA-3 |
| **DS-2.1** | 13.2 | PL-4 |
| **DS-2.2** | 13 | AC-6, PL-4 |
| **DS-3.0** | LAN/Rede interna | 9.4, 13.1 | SC-7 |
| **DS-3.1** | 11.2 |  |
| **DS-3.2** | 6.2, 13.1, 9 | AC-3, AC-17 |
| **DS-3.3** | 10.1 | CM-6, CM-7 |
| **DS-3.4** | 13.1 | SC |
| **DS-3.5** | 13.1 | SC |
| **DS-3.6** | 16.1 | SI-4 |
| **DS-3.7** | 9.4 | SC |
| **DS-3.8** | 9.1 | SC |
| **DS-3.9** | 12.6 | SC |
| **DS-3.10** | 12.3, 17.1 | SC |
| **DS-4.0** | Sem fio | 9.1, 13.1 | AC-18 |
| **DS-4.1** | 9.1, 13.1 | AC-18 |
| **DS-4.2** | 9.1, 13.1 | SI-4 |
| **DS-5.0** | Segurança do dispositivo de I/O | 10.7.1 | SC-7 |
| **DS-5.1** |  | AC-19, MP-2 |
| **DS-6.0** | Sistema de segurança | 12.2 | SI-3 |
| **DS-6.1** | 12.2 | SI-3 |
| **DS-6.2** | 12.2 | SI-3 |
| **DS-6.3** | 12.2 | SI-3 |
| **DS-6.4** | 12.5, 12.6 | SI-2, RA-5 |
| **DS-6.5** | 9.4 | AC-5, SC-2 |
| **DS-6.6** | 11.2 | PE-3 |
| **DS-6.7** | 6.2, 10.1, 11.1 | MA-4, PE-5 |
| **DS-6.8** | 8.1, 12.5 | CM-11 SI-7 |
| **DS-6.9** | 12.1, 12.5 | CM-10, SI-7 |
| **DS-6.10** | 12.6 | AC-3, AC-6, CM-7 |
| **DS-6.11** | 8.1 | CM-8 |
| **DS-6.12** | 8.1, 14.1, 14.2 |  |
| **DS-7.0** | Gestão de contas | 9 | AC-2 |
| **DS-7.1** | 9.1 | AC-2 |
| **DS-7.2** | 9.2, 9.4 | AC-2, AC-6, IA-4 |
| **DS-7.3** | 8.1, 9.2, 9.4 | AC-2, AC-6, IA-4 |
| **DS-7.4** | 12.4, 18.2 | AC-2, AC-6, IA-4 |
| **DS-7.5** | 12.1, 12.4 | AU-3, AU-6 |
| **DS-7.6** | 9.2, 9.4 | AU-2, AU-12 |
| **DS-7.7** | 9.2, 9.4 | PS-4, PS-5 |
| **DS-7.8** | 9.2, 9.4 | AC-2, PE-2 |
| **DS-8.0** | Autenticação | 9.1 | IA-2, IA-4 |
| **DS-8.1** | 9 | AC-7, IA-5 |
| **DS-8.2** | 9.4, 10.1 | AC-17 |
| **DS-8.3** | 9.2, 9.4 | AC-11 |
| **DS-8.4** | 9.4 | AC-1 |
| **DS-9.0** | Registro e monitoramento | 12.4 | SI-4, AU-2, AU-3 |
| **DS-9.1** | 12.4 | AU-1, AU-6 |
| **DS-9.2** | 12.4 | AU-1, AU-6 |
| **DS-9.3** | 12.4 | AU-1, AU-2, AU-6 |
| **DS-9.4** | 10.1 | AU-2, AU-3 |
| **DS-9.5** | 12.4 | AU-3, AU-8 |
| **DS-9.6** | 10.1.3, 10.10.3 | AU-9, AU-11 |
| **DS-9.7** | 12.4 | AU-6 |
| **DS-10.0** | Segurança móvel | 6.2, 11.2 | SC, AC, IA-2 |
| **DS-10.1** | 6.2, 11.2 | SC, AC |
| **DS-10.2** | 6.2, 11.2 | SC, AC |
| **DS-10.3** | 6.2, 11.2 | SC, AC |
| **DS-10.4** | 6.2, 11.2 | SC, AC |
| **DS-10.5** | 6.2, 11.2 | SC, AC |
| **DS-10.6** | 6.2, 11.2 | SC, AC |
| **DS-10.7** | 6.2, 11.2 | SC, AC |
| **DS-10.8** | 6.2, 11.2 | SC, AC |
| **DS-10.9** | 6.2, 11.2 | SC, AC |
| **DS-11.0** | Técnicas de segurança | 8.2, 10.1 |  |
| **DS-11.1** | 8.2, 10.1 | IA-5, SC-13 |
| **DS-11.2** | 8.2, 10.1 | SC-8, SC-12 |
| **DS-11.3** | 8.2, 10.1 | SC-12 |
| **DS-11.4** |  |  |
| **DS-11.5** |  |  |
| **DS-11.6** | 10.1 |  |
| **DS-11.7** | 10.1 |  |
| **DS-12.0** | Controle de conteúdo |  |  |
| **DS-12.1** |  |  |  |
| **DS-12.2** |  |  |  |
| **DS-12.3** |  |  |  |
| **DS-13.0** | Sistemas de transferência | 10.1, 13.2 | IA-5, SC-13 |
| **DS-13.1** | 10.1, 13.2 |  |
| **DS-14.0** | Metodologia do dispositivo de transferência | 13.1 |  |
| **DS-14.1** | 13.1 | AC-4, SC-7 |
| **DS-14.2** | 13.1 | AC-4, AC-20, SC-7 |
| **DS-14.3** | 13.2 | MP-6 |
| **DS-14.4** | 12.4, 13.2 |  |
| **DS-15.0** | Portal do cliente | 13.1 | AC-6 |
| **DS-15.1** | 9.2, 9.4 | IA-5 |
| **DS-15.2** | 9.2, 9.4 | AC-2, AC-3, AC-6 |
| **DS-15.3** | 12.6, 13.1 | AC-4, AC-20 |
| **DS-15.4** | 9.2, 9.4, 10.1 |  |
| **DS-15.5** | 10.1 | SC-8, SC-13 |
| **DS-15.6** | 9.4 | AC-4 |
| **DS-15.7** | 9.4 | AC-2 |
| **DS-15.8** | 12.6 | SI-7 |
| **DS-15.9** | 12.6 |  |
| **DS-15.10** |  |  |
| **DS-15.11** | 13.2 | AC-4 |
| **DS-15.12** | 12.1 |  |

