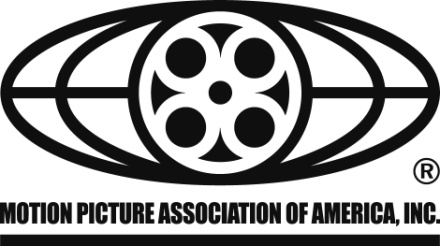
****

**Programa de seguridad de los contenidos de la MPAA**

**MEJORES PRÁCTICAS EN LA SEGURIDAD DE CONTENIDOS**

**PAUTAS COMUNES**

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

Versión 3.0

2 de abril de 2015

Antecedentes del documento

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Descripción** | **Autor** |
| 1.0 | 31 de diciembre de 2009 | Lanzamiento público inicial | Deloitte & Touche LLP  MPAA  Empresas miembro de la MPAA |
| 2.0 | 15 de mayo de 2011 | Actualizaciones y revisiones  Consolidación en pautas comunes y suplementos | PwC LLP  MPAA  Empresas miembro de la MPAA |
| 2.1 | 1 de enero de 2013 | Actualizaciones y revisiones | PwC LLP  MPAA  Empresas miembro de la MPAA |
| 3.0 | 2 de abril de 2015 | Actualizaciones y revisiones | MPAA  Empresas miembro de la MPAA |

Índice

[Antecedentes del documento i](#_Toc427411778)

[I. Información general de las mejores prácticas 2](#_Toc427411779)

[II. Información general de los establecimientos 4](#_Toc427411780)

[III. Gestión de riesgos 6](#_Toc427411781)

[IV. Formato de mejores prácticas 9](#_Toc427411782)

[V. Pautas comunes de mejores prácticas 10](#_Toc427411783)

[Anexo A: Glosario 100](#_Toc427411784)

[Anexo B: Definiciones de títulos y canales de distribución de la MPAA 105](#_Toc427411785)

[Anexo C: ESQUEMA DE ESTABLECIMIENTOS 109](#_Toc427411786)

[Anexo D: Esquema de medidas de control y sus referencias 121](#_Toc427411787)

[Anexo E: Preguntas frecuentes 126](#_Toc427411788)

[Anexo F: Políticas y procedimientos sugeridos 128](#_Toc427411789)

[Anexo G: Otros recursos y referencias 129](#_Toc427411790)

[Anexo H: Cómo notificar actividades de piratería a la MPAA 130](#_Toc427411791)

1. Información general de las mejores prácticas

**Introducción**

Durante más de tres décadas, la Motion Picture Association of America, Inc. (MPAA) (Asociación Cinematográfica de los Estados Unidos) ha gestionado evaluaciones sobre la seguridad de los contenidos a nombre de sus empresas miembro (miembros): Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Universal City Studios LLC; Twentieth Century Fox Film Corporation; Walt Disney Studios Motion Pictures y Warner Bros. Entertainment Inc.

A partir del año 2007, estas evaluaciones se realizaron con un modelo de encuestas, procesos y plantillas de informes estandarizados. Desde entonces, casi 500 establecimientos han sido encuestados en 32 países.

La MPAA se ha comprometido a proteger los derechos de quienes producen contenidos de carácter recreativo para públicos de todo el mundo. Desde las artes creativas hasta la industria de software, más y más personas de alrededor del mundo se ganan la vida con el poder de sus ideas. Esto significa que existe un interés cada vez mayor por proteger los derechos de propiedad intelectual y reconocer que estas medidas de protección son ejes fundamentales en una economía de información global sana.

El propósito del Programa de seguridad de los contenidos de la MPAA es fortalecer el proceso por el cual se protegen los contenidos de sus miembros durante la producción, posproducción, comercialización y distribución. Esto se logra a través de lo siguiente:

* La publicación de un conjunto de mejores prácticas por establecimiento de servicio delineando los controles estándares que ayudan a proteger los contenidos de los miembros.
* El análisis y la evaluación de la seguridad de los contenidos en establecimientos de terceros según lo publicado en las mejores prácticas.
* El énfasis en la importancia de asegurar los contenidos de los miembros.
* La utilización de un sistema de evaluación estandarizado para análisis individuales posteriores con respecto a la seguridad de los contenidos entre miembros y sus socios comerciales.

**Propósito y pertinencia**

El propósito de este documento es brindar a los proveedores futuros y actuales contactados por los miembros, un entendimiento de las expectativas generales en cuanto a la seguridad de contenidos y las mejores prácticas actuales de la industria. Las decisiones con respecto al uso de proveedores por parte de cualquier miembro las toma solo ese miembro unilateralmente.

Las mejores prácticas con respecto a la seguridad de contenidos han sido diseñadas para analizar los servicios que ofrecen cada establecimiento, el tipo de contenidos que el establecimiento gestiona y el período de lanzamiento en que opera el establecimiento.

Las mejores prácticas descritas en este documento están sujetas a leyes o normas locales, estatales, regionales, federales y nacionales.

Las mejores prácticas descritas en este documento, así como los estándares de la industria o referencias a ISO que el mismo incluya, están sujetos a cambios en forma periódica.

**El cumplimiento de las mejores prácticas es totalmente voluntario. No se trata de un programa de acreditación.**

**Proceso de excepción**

Si resultase imposible cumplir con una de las mejores prácticas, los establecimientos deben documentar el motivo por el cual no se puede dar cumplimiento e implementar medidas compensatorias en lugar de la mejor práctica. Las excepciones también deben informarse directamente al miembro.

**Preguntas o comentarios**

Si tiene preguntas o comentarios sobre las mejores prácticas, envíe un mensaje de correo electrónico a contentsecurity@mpaa.org

1. Información general de los establecimientos

La tabla que figura a continuación describe los servicios típicos que se ofrecen, los contenidos tratados y el período de lanzamiento para cada tipo de establecimiento.

| **N.º** | **Tipo de establecimiento** | **Servicios típicos del establecimiento** | **Tipo de contenidos** | **Período de lanzamiento** |
| --- | --- | --- | --- | --- |
| **1** | **Audio, doblaje y subtitulado** | * Doblaje en idioma original y extranjero * Subtitulado * SFX * Banda sonora * ADR/Foley | * Baja resolución * Marcado con una filigrana o de baja calidad * Contenidos completos o parciales * Pistas originales de audio | * Preestreno en cines * Preestreno en video |
| **2** | **Transporte, entrega y flete** | * Servicios de transporte * Servicios de entrega * Empresas de transporte | * Diversos | * Preestreno en cines * Preestreno en video * Catálogo |
| **3** | **Publicidad creativa** | * Interrumpidos * Sinopsis * Anuncios en TV * Avances * Gráficas * Anuncios en Internet | * Contenidos marcados con una filigrana, de baja calidad, completos o parciales * Imágenes fijas * Fragmentos | * Preestreno en cines * Preestreno en video * Catálogo |
| **4** | **Cine**  **digital** | * Masterización de cine digital * Duplicación * Administración de claves criptográficas | * Alta resolución – Contenidos completos o parciales * Copias originales para distribución en cines digitales * Paquetes para cine digital | * Preestreno en cines |
| **5** | **Servicios**  **digitales** | * Intermediación digital * Escaneo * Grabación en cinta * Restauración de cinta | * Imágenes nítidas y de alta resolución – Contenidos completos o parciales (cinta de película) | * Preestreno en cines * Catálogo |
| **6** | **Distribución** | * Distribución * Ejecución * Labores internas/Almacén de películas * Reciclaje de DVD y cintas | * Alta resolución * Imágenes nítidas | * Preestreno en cines * Preestreno en video * Catálogo |
| **7** | **Creación**  **de DVD** | * Compresión * Edición * Codificación * Regionalización * Extras * Control de calidad de disco grabado | * Copia completa | * Preestreno en video |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N.º** | **Tipo de establecimiento** | **Servicios típicos del establecimiento** | **Tipo de contenidos** | **Período de lanzamiento** |
| **8** | **Creación**  **de DVD** | * Compresión * Edición * Codificación * Regionalización * Extras * Control de calidad de disco grabado | * Copia completa | * Preestreno * en video |
| **9** | **Entretenimiento aéreo (In Flight Entertainment, IFE) y**  **servicios de hospitalidad** | * Laboratorio IFE * Integración en IFE * Hoteles * Aerolíneas * Trasatlánticos y transbordadores * Bibliotecas * Hospitales * Cárceles | * Alta resolución – Contenidos completos o parciales * Imágenes de baja calidad – Contenidos completos o parciales | * Preestreno en cines * Preestreno en video * Catálogo |
| **10** | **Servicios de posproducción** | * Telecine * Duplicación * Montaje * Finalización * Control de calidad | * Alta resolución – Contenidos completos o parciales | * Preestreno en cines * Preestreno en video * Catálogo |
| **11** | **Duplicación** | * Premasterización * Masterización * Duplicación * Creación de disco grabado | * Alta resolución * Imágenes nítidas | * Preestreno en video |
| **12** | **Efectos**  **visuales**  **(VFX)** | * Posproducción digital * Imágenes creadas por computadoras * Animación | * Alta resolución – Parcial * Fotogramas, tomas, secuencias e imágenes fijas * Guiones * Guiones gráficos | * Preestreno en cines * Posestreno en cines (2D a 3D) |
| **13** | **Aplicación** | * Desarrollo de aplicación | * Diversos | * Diversos |
| **14** | **Nube** | * Servidor * Centro de datos | * Diversos | * Diversos |

1. Gestión de riesgos

**Evaluación de riesgos**

Se debe identificar los riesgos a través de una evaluación de los mismos, y se debe implementar medidas de control adecuadas para disminuir el riesgo a un nivel aceptable y asegurar el cumplimiento de los objetivos comerciales.

La norma 27000 de la Organización Internacional de Normalización (Organization for Standardization, ISO) define el riesgo como la “combinación de la probabilidad de un evento y sus consecuencias”. Por ejemplo, cuál es la probabilidad de que alguien pueda hurtar los contenidos desde la red de un establecimiento y divulgarlos públicamente y cuál es la consecuencia comercial para una organización y el cliente si esto ocurre (por ej., incumplimiento contractual y/o pérdida de ingresos para ese período de lanzamiento).

La norma ISO 27001 también destaca la importancia de un sistema de gestión sólido que muestre cómo se puede establecer un Sistema de Gestión de Seguridad de la Información (Information Security Management System, ISMS).

**Clasificación de activos**

Una manera de clasificar activos en su establecimiento es seguir un proceso de cuatro pasos, el cual se resume a continuación:

Vigilar y evaluar la eficacia

Determinar un control de seguridad mínimo

Implementar controles

Identificar y clasificar activos

Junto con el miembro (su cliente), una organización tiene la responsabilidad de determinar cuáles activos del cliente requieren un mayor nivel de seguridad. La tabla que figura a continuación ofrece un ejemplo de cómo clasificar contenidos:

| **Clasificación** | **Descripción** | **Ejemplos** |
| --- | --- | --- |
| **Contenidos de alta seguridad** | Todo contenido que la organización considere que podría convertirse en pérdida financiera, reputación negativa para la marca o sanciones graves si tal activo se extraviara o fuera hurtado. | * Hurto de un éxito de taquilla antes del primer estreno en cines a nivel mundial. * Hurto de contenidos de un video antes del primer estreno en tiendas. * Hurto de copias originales o copias de películas. |

Cada mejor práctica suplementaria también incluye información adicional sobre riesgos relacionados con cada tipo de establecimiento.

**Medidas de control de seguridad**

El IT Governance Institute define las medidas de control como “las políticas, los procedimientos, las prácticas y las estructuras organizativas creadas para asegurar que se pueda dar cumplimiento a los objetivos comerciales y que se eviten o se detecten y corrijan los eventos no deseados”. Las medidas de control de seguridad normalmente se eligen según la clasificación del activo, su valor para la organización y el riesgo de que el activo se filtre o sea robado.

A fin de mitigar los riesgos identificados, las organizaciones deben implementar controles adecuados para cada riesgo específico. También se deben evaluar tales medidas en forma periódica para verificar su diseño y eficacia según el ambiente actual de riesgo.



**Sistema de gestión**



**Organización y gestión**



**Seguridad física**



**Transporte**



**Establecimiento**



**Seguridad digital**



**Infraestructura**



**IV. Organización del documento**



**MS-1 Concienciación de la seguridad ejecutiva/Omisión pág. 7**

**Las mejores prácticas están organizadas según el Modelo de Seguridad de Contenidos de la MPAA, el cual ofrece un marco para evaluar la capacidad de un establecimiento para proteger los contenidos de un cliente. Consta de temas de seguridad en tres áreas: sistema de gestión, seguridad física y seguridad digital. Los componentes del Modelo de Seguridad de Contenidos de la MPAA se derivan de normas ISO relevantes (27001-27002), estándares de seguridad (es decir, NIST, CSA, ISACA y SANS) y mejores prácticas de la industria.**

**MS-2 Gestión de riesgos pág. 7**

**MS-3 Organización de la seguridad pág. 8**

**MS-4 Políticas y procedimientos pág. 9**

**MS-5 Respuesta a incidentes pág. 12**

**MS-6 Continuidad del negocio y Recuperación ante desastres pág. 14**

**MS-7 Control de cambio y gestión de la configuración pág. 15**

**MS-8 Flujo de trabajo pág. 15**

**MS-9 Separación de responsabilidades pág. 16**

**MS-10 Verificación de antecedentes pág. 17**

**MS-11 Acuerdos de confidencialidad pág. 17**

**MS-12 Uso y verificación de agencias externas pág. 18**

**PS-1 Puntos de entrada y salida pág. 20**

**PS-2 Entrada y salida de visitantes pág. 21**

**PS-3 Identificación pág. 22**

**PS-4 Seguridad del perímetro pág. 22**

**PS-5 Alarmas pág. 23**

**PS-5 Autorización pág. 25**

**PS-8 Llaves pág. 26**

**PS-9 Cámaras pág. 28**

**PS-7 Control de acceso electrónico pág. 25**

**PS-10 Ingreso y vigilancia pág. 29**

**PS-11 Inspecciones pág. 30**

**Gestión de activos**

**PS-12 Seguimiento del inventario pág. 33**

**PS-13 Recuentos de inventario pág. 34**

**PS-14 Rastreo de medios vírgenes y materiales de inventario pág. 35**

**PS-15 Activos de clientes pág. 35**

**PS-16 Eliminación de residuos pág. 36**

**PS-17 Envío pág. 38**

**PS-18 Recepción pág. 39**

**PS-19 Etiquetado pág. 40**

**PS-20 Embalaje pág. 40**

**PS-21 Vehículos de transporte pág. 41**

**DS-1 Cortafuegos/Red de área amplia (Wide Area Network, WAN)/Seguridad del perímetro pág. 42**

**DS-2 Internet pág. 46**

**DS-3 Red de área local (Local Area Network, LAN)/Red interna pág. 48**

**DS-4 Inalámbrica pág. 51**

**DS-5 Seguridad del dispositivo I/O pág. 53**

**DS-6 Seguridad del sistema pág. 53**

**DS-7 Gestión de cuentas pág. 56**

**DS-7.7-8.4 Autenticación pág. 58-60**

**DS-9 Ingreso y vigilancia pág. 61**

**Gestión de los contenidos**

**DS-10 Seguridad en telefonía móvil pág. 63**

**Transferencia de los contenidos**

**DS-11 Técnicas de seguridad pág. 65**

**DS-12 Seguimiento del contenido pág. 67**

**DS-13 Sistemas de transferencia pág. 68**

**DS-14 Metodología de dispositivos de transferencia pág. 68**

**DS-15 Portal del cliente pág. 70**

1. Formato de mejores prácticas

Las mejores prácticas para cada tema de seguridad incluido en el Modelo de Seguridad de Contenidos de la MPAA se presentan con el siguiente formato:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sistema de gestión | Seguridad física | | | Seguridad digital | | |
| Organización y gestión | Establecimiento | Gestión de activos | Transporte | Infraestructura | Gestión de los contenidos | Transferencia de los contenidos |

El gráfico en la parte superior de cada página destaca el área de seguridad que se aborda en el contexto del Modelo de Seguridad de Contenidos de la MPAA.

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| PS-9.0 | Llaves | Limite la entrega de **llaves maestras** al personal autorizado únicamente (por ej., propietario, gerencia de los establecimientos). | * Mantenga un listado del **personal de la empresa** autorizado a sacar las **llaves maestras.** * Actualice el listado en forma periódica para eliminar **personal de la empresa** que ya no necesite acceso a las **llaves maestras.** |
| PS-9.1 | Implemente un proceso de ingreso y salida para rastrear y vigilar la entrega de las **llaves maestras.** | * Mantenga registros para darle seguimiento a la siguiente información: * **Personal de la empresa** que esté en posesión de cada una de las llaves maestras * Hora de ingreso y salida * Motivo de la salida |

P

**Glosario**

Todos los términos incluidos en el glosario están resaltados en **negrita**y se definen en el Anexo A.

**Guía de implementación**

Se ofrecen medidas adicionales y posibles pasos para la implementación, así como ejemplos, a fin de ayudar a las organizaciones a implementar las mejores prácticas.

**Mejor práctica**

Se explican las mejores prácticas para cada tema de seguridad.

**Tema de seguridad**

Cada área de capacidad consta de uno o más “Temas de seguridad”. Se aborda cada Tema de seguridad con una o más mejores prácticas.

**N.º**

A cada mejor práctica se le asigna un número de referencia con formato de XX-Y.Z. XX para el área general, Y para el Tema de seguridad y Z para la medida de control específica.