Anexo E — Perguntas mais frequentes

1. **Minha instalação precisa implementar todas as melhores práticas apresentadas?**

A conformidade com as melhores práticas é estritamente voluntária. Elas são diretrizes sugeridas a considerar ao planejar, implementar e modificar os procedimentos de segurança.

1. **Se minha unidade oferece vários serviços (por exemplo, laboratório de cinema e de pós-produção), qual conjunto de melhores práticas complementares devo aplicar?**

As unidades devem sempre aplicar o conjunto mais restritivo das melhores práticas complementares a menos que o processo de trabalho esteja separado um do outro, nesse caso, você deve aplicar somente as melhores práticas complementares ao ambiente para esse serviço.

1. **Minha unidade precisa aplicar todos os itens incluídos na seção "Orientações para implementação" das melhores práticas?**

Não. A informação contida nesta seção das diretrizes destina-se a ajudá-lo a determinar a melhor forma de estruturar um controle de segurança particular. Se sua empresa tiver uma avaliação de segurança de conteúdos realizada pela MPAA, a nossa avaliação somente comparará as práticas da sua instituição em relação à respectiva seção de melhor prática das diretrizes em um determinado ponto no tempo. (Para obter mais informações sobre como receber uma avaliação de segurança de conteúdos da MPAA, você pode entrar em contato conosco pelo e-mail contentsecurity@mpaa.org.

1. **E se o meu sistema atual não permitir a implementação das melhores práticas?**

Por favor, entre em contato com o fornecedor do respectivo sistema, a fim de identificar possíveis soluções para permitir que os sistemas sigam as melhores práticas. As soluções podem incluir correções, atualização da versão ou até mesmo mudança para um sistema mais seguro. Medidas de segurança alternativas também podem ser usadas, se as limitações técnicas impedirem a implementação das melhores práticas; no entanto, isto normalmente não é considerado para cobrir os riscos associados. Exceções à implementação das diretrizes de segurança devido às limitações do sistema devem ser formalmente documentadas e aprovadas por seus clientes.

1. **Ao aplicar as melhores práticas nesta diretriz, a minha unidade ainda precisa cumprir os requisitos de segurança definidos individualmente por um membro da MPAA?**

A implementação das melhores práticas é uma diretriz e não substitui as cláusulas contratuais específicas com um membro individual da MPAA. As decisões sobre o uso de fornecedores por qualquer membro específico são tomadas pelos membros exclusivamente de forma unilateral. A MPAA incentiva a usar as melhores práticas como uma diretriz para futuras discussões em torno da segurança com seus clientes.

Anexo F — Políticas e procedimentos sugeridos

Abaixo estão algumas áreas comuns para as quais as políticas e procedimentos de segurança devem ser desenvolvidas e implementadas a fim de salvaguardar o conteúdo:

1. **Políticas e procedimentos de segurança física**

* Segurança de pontos de entrada/saída
* Protocolo de acesso do visitante
* Identificação e autorização
* Protocolo de emergência
* Controles de acesso da unidade
* Monitoramento da unidade

1. **Inventário e gestão de ativos**

* Controle de estoque
* Protocolos de expedição
* Armazenagem do estoque no local, durante o transporte

1. **Segurança da tecnologia da informação**

* Política de uso da Internet
* Autenticação e autorização
* Política de senha
* Proteção de código malicioso/antivírus
* Observação: inclui tudo (uso aceitável, etc.)