1. Pautas comunes de mejores prácticas

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| MS-1.0 | Concienciación de la seguridad ejecutiva/Omisión | Establezca un sistema de gestión de seguridad de la información que implemente un marco de control para la seguridad de la información aprobada por los propietarios del negocio/gerencia superior. | * Por ejemplo, marco del Sistema de Gestión de Seguridad de la Información (Information Security Management System, ISMS) de ISO 27001, NIST, CoBIT, etc. |
| MS-1.1 | Revise las políticas y los procedimientos de la gestión de seguridad de la información al menos en forma anual. |  |
| MS-1.2 | Capacite y haga participar a la gerencia ejecutiva y a los propietarios en las responsabilidades de la empresa en cuanto a la protección de los contenidos al menos en forma anual. |  |
| MS-1.3 | Cree un grupo de gestión de seguridad de la información para establecer y revisar políticas de gestión de seguridad de la información. |  |
| MS-2.0 | Gestión de riesgos | Elabore un proceso formal y documentado de evaluación de riesgos en cuanto a la seguridad, centrado en flujos de trabajo de contenidos y en activos delicados a fin de identificar y dar prioridad a los riesgos de hurto y filtración de contenidos que son relevantes para el establecimiento. | * Defina un ámbito claro para la **evaluación de riesgos en cuanto a la seguridad y modifique según sea necesario**. * Incluya un enfoque sistemático que emplee la posibilidad de ocurrencia de un riesgo, el impacto para los objetivos comerciales/protección de contenidos y la clasificación de activos para asignar prioridades. * Consulte la norma MS-6.0 para ver las mejores prácticas sobre **flujos de trabajo** documentados. |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| MS-2.1 | Gestión de riesgos | Realice una **evaluación de riesgos** interna en forma anual y cuando ocurran cambios claves en el flujo de trabajo, al menos conforme a las Pautas comunes de las mejores prácticas de la MPAA y las Pautas suplementarias correspondientes, y documente los riesgos identificados y actúe para solucionarlos. | * Realice reuniones con la gerencia y con los interesados clave al menos en forma trimestral para identificar y dejar registro del hurto de contenidos y de los riesgos de filtración. * Realice un análisis de penetración externo y escaneos de vulnerabilidad de red internos y externos trimestrales, conforme a DS-1.8 y DS-1.9. * Identifique los riesgos claves en donde el establecimiento considera que se pueden producir pérdidas de contenidos. * Implemente y registre los controles para mitigar o reducir los riesgos identificados. * Vigile y evalúe la eficacia de las medidas de solución y los controles implementados al menos en forma trimestral. * Registre y prepare presupuestos para iniciativas, actualizaciones y mantenimiento de la seguridad. |
| MS-3.0 | Organización de la seguridad | Identifique los puntos de contacto claves de seguridad y formalmente defina las funciones y responsabilidades en cuanto a contenidos y protección de activos. | * Prepare gráficos organizativos y descripciones de cargos para facilitar la designación de funciones y responsabilidades según la seguridad de los contenidos. * Brinde capacitación por Internet o en vivo para preparar al personal de seguridad con respecto a las políticas y los procedimientos que son claves para sus funciones laborales. |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| MS-4.0 | Políticas y procedimientos | Establezca políticas y procedimientos con respecto a los activos y la seguridad de los contenidos; las políticas deben abordar los siguientes temas, como mínimo:   * Uso aceptable (por ej., redes sociales, Internet, teléfono, dispositivos personales, dispositivos móviles, etc.). * Políticas sobre el manejo y la clasificación de los contenidos y activos. * Continuidad del negocio (respaldo, retención y restauración). * Política sobre control de cambio y gestión de la configuración. * Política de confidencialidad. * Dispositivos digitales de grabación (por ej., teléfonos inteligentes, cámaras digitales, videograbadoras). * Política sobre excepciones (por ej., proceso para documentar desviaciones de la política). * Política sobre respuesta a incidentes. * Política sobre dispositivos móviles. * Políticas sobre redes, Internet y acceso inalámbrico. * Controles de contraseñas (por ej., longitud mínima de contraseñas, salvapantallas). * Política sobre seguridad. * Política sobre visitantes. * Política disciplinaria/sobre sanciones. * Método anónimo interno para informar piratería o mal manejo de contenido (por ejemplo, línea telefónica o dirección de correo electrónico). | * Considere flujos de trabajo específicos del establecimiento/negocios en el desarrollo de políticas y procedimientos. * Solicite que la gerencia ejecutiva autorice todas las políticas y todos los procedimientos antes de que se publiquen y divulguen. * Informe las medidas disciplinarias en la capacitación de orientación para nuevos empleados. * Consulte el Anexo F para ver la lista de las políticas y los procedimientos a tener en cuenta. |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| MS-4.1 | Políticas y procedimientos | Revise y actualice las políticas y los procedimientos de seguridad al menos en forma anual. | * Incluya los siguientes factores en la revisión gerencial anual de las políticas y los procedimientos de seguridad: * Tendencias recientes de seguridad * Retroalimentación de parte del personal de la empresa * Nuevas amenazas y vulnerabilidades * Recomendaciones de agencias regulatorias (es decir, FTC, etc.) * Incidentes de seguridad previos |
| MS-4.2 | Notifique y solicite la confirmación de todo **el personal de la empresa** (por ej., empleados, trabajadores temporarios, pasantes) y **empleados de agencias externas** (por ej., contratistas, trabajadores independientes, agencias proveedoras de funcionarios interinos) con respecto a todas las políticas, los procedimientos y/o requisitos de los clientes actuales. | * Proporcione el manual de la empresa que incluya todas las políticas generales y todos los procedimientos al contratar nuevo **personal para la empresa** y **empleados de agencias externas**. * Notifique al **personal de la empresa** y a los **empleados de agencias externas** las actualizaciones realizadas a las políticas, los procedimientos y requisitos de los clientes sobre la seguridad. * La gerencia debe retener la confirmación de las políticas, los procedimientos y requisitos de los clientes actuales para todo el **personal de la empresa** y los **empleados de agencias externas.** |
| MS-4.3 | Políticas y procedimientos | Desarrolle y actualice en forma regular un programa de concienciación de políticas y procedimientos sobre seguridad y capacite **al personal de la empresa** y a los **empleados de agencias externas** al momento de ser contratados y una vez al año sucesivamente en dichas políticas y procedimientos. Trate las siguientes áreas como mínimo:   * Políticas y procedimientos de seguridad de TI. * Manejo y seguridad de activos/contenido sobre requisitos generales y específicos del cliente. * Notificación escalada de incidentes de seguridad. * Política disciplinaria. * Administración de claves criptográficas y codificación para todas las personas que manipulen contenidos codificados. * Procesos de eliminación y destrucción de activos. | * Comunique mensajes de concienciación sobre la seguridad durante reuniones de la gerencia/personal. * Implemente procedimientos para darle seguimiento al **personal de la empresa** que haya completado la capacitación de seguridad anual (por ejemplo, depósito de bases de datos, bitácoras de asistentes, certificados de conclusión). * Proporcione capacitación personal o en línea al momento de la contratación para informar al **personal de la empresa** y a los **empleados de agencias externas** sobre incidentes comunes, riesgos correspondientes y sus responsabilidades de informar incidentes detectados. * Distribuya material sobre la concienciación de la seguridad, como carteles, correos electrónicos y boletines periódicos para alentar la concienciación de la seguridad. * Elabore capacitación y mensajes personalizados sobre responsabilidades laborales e interacción con contenidos delicados (por ejemplo, personal de TI, producción) para mitigar los problemas de piratería. * Considere grabar sesiones de capacitación y proporcionar las grabaciones como referencia. |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| MS-5.0 | Respuesta a incidentes | Establezca un plan formal de respuesta a incidentes que describa las acciones a tomar cuando se identifique y documente un incidente de seguridad. | * Considere incluir las siguientes secciones en el plan de **respuesta a incidentes**: * Definición de incidente * Notificación al equipo de seguridad. * Notificación escalada a la gerencia. * Análisis de impacto y prioridad. * Contención del impacto. * Erradicación y recuperación * Información de contactos clave, incluso información de contacto del estudio del cliente. * Notificación a clientes y socios comerciales afectados. * Notificación a las fuerzas del orden * Informe de detalles del incidente * Consulte la norma NIST SP800-61 Revisión 2 sobre Procedimientos en incidentes de seguridad informática. |
| MS-5.1 | Identifique el equipo de respuesta a incidentes de seguridad a cargo de identificar, analizar y remediar incidentes de seguridad. | * Incluya a representantes con distintas responsabilidades comerciales para abordar distintos tipos de incidentes de seguridad; tome en cuenta lo siguiente: * Gerencia * Seguridad física * Seguridad de la información * Equipo de redes * Recursos Humanos * Departamento jurídico * Proporcione capacitación para que los miembros del equipo de **respuesta a incidentes** comprendan sus funciones y responsabilidades al enfrentar incidentes. |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| MS-5.2 | Respuesta a incidentes | Establezca un proceso de notificación de incidentes de seguridad para que el personal pueda dar cuenta de incidentes identificados al equipo de **respuesta a incidentes**. | * Considere implementar una línea telefónica anónima o un sitio web que se pueda usar para informar de actividades inapropiadas y/o sospechosas. * Considere implementar una dirección de correo electrónico grupal para informar incidentes a todos los miembros del equipo de respuesta a incidentes. * Considere hacer uso de la línea telefónica para datos de la MPAA para recibir datos anónimos sobre actividades sospechosas (consulte la información de contacto de la línea para datos con atención las 24 horas en el Anexo H). |
| MS-5.3 | Notifique los incidentes en forma oportuna a los clientes cuyos contenidos puedan haber sido filtrados, hurtados o comprometidos de algún modo (por ej., activos extraviados de los clientes) y sostenga una reunión tras el incidente con la gerencia y el cliente. | * Implemente un proceso de notificación de infracción de la seguridad que incluya el uso de formularios de notificación. * Solicite la participación del departamento jurídico para determinar las medidas correctas que se deben tomar para informar la pérdida de contenidos a los clientes afectados. * Analice las lecciones aprendidas del incidente e identifique las mejoras al plan y al proceso de respuesta al incidente. * Realice un análisis de causa original para identificar las vulnerabilidades de la seguridad que hicieron posible el incidente. * Identifique e implemente medidas de control paliativas para evitar la repetición de incidentes similares. * Informe los resultados del análisis posterior al incidente, incluso el plan de medidas paliativas, a los clientes afectados. |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| MS-6.0 | Continuidad del negocio y recuperación ante desastres | Establezca un plan formal que describa las acciones a tomar para garantizar la continuidad del negocio. | * Considere incluir las siguientes secciones en el plan de **continuidad del negocio**: * Amenazas a contenidos y activos críticos, incluso la pérdida de energía y telecomunicaciones, la falla de sistemas, los desastres naturales, etc. * Sistema de información detallada, procedimientos de respaldo de metadatos y contenido, y documentación del sistema informático, incluso configuración de dispositivos de Red de área amplia (Wide Area Network, WAN) y Red de área local (Local Area Network, LAN)/Red interna críticos. * Codificación de respaldos (al menos codificación AES de 128 bit). * Fuente de energía de respaldo para mantener al menos 15 minutos del sistema CCTV, sistema de alarmas y sistemas informáticos críticos, incluso software para realizar un apagado seguro de los sistemas críticos. * Considere usar una ubicación de respaldo fuera del sitio. * Notificación al equipo de seguridad. * Notificación escalada a la gerencia. * Análisis de impacto y prioridad. * Contención del impacto. * Prioridades para la recuperación y procedimientos de recuperación detallados, incluso soluciones alternativas manuales y detalles de configuración de sistemas restaurados. * Información de contactos claves. * Notificación a clientes y socios comerciales afectados. * Pruebas de continuidad del negocio y procesos de recuperación ante desastres al menos en forma anual. |
| MS-6.1 | Identifique el equipo de continuidad del negocio responsable de detectar, analizar y remediar incidentes de continuidad. | * Incluya responsabilidades y funciones definidas. * Proporcione capacitación para que los miembros del equipo de continuidad del negocio comprendan sus funciones y responsabilidades. |
| MS-7.0 | Control de cambio y gestión de la configuración | Establezca políticas y procedimientos para garantizar que los nuevos datos, aplicaciones, red y componentes de sistemas hayan sido preaprobados por la directiva del negocio. | * Incluya documentación que describa la instalación, la configuración y el uso de dispositivos, servicios y características, y actualice la documentación según sea necesario. * Documente políticas y procedimientos para tratar con problemas conocidos. * Incluya políticas y procedimiento para informar vulnerabilidades de errores y seguridad. * Restrinja y vigile la instalación de hardware o software no autorizado. * Administre los riesgos asociados con cambios de datos, aplicaciones, infraestructura de redes y sistemas. * Documente y guarde todas las solicitudes de cambio, resultados de pruebas y aprobaciones de gerencia. |
| MS-8.0 | Flujo de trabajo | Documente **flujos de trabajo** que incluyan el seguimiento de contenidos y puntos de autorización. Incluye los siguientes procesos para el contenido físico y digital:   * Entrega (recepción/devolución) * Ingreso * Movimiento * Almacenamiento * Eliminación/Destrucción | * Use diagramas de flujo de procesos para documentar **flujos de trabajo.** * Incluya el procesamiento de activos y el tratamiento de la información cuando corresponda. * Evalúe cada punto de contacto en busca de riesgo de contenido. * Implemente medidas de control en torno a los puntos de autorización. * Identifique controles de aplicaciones relacionados. |
| MS-8.1 | Actualice el **flujo de trabajo** cuando existan cambios en el proceso y revise el proceso de **flujo de trabajo** al menos en forma anual para identificar cambios. | * Realice un seguimiento del **flujo de trabajo** de contenidos y de medidas de control implementadas para cada proceso a fin de identificar las áreas vulnerables. |
| MS-9.0 | Separación de responsabilidades | Separe las responsabilidades dentro del **flujo de trabajo** de contenidos. Implemente y documente formas de control compensatorias cuando no se puedan separar las responsabilidades. | * Documente las funciones y responsabilidades para eliminar la superposición de ciertas funciones laborales, como: * **Personal de bóvedas** y de servidor/sala de máquinas * Personal de envío y de recepción * Movimiento de activos dentro de los establecimientos (por ej., mensajeros) desde las **bóvedas** y desde el área de contenidos/producción * **Acceso a la carpeta de activos digitales** (por ej., el administrador de datos configura el acceso para el productor) * Personal de transferencia de contenidos desde el personal de producción * Separe las responsabilidades con controles manuales (por ej., aprobación del productor antes de trabajar en contenidos) o controles automáticos en el sistema de ordenación del trabajo (por ej., aprobación automática para cada etapa del **flujo de trabajo**) * Implemente formas de control compensatorias cuando no se pueda realizar la separación, como por ejemplo: * Vigile las actividades del personal de la empresa y/o empleados de agencias externas. * Retenga y revise las bitácoras de fiscalizaciones. * Implemente una separación física. * Haga cumplir la supervisión de la gestión. |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| MS-10.0 | Verificación de antecedentes | Realice verificaciones de antecedentes a todo el **personal de la empresa** y a **empleados de agencias externas.** | * Realice verificaciones de antecedentes de conformidad con las leyes, normas, estatutos sindicales y consideraciones culturales relevantes. * Verifique los antecedentes de posible **personal de la empresa** y de **empleados de agencias externas** con métodos que son proporcionales a las necesidades comerciales, la sensibilidad de los contenidos que accedan y los posibles riesgos de hurto o filtración de los contenidos. * Verifique los antecedentes personales, académicos y profesionales cuando sea necesario. * Si la ley no permite la verificación de antecedentes, documéntelo como una excepción y use las referencias de los postulantes. |
| MS-11.0 | Acuerdos de confidencialidad | Exija que todo el **personal de la empresa** firme un acuerdo de confidencialidad (por ej., uno de no divulgación) al ser contratados y una vez al año en lo sucesivo, el cual debe incluir instrucciones sobre cómo tratar y proteger los contenidos. | * Incluya instructivos sobre la prohibición de divulgación con respecto a la confidencialidad luego de la finalización de la relación laboral o contrato. * Explique la importancia de la confidencialidad/acuerdo de no divulgación en términos comunes, si fuese necesario. * Asegúrese de que toda la información importante de equipos usados por **personal de la empresa** para tratar contenidos comerciales delicados se transfiera a la organización y se eliminen en forma segura de los equipos. * La gerencia debe retener los acuerdos de confidencialidad firmados de todo el **personal de la empresa.** |
| MS-11.1 | Solicite que todo el **personal de la empresa** devuelva todos los contenidos e información de clientes que se encuentre en su posesión tras la finalización de la relación laboral o contrato. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| MS-12.0 | Uso y verificación de agencias externas | Exija que todos los **empleados de agencias externas** (por ej., trabajadores independientes) que manejen contenidos, firmen acuerdos de confidencialidad (por ej., de no divulgación) al inicio de las labores. | * Incluya guías sobre no divulgación en las políticas relacionadas con la confidencialidad durante y después del empleo, acuerdo o contrato. * Explique la importancia de la confidencialidad/acuerdo de no divulgación en términos comunes, si fuese necesario. * Asegúrese de que toda la información importante de equipos usados por **empleados de agencias externas** para tratar contenidos comerciales delicados se transfiera a la organización y se eliminen en forma segura de los equipos. * La gerencia debe retener los acuerdos de confidencialidad firmados de todos los **empleados de agencias externas**. * Incluya requisitos para manejar y proteger contenido. |
| MS-12.1 | Solicite que todos los **empleados de agencias externas** devuelvan todos los contenidos e información de clientes que se encuentre en su posesión tras la finalización del contrato. |  |
| MS-12.2 | Incluya requisitos de seguridad en los contratos de empleados de agencias externas. | * Solicite que los **empleados de agencias externas** cumplan con los requisitos de seguridad especificados en los contratos de empleados de agencias externas y los requisitos de los clientes. * Incluya una cláusula que le otorgue derecho a fiscalizar las actividades que involucren contenidos delicados. * Implemente un proceso para vigilar el cumplimiento de los requisitos de seguridad. |
| MS-12.3 | Implemente un proceso para recuperar **contenido** al finalizar la relación laboral. | * Asegúrese de que todo el **contenido** de equipos de empleados de agencias externas se transfiera a la organización y se elimine en forma segura del equipo. |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| MS-12.4 | Uso y verificación de agencias externas | Solicite que los **empleados de agencias externas** cuenten con seguros cuando sea pertinente (por ej., servicios de transporte). | * Solicite que los **empleados de agencias externas** presenten evidencia de seguros y mantenga un registro de los proveedores de seguros y de los números de póliza. * Solicite que el seguro de los empleados de agencias externas tenga un cierto nivel de cobertura. * Solicite actualizaciones anuales de la información cuando los contratos se renueven. |
| MS-12.5 | Restrinja el acceso de empleados de agencias externas a las áreas de contenidos/producción, salvo que sea necesario para sus funciones. | * Asegúrese de que los **empleados de agencias externas** no tengan acceso electrónico a las áreas donde se almacenen contenidos. * Acompañe a los **empleados de agencias externas** (por ej., equipos de limpieza) cuando el acceso a áreas restringidas (por ej., **bóvedas**) sea necesario. |
| MS-12.6 | Notifique a los clientes si se utilizan **subcontratistas** para manejar el contenido u otra compañía se encarga del trabajo. | * Solicite la aprobación/confirmación del cliente por escrito. * Solicite que los subcontratistas repasen las actividades estándares de **debida diligencia**. * El trabajo a cargo de otra compañía debe ser informado a los estudios de los miembros de la MPAA y se debe completar y proporcionar el Cuestionario del proveedor de la MPAA a los estudios de los miembros para la debida diligencia. |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| PS-1.0 | Puntos de entrada y salida | Asegure todos los puntos de entrada y salida del establecimiento en todo momento, incluso ventanas y puertas de las zonas de carga. | * Permita que los puntos de entrada y salida estén sin llave durante las horas hábiles si el área de recepción está separada del resto del establecimiento con puertas de acceso controlado. |
| PS-1.1 | Controle el acceso a áreas en donde se gestionan contenidos separando el área de contenidos de otras áreas del establecimiento (por ej., oficinas administrativas, salas de espera, zonas de carga, áreas de recolección y entrega de transporte, duplicación y masterización). | * Permita el acceso a áreas de contenidos/producción cuando sea necesario solamente. * Solicite que las salas empleadas para fines de proyección tengan acceso controlado (por ej., las cabinas de proyección). * Restrinja el acceso a salas donde haya reproductores de **medios** (por ej., Blu-ray, DVD). * Haga cumplir un modelo de separación de responsabilidades que restrinja el acceso de cualquier persona a ambas habitaciones, tanto de duplicación como de masterización. |
| PS-1.2 | Controle el acceso en donde existan negocios en un establecimiento, lo que incluye, entre otros, lo siguiente:   * Separar áreas de trabajo. * Implementar entradas y salidas de acceso controlado que se puedan segmentar por unidad comercial. * Registrar y vigilar todas las entradas y salidas dentro de un establecimiento. * Se deben informar todos los locatarios al cliente antes del inicio de las labores. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| PS-2.0 | Entrada y salida de visitantes | Mantenga un registro detallado de los visitantes e incluya lo siguiente:   * Nombre * Empresa * Hora de entrada y salida * Persona(s) visitada(s) * Firma del visitante * Número de tarjeta asignada | * Compruebe la identidad de todos los visitantes con una forma válida de identificación con foto (por ej., licencia de conducir o identificación emitido por el estado). * Considere ocultar los nombres de visitantes anteriores. |
| PS-2.1 | Asigne una **tarjeta de identificación** o un autoadhesivo, el cual debe estar siempre a la vista, a cada visitante y retírelos a la salida. | * Haga que las tarjetas de visitantes se distingan fácilmente de las tarjetas del **personal de la empresa** (por ej., tarjetas codificadas en plástico de color). * Considere la rotación diaria de las tarjetas de papel o el color de los autoadhesivos. * Considere usar tarjetas que cambien de color al caducar. * Registre la asignación de tarjetas a la entrada y salida. * Las tarjetas de visitantes deben tener números secuenciales y se las debe asignar en orden. * Cuente las tarjetas diariamente. |
| PS-2.2 | No brinde acceso con tarjeta a las áreas de contenidos/producción a los visitantes. |  |
| PS-2.3 | Exija que los visitantes sean acompañados por empleados autorizados mientras estén en el establecimiento o en áreas de contenidos/producción. |  |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| PS-3.0 | Identificación | Entregue al **personal de la empresa** y a los **empleados de agencias externas** con antigüedad (por ej., conserjes) **tarjetas** de **identificación** con foto que deberán estar visibles constantemente. | * Entregue **tarjetas de identificación** con foto a todo el **personal de la empresa** y a **empleados de agencias externas** con antigüedad luego de realizar una verificación de antecedentes. * Establezca e implemente un proceso para recuperar inmediatamente las **tarjetas de identificación** con foto tras la finalización de las relaciones laborales. * Considere omitir la ubicación, nombre de la compañía, logotipo y otra información específica en la **tarjeta de identificación** con foto. * Considere usar la **tarjeta de identificación con foto** como tarjeta de acceso cuando sea posible. * Exija que los empleados den cuenta de inmediato de **tarjetas de identificación con foto** extraviadas o hurtadas. * Proporcione un número telefónico o sitio web con atención todos los días y a cualquier hora para informar **tarjetas de identificación con foto** extraviadas o hurtadas. * Capacite y aliente a los empleados a detener a personas sin una identificación visible. |
| PS-4.0 | Seguridad del perímetro | Implemente controles de seguridad del perímetro que aborden los riesgos a los que pueden estar expuestos los establecimientos según lo descubierto por la **evaluación de riesgos** de la organización. | * Implemente medidas de control de la seguridad según la ubicación y disposición de los establecimientos, tales como: * Restringir el acceso al perímetro con murallas, rejas y/o portones que, como mínimo, estén asegurados en los períodos de receso; las murallas y rejas deben ser de por lo menos 2,5 metros (8 pies). * Asegurar y rodear, según las necesidades, las áreas comunes externas, como áreas para fumadores y balcones abiertos. * Cobertura con cámaras de las áreas comunes externas (por ej., las áreas para fumadores), así como de los estacionamientos. * Ser consciente de que el uso exagerado de señalización de la empresa podría convertirla en un objetivo para delincuentes. * Usar alarmas alrededor del perímetro si fuese necesario. |
| PS-4.1 | Coloque guardias de seguridad en las entradas del perímetro y puntos de entrada y salida regulares. |  |
| PS-4.2 | Seguridad del perímetro | Implemente un proceso de ronda diario de seguridad con un horario al azar e ingrese los resultados de las rondas en una bitácora. | * Solicite a los guardias de seguridad que patrullen tanto las áreas interiores como las exteriores. * Se debe revisar las salidas de emergencia, incluso la verificación de los sellos. * Considere usar un sistema de vigilancia de las rondas de los guardias para darle seguimiento a las rondas (por ej., un punto de verificación) y verifique las cerraduras. |
| PS-4.3 | Cierre con llave las puertas del perímetro en todo momento. | * Implemente un brazo electrónico activado por el personal de seguridad a fin de controlar el ingreso de vehículos al recinto. * Distribuya permisos para estacionar al personal de la empresa y a los empleados de agencias externas que hayan llenado los formularios correspondientes. * Solicite que los vehículos de los visitantes cuenten con identificación y asegúrese de que todos los visitantes hayan sido autorizados previamente a ingresar a las instalaciones. |
| PS-5.0 | Alarmas | Instale un sistema de alarmas centralizado y audible que cubra todos los puntos de entrada y salida (incluso salidas de emergencia), ventanas, zonas de carga, salidas de incendio y áreas restringidas (por ej., **bóvedas**, servidores/sala de máquinas, etc.). | * Coloque alarmas en todas las entradas para alertar al personal de seguridad cuando ocurra un ingreso no autorizado a los establecimientos. * Active la alarma cuando el establecimiento esté sin supervisión. |
| PS-5.1 | Instale de forma eficaz sensores de movimiento en las áreas restringidas (por ej., **bóvedas**, servidor/sala de máquinas) y configúrelos para que den una alerta adecuada al personal de seguridad y de otro tipo (por ej., gerentes de proyecto, productor, jefe editorial, equipo de respuesta a incidentes, etc.). | * Asegúrese de que el sistema de alarmas cubra las áreas de almacenamiento y **bóvedas** (por ej., a través de sensores de movimiento) después del horario hábil regular a modo de medida adicional de seguridad. |
| PS-5.2 | Instale alarmas con sensores para puertas en las áreas restringidas (por ej., bóvedas, servidor, sala de máquinas) de modo que anuncien cuando los puntos de entrada y salida delicados estén abiertos por un plazo superior a uno predeterminado (por ej., 60 segundos). | * Configure las puertas de acceso controlado para que activen las alarmas y alerten al personal de seguridad cuando las puertas permanezcan abiertas durante un período prolongado. |
| PS-5.3 | Alarmas | Configure las alarmas de modo que den notificaciones escaladas directamente al personal a cargo de la seguridad y de otro tipo (por ej., gerentes de proyecto, productor, jefe editorial, equipo de respuesta a incidentes, etc.). | * Establezca e implemente procedimientos escalados a seguir si no se recibe una respuesta oportuna de parte del personal de seguridad tras la notificación. * Considere implementar la notificación automática a las fuerzas del orden en cuanto ocurra una violación de la seguridad. * Implemente procedimientos de notificación durante los fines de semana y luego de las horas hábiles. |
| PS-5.4 | Asigne códigos de habilitación y deshabilitación únicos a cada persona que requiera acceso al sistema de alarmas, y restrinja el acceso al resto del personal. | * Use códigos de alarmas únicos para saber qué miembro del personal de seguridad tenía la responsabilidad de habilitar y deshabilitar la alarma. * Actualice los códigos asignados de las alarmas en intervalos aprobados por la gerencia para reducir el riesgo asociado con compartir y perder códigos. |
| PS-5.5 | Revise la lista de usuarios que pueden habilitar y deshabilitar los sistemas de alarmas en forma trimestral o al momento del cambio de personal. | * Elimine a los usuarios que hayan dejado la empresa o que hayan asumido funciones laborales distintas. * Desactive los códigos de alarmas que fueron asignados a usuarios eliminados. |
| PS-5.6 | Ponga a prueba el sistema de alarmas en forma trimestral. | * Simule una violación de la seguridad física y asegúrese de lo siguiente: * El sistema de alarma detecta la violación de la seguridad. * El personal de seguridad recibe la alerta. * El personal de seguridad responde en forma oportuna de acuerdo a los procedimientos. |
| PS-5.7 | Implemente medidas de protección contra incendios para que en caso de un apagón, las puertas de salida de emergencia no abran y todas las otras no cierren para evitar el acceso no autorizado. |  |
| PS-6.0 | Autorización | Registre e implemente un proceso para gestionar el acceso a los establecimientos y mantenga un registro de los cambios a los **derechos de acceso.** | * Designe una persona para autorizar el acceso a los establecimientos. * Notifique al personal correspondiente (por ej., gerencia de los establecimientos) de los cambios en el estatus del empleado. * Elabore un formulario físico o electrónico que debe llenar un supervisor para solicitar acceso a los establecimientos para **personal de la empresa** y/o **empleados de agencias externas.** * Asigne la responsabilidad de investigar y aprobar las solicitudes de acceso. |
| PS-6.1 | Restrinja el acceso a los sistemas de producción al personal autorizado únicamente. |  |
| PS-6.2 | Evalúe el acceso a las áreas restringidas (por ej., **bóvedas**, servidor/sala de máquinas) trimestralmente y cuando las funciones o el estatus del **personal de la empresa** y/o de los **empleados de agencias externas** cambien. | * Valide el estado del personal de la empresa y de los empleados de agencias externas. * Elimine los derechos de acceso de usuarios que ya no prestan servicios. * Verifique que el acceso siga siendo apropiado para la función laboral de los usuarios. |