1. **Políticas e procedimentos de recursos humanos**

* Incluindo a segurança nas responsabilidades de trabalho
* Triagem de pessoal
* Acordos de proteção de confidencialidade, direitos de propriedade e propriedade intelectual
* Termos e condições de emprego
* Segregação de funções (SOD)
* Rescisão de contrato de trabalho
* Medidas disciplinares
* Programa de treinamento e conscientização de segurança
* Triagem e verificação de antecedentes/referências dos funcionários e contratados temporários/autônomos
* Acordos de não divulgação do funcionário, do contratado temporário e do autônomo (NDAs)
* Retenção de registros

1. **Terceiros**

* Contratos de terceiros
* Acordos de não divulgação (NDAs)

1. **Resposta a incidentes**

* Identificação e análise de incidentes
* Escalação e relatórios de incidentes
* Processos e procedimentos de resposta a incidentes
* Procedimentos de revisão e lições aprendidas pós-mortem

Anexo G — Outros recursos e referências

International Organization for Standardization (ISO), Standard 27001. *Information technology - Security techniques - Information security management systems – Requirements.* Outubro de 2005.<http://www.27000.org/iso-27001.htm>

International Organization for Standardization (ISO), Standard 27002*. Information technology - Security techniques - Code of practice for information security management.* Julho de 2007.[http ://www.27000.org/iso-27002.htm](http://www.27000.org/iso-27002.htm)

International Organization for Standardization (ISO), Standard 27005. *Information technology - Security technique- Information security risk management*. Junho de 2008.<http://www.27000.org/iso-27005.htm>

National Institute of Standards and Technology Special Publication 800-53. *Recommended Security Controls for Federal Information Systems*, Fevereiro de 2005. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

National Institute of Standards and Technology Special Publication IR 7298. *Glossary of Key Information Security Terms,* abril de 2006.

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

SysAdmin, Audit, Networking, and Security (SANS Institute). *Glossary of Terms Used in Security and Intrusion Detection*

<http://www.sans.org/resources/glossary.php#m>

The Open Web Application Security Project (OWASP) – Testing Guide

<http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf>

National Institute of Standards and Technology Special Publication 800-88. *Guidelines for Media Sanitization*, setembro de 2006. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

National Industrial Security Program - Operating Manual (DoD 5220.22-M), fevereiro de 2006

http://dtic.mil/whs/directives/corres/pdf/522022m.pdf

The Center for Internet Security – Security Benchmarks http://benchmarks.cisecurity.org/

National Security Agency - Security Configuration Guides https://www.nsa.gov/ia/mitigation\_guidance/security\_configuration\_guides/

National Institute of Standards and Technology Special Publication 800-92. *Guide to Computer Security Log Management,* setembro de 2006. <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>

National Institute of Standards and Technology Special Publication 800-44. *Guidelines on Securing Public Web Servers,* setembro de 2007. <http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf>

National Institute of Standards and Technology Special Publication 800-40. *Creating a Patch and Vulnerability Management Program,* novembro de 2005. <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>

Anexo H — Denúncia de pirataria para a MPAA

**Denúncia de pirataria on-line para a MPAA**

Você pode denunciar a pirataria diretamente para a MPAA:

http://www.mpaa.org/contact-us/

**Linhas de dicas sobre pirataria 24 horas da MPAA e MPA**

A lista a seguir apresenta as informações de contato da linha de dicas 24 horas para cada país onde a MPAA trabalha com um escritório local de proteção de conteúdo:

|  |  |
| --- | --- |
| **América do Norte e América Latina** | |
| Canadá | (800) 363-9166 |
| Estados Unidos | (800) 371-9884 |
| **Europa, Oriente Médio e África (região EMEA)** | |
| Bélgica | +32 2 778 2711 |
| Itália | (800) 864 120 |
| Países Baixos | (909) 747 2837 |
| Ucrânia | +38 0 445 013829 |
| Reino Unido | (800) 555 111 |
| **Ásia-Pacífico (região APAC)** | |
| Austrália | +61 29997 8011 |
| Hong Kong | +65 6253-1033 |
| Malásia | +65 6253-1033 |
| Nova Zelândia | +65 6253-1033 |
| Filipinas | +65 6253-1033 |
| Cingapura | +65 6253-1033 |
| Taiwan | +65 6253-1033 |

Uma lista completa de informações de contato em geral de todos os escritórios regionais e nacionais de proteção de conteúdo está localizada em: <http://www.mpaa.org/contact-us/>

**Recursos on-line da MPAA**

Informações adicionais sobre a MPAA também podem ser encontradas neste site: [www.mpaa.org](http://www.mpaa.org)

Você também pode aprender sobre os programas de proteção de conteúdo em todo o mundo durante a exposição em: [www.fightfilmtheft.org](http://www.fightfilmtheft.org)

**Fim do documento**