| PS-7.0 | Control de acceso electrónico | Implemente acceso electrónico en todo el establecimiento para cubrir todos los puntos de entrada y salida y todas las áreas de almacenamiento, transmisión o procesamiento de contenidos. | * Asigne acceso electrónico a áreas específicas de los establecimientos según las funciones laborales y responsabilidades. * Actualice el acceso electrónico según corresponda cuando las funciones cambien o al finalizar la relación laboral del personal de la empresa y de empleados de agencias externas. * Mantenga un registro que ilustre el número del dispositivo de acceso electrónico asignado al personal de la empresa. * Consulte Ingreso y vigilancia PS-10.0 * Revise en qué ocasiones no se requiere acceso electrónico para las áreas comunes (por ej., ascensores públicos). |
| PS-7.1 | Control de acceso electrónico | Restrinja la administración del sistema de acceso electrónico al personal correspondiente. | * Restrinja la administración del sistema electrónico al personal designado, y no permita que ninguna persona acceda a los contenidos de producción para realizar tareas administrativas relacionadas con el acceso electrónico. * Asigne un equipo independiente que administre y gestione el acceso electrónico. |
| PS-7.2 | Guarde las tarjetas y los **dispositivos de acceso electrónico** (por ej., tarjetas de acceso, portallaves) en un armario con cerradura y asegúrese de que los **dispositivos de acceso electrónico** permanezcan deshabilitados antes de ser asignados al personal. Guarde los dispositivos de acceso electrónico no asignados (por ej., tarjetas de acceso, portallaves) en un armario con cerradura y asegúrese de que permanezcan deshabilitados antes de ser asignados al personal. | * Limite el acceso al armario con cerradura al equipo de administración del sistema de **tarjetas de acceso**/**dispositivo de acceso electrónico**. * Solicite la firma de quienes retiren inventario. |
| PS-7.3 | Deshabilite en el sistema los **dispositivos** de acceso electrónico(por ej., tarjetas de acceso, portallaves) extraviados antes de emitir un nuevo **dispositivo de acceso electrónico**. | * Indique al **personal de la empresa** y a los **empleados de agencias externas** que den cuenta de **dispositivos de acceso electrónico** extraviados de inmediato para evitar el acceso no autorizado a los establecimientos. * Solicite una identificación antes de emitir **dispositivos de acceso electrónico** de reemplazo. |
| PS-7.4 | Emita **dispositivos de acceso electrónico a terceros** con una fecha de caducidad fija (por ej., 90 días) según un marco referencial aprobado. | * Asegúrese de que los **dispositivos de acceso electrónico** a **terceros** puedan ser fácilmente distinguidos de los **dispositivos de acceso electrónico** del personal de la empresa * Asegúrese de que la fecha de caducidad se pueda distinguir fácilmente en los **dispositivos de acceso electrónico**. * Asigne **dispositivos de acceso electrónico** para terceros, solo cuando sea necesario. |
| PS-8.0 | Llaves | Limite la entrega de **llaves maestras** y/o llaves para áreas restringidas al personal autorizado únicamente (por ej., propietario, gerencia de los establecimientos). | * Mantenga un listado del **personal de la empresa** autorizado a sacar las **llaves maestras.** * Actualice el listado en forma periódica para eliminar **personal de la empresa** que ya no necesite acceso a las **llaves maestras.** |
| PS-8.1 | Implemente un proceso de ingreso y salida para rastrear y vigilar la entrega de las **llaves maestras y/o llaves para áreas restringidas.** | * Mantenga registros para darle seguimiento a la siguiente información: * **Personal de la empresa** que esté en posesión de cada una de las llaves maestras * Hora de ingreso y salida * Motivo de la salida * Solicite la devolución de las **llaves maestras** en un plazo determinado, e identifique dónde se encuentran las llaves que no fueron devueltas a tiempo. |
| PS-8.2 | Use llaves que solo pueda copiar un cerrajero específico para los puntos externos de entrada y salida. | * Use llaves de alta seguridad (cilindros) que ofrecen más resistencia a dos o más de los siguientes métodos: * Uso de ganzúas * Copiado con moldes * Duplicación de llaves * Perforación * Otras formas de ingreso forzado |
| PS-8.3 | Haga un inventario de las **llaves maestras** y de las llaves para las áreas restringidas, incluidos los puntos de entrada y salida de los establecimientos, en forma trimestral. | * Identifique, investigue y atienda el problema de llaves extraviadas o robadas. * Revise las bitácoras para determinar quién fue el último en tomar una llave que se encuentra extraviada. * Cambie las cerraduras cuando se extravíen **llaves maestras** o llaves para áreas restringidas. |
| PS-8.4 | Obtenga todas las llaves de los empleados/terceros que ya no presten servicios o aquellos que ya no necesitan el acceso. |  |
| PS-8.5 | Llaves | Implemente control de acceso electrónico o vuelva a generar otras llaves para todo el establecimiento cuando la llave maestra o submaestra se extravíe. |  |
| PS-9.0 | Cámaras | Instale un sistema de **CCTV** que grabe todos los puntos de entrada y salida de los establecimientos y de las áreas restringidas (por ej., servidor/sala de máquinas, etc.). | * Se debe esconder discretamente la instalación y el cableado y no debe encontrarse dentro del alcance razonable. * El establecimiento no debe asumir que el circuito cerrado de televisión (CCTV) proporcionado por el edificio es adecuado. * Coloque cámaras en todas las entradas del establecimiento. * Asegúrese de que las cámaras cubran las áreas de almacenamiento y **bóvedas**. |
| PS-9.1 | Revise el posicionamiento de las cámaras y las grabaciones para garantizar la cobertura adecuada, la función, la calidad de la imagen, la iluminación y la frecuencia de las fotos de las grabaciones de vigilancia al menos en forma diaria. | * Revise el posicionamiento de las cámaras para asegurarse de que la visión de los puntos de entrada y salida y de otras zonas delicadas no esté bloqueada. * Busque soluciones para las cámaras en lugares oscuros (por ej., cámaras para poca luz o con infrarrojo, luces detectoras de movimiento). * Revise la calidad de la imagen para asegurarse de que la iluminación sea la correcta y que se puedan distinguir los rostros. * Revise la frecuencia de las fotos para asegurarse de que se graban bien las actividades. * Coloque las cámaras de forma tal que no se grabe ningún contenido a la vista. * Grabe con una resolución suficiente para poder identificar los rasgos faciales. * Grabe con una frecuencia mínima de 7 fotogramas por segundo. |
| PS-9.2 | Restrinja el acceso físico y lógico a la **consola de CCTV** y a los equipos de **CCTV** (por ej., videograbadoras) únicamente al personal responsable de administrar y vigilar el sistema. | * Coloque los equipos de **CCTV** en un lugar de acceso controlado seguro (por ej., sala de computación, armario con cerradura, jaula). * Realice revisiones de acceso en forma periódica para asegurarse de que solo las personas correspondientes tengan acceso al equipo de vigilancia. * Asegúrese de que la consola web para sistemas de **CCTV** con IP cuente con acceso restringido solo al personal autorizado y de que existan medidas de control para la gestión de cuentas (por ej., complejidad de las contraseñas, ingreso individual por usuarios, registros y vigilancia). |
| PS-9.3 | Cámaras | Asegúrese de que la grabación de las cámaras incluya la fecha y la hora correcta y mantenga las grabaciones de vigilancia por **CCTV** y las bitácoras de acceso electrónico al menos por 90 días, o el máximo plazo permitido por la ley, en un lugar seguro. | * Indique la hora y la fecha en el **medio** físico empleado para las grabaciones de las cámaras que se guarde en cinta o disco. * Asegúrese de que se mantenga la hora correcta en los equipos grabadores de las cámaras digitales. * Revise la fecha y la hora correcta para comprobar su exactitud al menos en forma semanal. * Considere guardar las bitácoras en un armario de telecomunicaciones con acceso controlado o en la sala de computación. * Determine el espacio típico necesario para un día de registro y asegúrese de que el tamaño del registro sea lo suficientemente grande como para almacenar datos durante al menos 90 días, o el plazo máximo de retención permitido por la ley. * Considere retener las grabaciones de vigilancia por CCTV hasta la fecha de lanzamiento de la primera producción. |
| PS-9.4 | Designe a un empleado o a un grupo de empleados para que observen las imágenes durante las horas hábiles e inmediatamente investiguen los incidentes de seguridad detectados. | * Incorpore el proceso de respuesta a incidentes para gestionar los incidentes de seguridad. * Considere agregar un monitor de vigilancia en la mesa de recepción o en la oficina de TI. |
| PS-10.0 | Ingreso y vigilancia | Anote y evalúe el acceso electrónico a las áreas restringidas para detectar eventos sospechosos al menos en forma semanal. | * Identifique y documente los eventos que se consideren sospechosos. * Considere la implementación de un proceso de notificación automático que envíe alertas en tiempo real al personal de seguridad correspondiente cuando se detecte actividades de acceso electrónico sospechosas. * Guarde las bitácoras como mínimo un año. * Registre y evalúe los siguientes eventos: * Intentos de acceso fallidos repetidos. * Acceso inusual para la hora del día. * Acceso sucesivo a la puerta en distintas zonas. |
| PS-10.1 | Ingreso y vigilancia | Anote y evalúe el acceso electrónico al menos en forma diaria para las siguientes áreas:   * Bóvedas de originales y prensas de estampado. * Premasterización. * Servidor/sala de máquinas. * Sala de residuos. * Jaulas de alta seguridad. | * Identifique y registre los eventos que se consideran inusuales. * Considere la implementación de un proceso de notificación automático que envíe alertas en tiempo real al personal de seguridad correspondiente cuando se detecte actividades de acceso electrónico sospechosas. |
| PS-10.2 | Investigue las actividades de acceso electrónico sospechosas que se detecten. | * Identifique y comunique contactos claves que deban ser notificados al detectar actividades de acceso electrónico inusuales. * Establezca e implemente procedimientos escalados que se deban seguir si los contactos principales no responden a la notificación del evento en forma oportuna. |
| PS-10.3 | Mantenga un registro en curso de todos los incidentes de acceso electrónico confirmados e incluya la documentación de toda actividad de seguimiento realizada. | * Aproveche el formulario para notificar **respuestas a incidentes** para registrar los incidentes con **tarjeta de acceso/dispositivo de acceso electrónico** confirmado. * Revise todos los incidentes recientes con **tarjetas de acceso** **/dispositivo de acceso electrónico** en forma periódica y realice análisis de causa original para identificar vulnerabilidades y soluciones adecuadas. |
| PS-11.0 | Inspecciones | Establezca una política, según lo permitido por las leyes locales, que permita que la seguridad busque al azar personas, bolsas, paquetes y elementos personales para el contenido de clientes. | * Comunique las políticas sobre inspecciones a todo el **personal de la empresa** y a los **empleados de agencias externas.** * Realice inspecciones en forma periódica al **personal de la empresa** y a los **empleados de agencias externas** para validar la política. |
| PS-11.1 | Inspecciones | Implemente un proceso de inspección a la salida que se pueda aplicar a todo el personal y visitantes al establecimiento, incluso:   * Quitarse los abrigos, gorros y cinturones para realizar una inspección. * Sacarse todos los artículos de los bolsillos. * Realizar una inspección por encima de la ropa con la supervisión del personal de seguridad. * Inspección minuciosa de todos los bolsos. * Inspección de bandejas de CD/DVD de las computadoras portátiles. * Exploración con detectores manuales de metales que se colocan a unas tres pulgadas de la persona. | * Indique a los guardias de seguridad que busquen artículos que se prohíbe sacar del recinto (por ej., cámaras) o material fílmico que no se puede sacar del recinto sin la autorización correspondiente. * Informe las políticas sobre inspecciones de salida a todo el personal de la empresa y los empleados de agencias externas. * Realice los cambios de turnos en forma alternada para evitar largas filas y tiempos de espera excesivos. |
| PS-11.2 | No permita que el personal ingrese o salga del establecimiento con dispositivos digitales de grabación (por ej., unidades **USB**, cámaras digitales, teléfonos celulares) e incluya la búsqueda de tales artículos en el procedimiento de inspección a la salida. | * Confisque todos los dispositivos digitales de grabación que se detecten y guárdelos en casilleros seguros. * Registre todo incidente de intento de hurto de contenidos. * Tome las medidas disciplinarias necesarias contra quienes intenten hurtar contenidos. * Implemente y haga cumplir una política que prohíba los dispositivos móviles o celulares con funcionalidad digital de grabación. * Permita el uso de teléfonos celulares con funcionalidad digital de grabación si se usan etiquetas adhesivas a prueba de adulteraciones. |
| PS-11.3 | Haga cumplir el uso de bolsas plásticas y contenedores de comida transparentes para transportar cualquier tipo de alimento a las áreas de producción. | * Considere designar un área para consumir alimentos fuera del área de producción. |
| PS-11.4 | Implemente una política de código de vestir que prohíba el uso de atuendos demasiado grandes (por ej., pantalones holgados, sudaderas con capucha de varias tallas más grandes). |  |
| PS-11.5 | Use etiquetas adhesivas u hologramas numerados a prueba de adulteraciones para identificar los dispositivos autorizados que puedan ingresar y salir del establecimiento. |  |
| PS-11.6 | Inspecciones | Implemente un proceso para poner a prueba el procedimiento de inspección a la salida. | * Realice fiscalizaciones periódicas al proceso de inspección para asegurarse de que los guardias de seguridad lo realicen correctamente. * Identifique formas de mejorar el proceso de inspección a la salida. * Registre todas las fiscalizaciones y mejoras al proceso de inspección. |
| PS-11.7 | Realice un proceso de inspección de vehículos al azar a la salida del estacionamiento. |  |
| PS-11.8 | Separe las líneas de duplicación que procesan contenidos muy delicados y realice inspecciones al salir de las áreas separadas de salida. |  |
| PS-11.9 | Implemente medidas adicionales de control para vigilar las actividades de los guardias de seguridad. | * Revise el proceso de inspección a la salida para los guardias de seguridad a la salida. * Separe las responsabilidades de los guardias de seguridad en la supervisión de la planta y las áreas de producción de los puntos de salida (por ej., proceso de inspección). |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| PS-12.0 | Seguimiento del inventario | Implemente un sistema de gestión de activos de los contenidos para tener un seguimiento detallado de los bienes físicos (es decir, recibidos del cliente y creado en el establecimiento). | * Solicite un formulario de descargo de responsabilidades u orden de trabajo para confirmar que los contenidos pueden ser sacados por una persona específica. * Solicite que las personas presenten una identificación para fines de autenticación. * Solicite una etiqueta (por ej., código de barras, identificación única) para todos los activos. * Registre todos los activos que sean sacados o devueltos. * Registre la duración esperada de cada préstamo. * Considere el uso de una alerta automatizada para proporcionar notificaciones de activos que no hayan sido devueltos al final del día laborable o del período de tiempo autorizado. * Haga un seguimiento de las personas que tienen activos en su poder que no han devuelto. * Registre la ubicación de cada activo. * Registre la fecha y hora de cada transacción. |
| PS-12.1 | Identifique los activos de clientes y los medios creados (por ej., cintas, discos duros) con código de barra o números de identificación únicos asignados al recibirlos y guarde los activos en la bóveda cuando no estén en uso. | * Use doble códigos de barra para darle seguimiento a los activos (es decir, coloque códigos de barra en el activo y el contenedor o caja). * Envíe los activos directamente a la **bóveda** luego de haber sido verificados con código de barras y devuélvalos a la **bóveda** inmediatamente cuando no se los necesite. |
| PS-12.2 | Guarde los registros de las transacciones de movimiento de los activos durante al menos un año. | * Guarde las bitácoras físicas o digitales de todos los movimientos de activos; las bitácoras deben incluir: * Código de barra o identificación única del activo que se sacó o se devolvió. * Hora y fecha del préstamo o de la devolución. * Nombre y número de identificación único de la persona que sacó un activo. * Razón del préstamo. * Ubicación del activo. |
| PS-12.3 | Seguimiento del inventario | Revise las bitácoras del sistema de **gestión de activos** de contenidos al menos en forma semanal e investigue las anormalidades. | * Identifique los activos que no hayan sido devueltos a la fecha de devolución esperada. * Haga un seguimiento de las personas que sacaron los activos faltantes. * Implemente procedimientos disciplinarios para quienes no respeten las políticas de **gestión de activos**. * Considere implementar notificaciones automáticas cuando los activos sean sacados por períodos prolongados. |
| PS-12.4 | Use el alias del título de la película de los estudios cuando sea oportuno en los activos físicos y en los sistemas de seguimiento de los activos. | * Considere eliminar los nombres de los estudios en los activos físicos cuando corresponda. |
| PS-12.5 | Implemente y evalúe un informe diario de antigüedad para identificar los activos muy delicados que se saquen de la **bóveda** y no se devuelvan. | * Realice informes diarios de antigüedad ya sea manualmente o con un sistema de **gestión de activos**. * Investigue todas las excepciones. |
| PS-12.6 | Cierre con llave y registre los activos que estén retrasados o se devuelvan si no se pudo entregar los envíos a tiempo. | * Establezca un procedimiento para almacenar activos en un área de acceso controlado. * Mantenga la documentación que detalle el almacenamiento de activos en el recinto, incluso la fecha y el motivo del almacenamiento. |
| PS-13.0 | Recuentos de inventario | Realice un inventario trimestral de los activos de cada cliente, compárelo con los registros de la **gestión de activos** e inmediatamente informe las diferencias a los clientes. |  |
| PS-13.1 | Separe las responsabilidades entre el personal de la **bóveda** y las personas responsables de realizar los recuentos de inventario. | * Asigne personal ajeno a la **bóveda** para que realice verificaciones al azar del recuento de inventario. |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| PS-14.0 | Rastreo de medios vírgenes y materiales de inventario | Etiquete (por ej., con código de barras, identificador único asignado) los medios vírgenes y materiales de inventario por unidad al recibirlos. | * No permita la presencia de **medios** vírgenes o materiales de inventario en áreas aseguradas de producción salvo que se necesiten para fines de producción. |
| PS-14.1 | Establezca un proceso para darle seguimiento al consumo de materia prima (por ej., policarbonato) en forma mensual. | * Compare los materiales de inventario actuales y las órdenes de trabajo para identificar diferencias en el inventario. * Establezca un umbral de varianza que active el proceso de **respuesta a incidentes** cuando se sobrepase. * Considere la realización de recuentos físicos de los materiales de inventario como parte del proceso mensual de seguimiento. |
| PS-14.2 | Almacene **medios** vírgenes o materiales de inventario en un lugar seguro. | * Solicite formas de control de acceso (por ej., armarios con cerradura, cajas fuertes) para evitar el acceso no autorizado. * Restrinja el acceso a **medios** vírgenes/materiales de inventario al personal responsable de la producción únicamente. * Solicite que las personas presenten solicitudes apropiadas de órdenes de trabajo para sacar **medios** vírgenes/materiales de inventario. |
| PS-15.0 | Activos de clientes | Restrinja el acceso a los activos terminados de clientes al personal responsable de darle seguimiento y gestionar los activos únicamente. | * Restrinja el acceso solo al personal de la **bóveda**, quienes pueden posteriormente autorizar a que otras personas saquen activos de los clientes si presentan una solicitud válida de orden de trabajo. * Separe las responsabilidades a fin de que ningún miembro del personal de la **bóveda** manipule datos de producción para procesar. |
| PS-15.1 | Guarde los activos de clientes en un área restringida y segura (por ej., **bóveda**, caja fuerte u otro almacenamiento seguro). | * Implemente una caja fuerte o jaula de alta seguridad adicional dentro de la **bóveda** para títulos muy delicados. * Instale la caja fuerte a la pared o al piso al atornillarla a la estructura de la sala. |
| PS-15.2 | Solicite que dos miembros del **personal de la empresa** con tarjetas de acceso individuales desactiven las áreas muy delicadas (por ej., caja fuerte, jaula de alta seguridad) después de la jornada laboral. |  |
| PS-15.3 | Activos de clientes | Use una caja fuerte a prueba de fuego para almacenar paquetes no enviados que se guarden en el establecimiento durante la noche. | * Instale la caja fuerte en una superficie inmóvil (por ej., una pared, el piso) por razones de seguridad. |
| PS-15.4 | Implemente un área segura especial (por ej., una jaula de seguridad, una sala segura) para almacenar copias de películas que no se hayan entregado; la sala debe tener llave, acceso controlado y debe ser vigilada con cámaras y/o guardias de seguridad. | * Restrinja el acceso al personal que lo requiera dadas sus funciones laborales únicamente. * Asegúrese de que el área de almacenamiento de copias de películas esté en un área interior, totalmente cerrada y sea vigilada en todo momento. * Implemente un proceso para revisar las imágenes de vigilancia en forma constante. |
| PS-16.0 | Eliminación de residuos | Solicite que los materiales con activos de los clientes rechazados, dañados u obsoletos sean borrados, desmagnetizados, picados o destruidos físicamente antes de tirarlos. | * Implemente procesos para realizar inventarios y comparar los materiales, y luego recicle en forma segura o destruya el material rechazado, dañado y obsoleto. * Dañe irreparablemente los medios antes de colocarlos en el contenedor de residuos. * Considere consultar la norma 5220.22-M del Departamento de Defensa de los EE. UU. sobre estándares para picar y borrar material digital (consulte el anexo G). |
| PS-16.1 | Guarde los elementos que se van a reciclar o destruir en un lugar o contenedor seguro para evitar que se copien los contenidos o se vuelvan a usar los activos antes de la eliminación. | * Establezca e implemente políticas que restrinjan la duración (por ej., 30 días) de almacenamiento de materiales rechazados, dañados y obsoletos antes del reciclaje o la destrucción. * Guarde los activos muy delicados en áreas seguras (por ej., **bóvedas**, cajas fuertes) antes del reciclaje o la destrucción. * Asegúrese de que los recipientes de basura se guarden bajo llave. |
| PS-16.2 | Mantenga una bitácora de la eliminación de activos durante al menos 12 meses. | * Integre el registro de eliminación de activos con el proceso de **gestión de activos**. * En las bitácoras de eliminación, incluya un registro final de eliminación para activos eliminados en bitácoras de eliminación. |
| PS-16.3 | Eliminación de residuos | Se debe llevar a cabo la destrucción en el establecimiento. Dos miembros del personal de la empresa deben supervisar y confirmar la destrucción en el establecimiento. Si se involucra una compañía externa en la destrucción, dos miembros del personal de la empresa deben supervisar y confirmar la destrucción y se deben retener los certificados de destrucción. | * Considere solicitar la siguiente información en el certificado de destrucción: * Fecha de destrucción * Descripción de los activos destruidos o eliminados * Método de destrucción * Nombre de la persona responsable de la destrucción de los activos |
| PS-16.4 | Use la automatización para transferir discos rechazados desde las máquinas de duplicados directamente hasta los contenedores de residuos (sin manipulación por parte de operadores de maquinarias). | * Use separación de responsabilidades (por ej., el personal que fabrica el disco grabado no es el mismo que destruye el disco) cuando la eliminación automática no es una opción. * Mantenga una bitácora con firmas de la fecha y la hora de la eliminación del disco. |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| PS-17.0 | Envío | Solicite que los establecimientos generen una orden de trabajo o envío válida para autorizar los envíos de activos de clientes fuera de estos. | * Incluya la siguiente información en la orden de trabajo o envío: * Número de orden de trabajo o envío * Nombre y empresa de la persona que recogerá los contenidos * Fecha y hora de la recolección * Contacto en los establecimientos * Elabore un formulario para registrar activos salientes que son transportados por métodos inusuales. |
| PS-17.1 | Realice un seguimiento y registre los detalles de envío de los activos de clientes; como mínimo, incluya lo siguiente:   * Hora de envío * Nombre y firma de quien realiza el envío * Nombre del destinatario * Domicilio del destinatario * Número de seguimiento de la empresa de transporte * Referencia a la orden de trabajo correspondiente | * Solicite una firma de acuse de recibo * Guarde las bitácoras de envío durante 1 año como mínimo |
| PS-17.2 | Asegure los activos de los clientes que esperan ser recogidos. | * Trabe las puertas y ventanas de las áreas de envío y recepción cuando no haya nadie en ellas. * Se deben cerrar con llave los activos hasta que se entreguen al proveedor/transporte. |
| PS-17.3 | Verifique los activos de los clientes que salgan de los establecimientos con una orden de trabajo o de envío válida. | * Solicite una identificación válida de las empresas de transporte y del personal de entrega para autenticar a quienes recojan los envíos según la orden de trabajo correspondiente. * Confirme que el conteo del envío coincida con la documentación de envío. * Informe de inmediato de cualquier discrepancia o daño en los bienes enviados. |
| PS-17.4 | Envío | Prohíba que el personal de transporte y entrega ingrese a las áreas de contenidos/producción de los establecimientos. | * Acompañe al personal de entrega si el acceso a las áreas de contenidos/producción es necesario. |
| PS-17.5 | Registre y mantenga una bitácora diferente para la información sobre los conductores de camiones. | * Mantenga una bitácora de todos los conductores de camiones e incluya los siguientes datos: * Nombre * Etiquetas de la licencia para el tractor y el remolque * Empresa de afiliación * Fecha y hora de la recolección * Contenidos manipulados |
| PS-17.6 | Observe y vigile el empaquetado y sellado de los remolques en el establecimiento antes del envío. | * Solicite al personal de seguridad que esté presente en todo momento mientras se cargan y sellan los remolques. |
| PS-17.7 | Registre, vigile y revise el tiempo de viaje, las rutas y las horas de entrega de los envíos realizados entre establecimientos. | * Establezca un punto de referencia para las horas de entrega entre los puntos de envío comunes y vigile las horas reales para conocer la varianza. * Investigue, informe y envíe las varianzas importantes al personal correspondiente. * Designe zonas de descanso aprobadas. * Considere implementar un sistema de seguimiento GPS en tiempo real para monitorear y alertar en caso de demoras no esperadas. |
| PS-17.8 | Prohíba la transferencia de elementos fílmicos que no sean para fines aprobados para el estudio del cliente. |  |
| PS-17.9 | Envíe las copias para exhibiciones preestreno en segmentos (por ej., carretes pares versus carretes impares). |  |
| PS-18.0 | Recepción | Inspeccione los activos de los clientes entregados al momento de recibirlos y compárelos con los documentos de envío (por ej., boletas de empaque, manifiestos). | * Identifique y registre toda discrepancia (por ej., objetos faltantes, **medios** dañados). * Informe las discrepancias a la gerencia, a los clientes o al remitente de inmediato. |
| PS-18.1 | Recepción | Mantenga una bitácora de recepción que deberá completar el personal designado al recibo de las encomiendas. | * Registre la siguiente información: * Nombre y firma de la empresa de transporte/entrega * Nombre y firma del destinatario * Fecha y hora del recibo * Detalles de los activos recibidos |
| PS-18.2 | Haga de inmediato lo siguiente:   * Etiquete (por ej., con códigos de barra, números de identificación únicos asignados) los activos recibidos. * Ingrese los activos en el sistema de **gestión de activos**. * Cambie los activos al área restringida (por ej., **bóveda**, caja fuerte). | * Guarde los activos recibidos que no se puedan etiquetar y enviar a la bóveda de inmediato en un **área intermedia** segura (por ej., jaulas de alta seguridad). |
| PS-18.3 | Implemente un método seguro para recibir encomiendas durante la noche. | * Asegúrese de que los horarios de las encomiendas esperadas solo sean conocidos por las personas que deben conocerlos. |
| PS-19.0 | Etiquetado | Prohíba el uso de información de títulos, incluso sobrenombres (“alias”) en la parte externa de los paquetes, salvo que el cliente solicite otra cosa. |  |
| PS-20.0 | Embalaje | Envíe todos los activos de clientes en contenedores cerrados/sellados, y use contenedores con cerradura según el valor de los activos o si lo indica el cliente. |  |
| PS-20.1 | Implemente al menos una de las siguientes medidas de control:   * Cinta a prueba de adulteraciones. * Embalajes a prueba de adulteraciones. * Sellos a prueba de adulteraciones (por ejemplo, en forma de hologramas). * Contenedores seguros (por ej., maletines Pelican con cerraduras con combinación). | * Establezca e informe un plan sobre cómo manejar bienes que han sido alterados. * Informe todas las instancias de alteraciones al equipo de respuesta a incidentes (MS-5.0) |
| PS-20.2 | Embalaje | Use empaquetado retráctil en todos los envíos, e inspeccione el embalaje antes del envío final para asegurarse de que esté bien empaquetado. | * Use empaquetado retráctil en los activos individuales (por ej., cajas, paletas) o sobre un eje si se realiza embalaje de bultos. |
| PS-21.0 | Vehículos de transporte | Cierre con llave los automóviles y camiones en todo momento, y no deje paquetes a la vista. | * No deje paquetes desatendidos. |
| PS-21.1 | Incluya las siguientes características de seguridad en los vehículos de transporte (por ej., remolques):   * Separación de la cabina del conductor. * Capacidad de cerrar y sellar las puertas del área de carga. * GPS para envíos de alta seguridad. | * Use vehículos equipados con sistemas de seguimiento GPS para la entrega de contenidos delicados y activos de alto valor. |
| PS-21.2 | Aplique sellos numerados a las puertas de carga para los envíos de títulos muy delicados. | * Solicite a los guardias de seguridad que apliquen, registren y vigilen los sellos. * Considere medidas de seguridad adicionales para paquetes muy delicados (por ej., área de carga cerrada/asegurada, maletines Pelican cerrados con llave). |
| PS-21.3 | Solicite el uso de escoltas de seguridad cuando se entreguen contenidos muy delicados en áreas de alto riesgo. | * Contrate personal de seguridad capaz de proteger contenidos muy delicados contra intercepciones, asaltos y otras situaciones que podrían traducirse en el hurto de contenidos. |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| DS-1.0 | Cortafuegos/WAN  Seguridad del perímetro | Separe las redes externas/WAN de las redes internas al usar cortafuegos de inspección con Listas de control de acceso que prevengan el acceso no autorizado a cualquier red interna y con la capacidad de mantener el tráfico de carga y descarga. | * Configure los **cortafuegos** de las **WAN** con Listas de control de acceso que denieguen el tráfico a redes internas distintas a los hosts de Internet que residen en el **DMZ.** * Configure la **WAN** de modo que impida que la red interna de contenidos/producción tenga acceso directo a redes. * Incluya documentación detallada de WAN que muestre precisamente y describa la cantidad de conexiones que se originan o destinan a todos los dispositivos externos. * Se deben configurar las reglas del cortafuegos para generar bitácoras de todo el tráfico y para todas las modificaciones de configuración. Se deben inspeccionar las bitácoras al menos en forma mensual. * El cortafuegos debe tener una suscripción a un antivirus y actualizaciones de detección de intrusos. Se debe actualizar al menos en forma semanal. * Considere incluir lo siguiente en la configuración del cortafuegos: * Filtros antispoofing. * Bloquee direcciones IP no viables. * Bloquee direcciones internas de puertos externos. * Bloquee solicitudes de eco del Protocolo de mensajes de control de Internet (Internet Control Message Protocol, ICMP) y Protocolo de datagrama del usuario (User Datagram Protocol, UDP) . * Bloquee puertos y servicios sin utilizar. * Bloquee transferencias de zona de servidor de nombres de dominio (Domain Name Server, DNS) no autorizadas. * Aplique filtros de salida para que el tráfico saliente solo pueda provenir de una dirección interna. |

|  |  |  |  |
| --- | --- | --- | --- |
| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| DS-1.1 | Cortafuegos/WAN  Seguridad del perímetro | Implemente un proceso para evaluar cada 6 meses las **Listas de control de acceso (Access Control Lists, ACL)** de los cortafuegos para confirmar que las especificaciones de configuración son adecuadas y que el negocio las requiere. | * Exporte las **ACL** desde los cortafuegos y/o enrutadores. * Revise las **ACL** para confirmar que el acceso a las redes es adecuado. * Solicite que la gerencia apruebe las revisiones y cualquier modificación de regla del cortafuegos. * Actualice las **ACL** según corresponda. |
| DS-1.2 | Rechace los protocolos por defecto y habilite solo los protocolos seguros específicos permitidos para acceder a la WAN y al cortafuegos. | * Restrinja los protocolos de comunicación no cifrados, tales como **Telnet** y **FTP.** * Sustituya los protocolos no cifrados con versiones cifradas. |
| DS-1.3 | Ubique servidores de acceso externo (por ej., servidores web) dentro de la **DMZ**. | * Aísle los servidores de la **DMZ** de modo que solo brinden un tipo de servicio por servidor (por ej., servidor web, etc.). * Implemente **ACL** para restringir el acceso a la red interna desde la **DMZ.** |
| DS-1.4 | Implemente un proceso para parchar los dispositivos de infraestructura de red (por ej., cortafuegos, enrutadores, conmutadores, etc.), red de área de almacenamiento (Storage Area Network, SAN)/almacenamiento anexado a la red (Network Attached Storage, NAS) y servidores. | * Implemente un proceso regular (por ej., mensual) para identificar, evaluar y probar los parches de los dispositivos de infraestructura de red, SAN/NAS y servidores. * Actualice los dispositivos de infraestructura de red, SAN/NAS y servidores para parchar los niveles que tratan vulnerabilidades importantes en la seguridad. * Aborde los parches críticos dentro de las 48 horas. * Considere aplicar un sistema de gestión de parches centralizado. |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| DS-1.5 | Cortafuegos/WAN  Seguridad del perímetro | Refuerce los dispositivos de infraestructura de red, SAN/NAS y servidores según los estándares de configuración de seguridad. Deshabilite el Protocolo de gestión de redes simple (Simple Network Management Protocol, SNMP) cuando no se use o use solamente SNMPv3 o una versión superior y seleccione nombres de comunidad SNMP que sean contraseñas muy seguras. | * Considere los siguientes opciones de reforzamiento: * Deshabilite cuentas de invitado y funciones de compartir. * Instale antivirus/antimalware. * Active cortafuegos de software. * Elimine el software innecesario. * Desinstale/deshabilite los servicios innecesarios. * Solicite que todos los usuarios actúen como usuarios restringidos. * Use una **ACL** que restrinja el acceso al dispositivo para que solo se usen sistemas de gestión autorizados para conectarse con SNMP. * Consulte los siguientes estándares de reforzamiento de seguridad para reforzar los dispositivos de infraestructura de red: * NIST * SANS * NSA |
| DS-1.6 | No permita la gestión remota del cortafuegos desde una interfaz externa. | * En su lugar, use la autenticación con dos factores y una conexión de **Red privada virtual (Virtual Private Network, VPN)** con un AES de 128 bits o más para llevar a cabo funciones de administración remota. * Exija que las personas proporcionen dos de las siguientes opciones para lograr acceso remoto no administrativo: * Información que la persona conoce (por ej., contraseña, nombre de usuario). * Un artículo físico único que la persona tenga (por ej., ficha, **tarjetas de acceso**, teléfono inteligente, certificado). * Una biometría/cualidad física única de la persona (por ej., huella digital, retina). |
| DS-1.7 | Cortafuegos/WAN  Seguridad del perímetro | Realice respaldos de los dispositivos de infraestructura de red/SAN/NAS y servidores en un servidor seguro central en la red interna. | * Configure los dispositivos de infraestructura de red de modo que guarden los respaldos de los archivos de configuración de manera segura (por ej., cifrado) en la red interna. * Asegúrese de que solo los administradores autorizados tengan acceso al lugar de almacenamiento y los respaldos cifrados. * Asegúrese de que las restricciones estén activadas para mitigar los ataques mediante fuerza bruta y el acceso no autorizado a los archivos de configuración si se usa el Protocolo Trivial de Transferencia de Archivos (Trivial File Transfer Protocol, TFTP) para los respaldos. |
| DS-1.8 | Realice escaneos de vulnerabilidad trimestrales de todos los hosts y rangos de IP externos como mínimo y solucione los problemas. | * Remedie los problemas críticos que brindan acceso no autorizado a contenidos en forma oportuna. * Garantice que las herramientas usadas para el escaneo/prueba busquen tecnologías de virtualización, si se usan. * Considere que una agencia independiente lo lleve a cabo. |
| DS-1.9 | Realice un análisis de penetración anual de todos los hosts y rangos de IP externos como mínimo y solucione los problemas. | * Remedie los problemas críticos que brindan acceso no autorizado a contenidos en forma oportuna. * Garantice que las herramientas usadas para el escaneo/prueba busquen tecnologías de virtualización, si se usan. * Considere que una agencia independiente lo lleve a cabo. |
| DS-1.10 | Asegure cualquier conexión punto a punto al usar conexiones privadas dedicadas y al usar codificación. | * Use un estándar de codificación avanzado (AES) de 128 bits o más para la codificación. |
| DS-1.11 | Implemente un protocolo de servicio de tiempo sincronizado (por ej., protocolo de tiempo de red) para garantizar que todos los sistemas tengan una referencia horaria común. | * Garantice que todos los sistemas tengan la hora correcta y consistente. * Garantice que los datos de tiempo estén protegidos. * Garantice que la configuración horaria se reciba de fuentes horarias aceptadas por la industria. |
| DS-1.12 | Cortafuegos/WAN  Seguridad del perímetro | Establezca, documente e implemente requisitos de seguridad básicos para servicios y dispositivos de infraestructura de red de WAN. | * Garantice que los valores predeterminados del sistema que puedan generar vulnerabilidades se modifiquen antes de que entren en funcionamiento. * Considere una vigilancia continua para informar un cumplimiento de la infraestructura con referencias de seguridad. |
| DS-2.0 | Internet | Prohíba la red de producción y todos los sistemas que procesen o almacenen contenido digital al acceder directamente a Internet, incluso correo electrónico. Si una razón comercial requiere acceso a Internet desde la red de producción o desde sistemas que procesan o almacenan contenido digital, solo se permiten métodos aprobados mediante el uso de una sesión de escritorio/aplicación alojada en forma remota. | * Gestione las excepciones con un sistema de entrada a Internet (por ej., Citrix, Terminal Services, VNC, etc.) con las siguientes formas de control: * El sistema es controlado con acuciosidad cuando la navegación por Internet es la única función del servidor. * El acceso a sitios restringidos está prohibido, incluso a sitios de correo electrónico de Internet, de transferencia de archivos entre personas, casilleros digitales y otros sitios maliciosos conocidos. * Restrinja la transferencia de contenidos desde o hacia el sistema. * Parche y actualice frecuentemente el sistema con las definiciones de virus más recientes. * Evalúe frecuentemente la actividad del sistema. * Bloquee el esquema de discos locales, bloquee el almacenamiento masivo de Bus de serie universal (Universal Serial Bus, USB), bloquee el esquema de impresoras, bloquee funciones de copiar y pegar y bloquee la descarga/carga en el sistema de entrada a Internet desde la red de producción. * Implemente **reglas de cortafuegos** para denegar todo tráfico saliente por defecto y permita en forma explícita el tráfico a los sistemas y puertos específicos que requieran transmisión saliente a las redes internas designadas, como servidores de definición de antivirus, servidores de parche, servidores de licencia (solo cuando las licencias locales no están disponibles), etc. |

| N.º | Tema de seguridad | Mejor práctica | | Guía de implementación |
| --- | --- | --- | --- | --- |
| DS-2.1 | Internet | Implemente dispositivos o software de filtrado de correo electrónico que bloqueen lo siguiente desde **redes distintas a las de producción**:   * Posibles mensajes fraudulentos de correo electrónico. * Archivos adjuntos prohibidos (por ej., secuencias de Visual Basic, archivos ejecutables, etc.). * El tamaño máximo de archivos es de 10 MB. * Dominios conocidos que originan malware o virus. | | * Identifique los tipos de contenidos restringidos para archivos adjuntos de correo electrónico y cuerpo de los mensajes. * Implemente una solución de filtración de correo electrónico y configúrela según los tipos de contenidos restringidos. |
| DS-2.2 | Implemente soluciones o dispositivos de filtración de Internet que restrinjan el acceso a sitios web conocidos por permitir la transferencia de archivos entre personas, transmitir virus, tener origen pirata u otros sitios maliciosos. | | * Implemente aplicaciones de filtración de Internet/servidores intermediarios para detectar y prevenir el acceso a sitios web maliciosos. |
| DS-3.0 | LAN/Red interna | Aísle la **red de contenidos/producción** de las **redes distintas a las de producción** (por ej., red de oficina, **DMZ**, Internet, etc.) a través de la separación física o lógica de las redes. | | * Defina las Listas de control de acceso que expresamente permiten el acceso a la **red de contenidos/producción** desde hosts específicos que requieren acceso (por ej., servidores de antivirus, servidores de gestión de parches, servidores de entrega de contenidos, etc.) * Incluya los puertos y servicios expresamente definidos que deban permitir el acceso en las **Listas de control de acceso.** * Divida o separe las redes en base a las áreas de seguridad definidas. * Implemente **reglas de cortafuegos** para denegar todo tráfico saliente por defecto y permita en forma explícita el tráfico a los sistemas y puertos específicos que requieran transmisión saliente a las redes internas designadas, como servidores de definición de antivirus, servidores de parche, servidores de entrega de contenidos, servidores de licencia (solo cuando los servidores de licencias locales no están disponibles), etc. * Implemente **reglas de cortafuegos** para denegar todo tráfico entrante por defecto y permita en forma explícita puertos y sistemas específicos que requiere transmisión entrante de servidores de entrega de contenidos designados. * Consulte la norma DS-2.0 para asesorarse con respecto al acceso a Internet en el entorno de producción. * Asigne **direcciones** de **IP estáticas** a través de la dirección MAC en los **conmutadores.** * Inhabilite el **DHCP** en la **red de contenidos/producción.** * Prohíba que cualquier sistema informático de producción se conecte a más de una red a la vez. * Prohíba que se use o almacene contenido en redes distintas a las de producción. |
| DS-3.1 | Restrinja el acceso a los sistemas de contenidos/producción al personal autorizado. | | * Considere usar candados con cable de Ethernet para asegurarse de que un cable de red no se conecte a un dispositivo alternativo/no autorizado. |
| DS-3.2 | LAN/Red interna | Restrinja el acceso remoto a la **red de contenidos/producción** solo al personal aprobado que requiera acceso para desarrollar sus responsabilidades laborales. | | * Prohíba el acceso remoto a la red de contenidos/producción. * Mantenga un listado del **personal de la empresa** con autorización de acceso a la **red de contenidos/producción.** * Establezca procesos de gestión para revisar la actividad remota del acceso de vigilancia de los sistemas que residen en la **red de contenidos/producción.** * Configure los sistemas de acceso remoto para usar cuentas individuales. * Restrinja el acceso remoto a un solo método con Listas de control de acceso. * En el caso de que se requiera un acceso remoto de emergencia, implemente lo siguiente: * Use la autenticación con dos factores y preferentemente con un certificado. * Bloquee protocolos de transferencia de archivos, incluso FTP, Secure Shell (SSH), Charla interactiva en Internet (Internet Relay Chat, IRC), Gestión de información (Information management, IM). * **La configuración de VPN** no debe permitir el túnel dividido. * Utilice un modelo de host de plataforma/bastión como intermediario para conectarse con la red de producción. |
| DS-3.3 | Use conmutadores o dispositivos de capa 3 para gestionar el tráfico de red e inhabilite todos los puertos sin uso del **conmutador** en la **red de contenidos/producción** para evitar análisis de paquetes por parte de dispositivos no autorizados. | | * Solicite que los administradores de dispositivos usen una autenticación sólida, incluso: * El uso de un protocolo cifrado. * Función hash con sal para la contraseña. * Contraseña separada para comandos de ejecución. * Conéctese a la consola de dispositivos y actualice los archivos de configuración para inhabilitar los puertos sin uso del **conmutador**. * Active el ingreso en conmutadores o dispositivos de capa 3. |
| DS-3.4 | Restrinja el uso de dispositivos no operados por el conmutador, tales como hubs y repetidores, en la **red de contenidos/producción.** | | * Reemplace los hubs y repetidores con **conmutadores** o dispositivos de capa 3. |
| DS-3.5 | LAN/Red interna | Prohíba la arquitectura dual-home (puentes de red físicos) en sistemas informáticos dentro de la **red de contenidos/producción.** | | * En su lugar, use puentes de red lógicos en la capa externa de la red (por ej., **enrutadores**, **cortafuegos**, **conmutadores**, etc.) en lugar de usar varios **NIC** en un sistema informático. |
| DS-3.6 | Implemente un sistema basado en la red de detección de intrusos (Intrusion Detection System, IDS)/prevención de intrusos (Intrusion prevention systems, IPS) en la **red de contenidos/producción**. | | * Configure el sistema basado en la red de detección/prevención de intrusos de modo que dé alertas o evite actividades sospechosas en la red. * Obtenga una suscripción a antivirus/antimalware para **IDS/IPS** * Actualice las definiciones de firmas de ataque/políticas y antivirus/antimalware en **IDS/IPS** al menos en forma semanal. * Registre todas las modificaciones de actividad y configuración para el **IDS/IPS**. * Implemente software de detección de intrusos con base en el host en todas las estaciones de trabajo. |
| DS-3.7 | Deshabilite el Protocolo de gestión de redes simple (SNMP) cuando no se use o use solamente SNMPv3 o una versión superior y seleccione nombres de comunidad SNMP que sean contraseñas muy seguras. | | * Use una **ACL** que restrinja el acceso al dispositivo para que solo se usen sistemas de gestión autorizados para conectarse con SNMP. |
| DS-3.8 | Refuerce los sistemas antes de ubicarlos en **LAN/Red interna**. | | * Consulte DS-1.5 en caso de sugerencias. |
| DS-3.9 | Realice escaneos de vulnerabilidad de red interna y soluciones cualquier problema al menos en forma anual. | | * Garantice que las herramientas usadas para el escaneo busquen tecnologías de virtualización, si se usan. * Incluya lo siguiente: * Redes de producción * Redes distintas a las de producción * Dispositivos/máquinas conectadas * Dispositivos/máquinas no conectadas |
| DS-3.10 | LAN/Red interna | Realice respaldos de la red de área local de SAN/NAS, servidores y estaciones de trabajo en un servidor seguro central en la red interna. | | * Configure los dispositivos de red de área local de modo que guarden los respaldos de los archivos de configuración de manera segura (por ej., cifrado) en la red interna. * Asegúrese de que solo los administradores autorizados tengan acceso al lugar de almacenamiento y los respaldos cifrados. |
| DS-4.0 | Inalámbrica/WLAN | No permita la arquitectura inalámbrica y el uso de dispositivos inalámbricos en la **red de contenidos/producción.** | | * Restrinja las redes inalámbricas de invitados de modo que tengan acceso únicamente a Internet y no a la **red de contenidos/producción.** * Elimine o inhabilite el acceso inalámbrico en las estaciones de trabajo/computadoras portátiles que procesen o almacenen contenidos en la red de contenidos/producción. |
| DS-4.1 | Inalámbrica/WLAN | Configure las redes inalámbricas **distintas a las de producción** (por ej., redes administrativas y de invitados) con las siguientes medidas de control de seguridad:   * Deshabilite la Privacidad Equivalente a Cableado (Wired Equivalent Privacy, WEP)/acceso protegido Wi-Fi (Wi-Fi Protected Access, WPA) * Solamente active una codificación (WPA2) de **AES** de 128 bitso más. * Separe las redes de “invitados” de las demás redes de la empresa. * Cambie las credenciales de ingreso de administrador asignadas por defecto. * Cambie el nombre de red asignada por defecto (**Identificador de Conjunto de Servicio [Service Set Identifier, SSID]**). | * Considere medidas de control para seguridad como las siguientes: * Usar nombres de **SSID** específicos que no sean de compañía. * Habilitar IEEE 802.1X o IEEE 802.11i si la opción está presente. * Usar RADIUS para fines de autenticación si la opción está presente. * Habilite la **filtración de dirección MAC.** * Ponga en lista negra las direcciones MAC inalámbricas de dispositivos y estaciones de trabajo de producción. * Configure el punto/controlador de acceso inalámbrico de modo que transmita solo dentro del rango especificado. * Implemente un marco 802.1X para arquitectura inalámbrica, el cual incluya lo siguiente: * Servicios de acceso remoto a través de llamadas de usuarios (Remote Access Dial In User Service, RADIUS) para la autenticación, autorización y seguimiento. * Servidor de protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol, LDAP), como Active Directory, para gestionar las cuentas de usuarios. * Infraestructura de clave pública para generar y gestionar los certificados de los clientes y servidores. * Implementa las siguientes medidas de control si se debe usar las llaves previamente compartidas: * Configure WPA2 con **codificación** CCMP (**AES de 128 bits**) o más * Configure una frase secreta compleja (consulte la norma DS-8.1 para consultar las recomendaciones sobre complejidad de las frases secretas). * Cambie la frase secreta al menos cada 90 días y cuando el **personal de la empresa** clave finalice la relación laboral. | |
| DS-4.2 | Inalámbrica/WLAN | Implemente un proceso para buscar puntos de acceso inalámbrico invasores y remediar los problemas validados. | | * Implemente un proceso para recorrer y revisar los establecimientos en búsqueda de puntos de acceso inalámbrico sin protección al menos en forma trimestral. * Configure una solución de acceso inalámbrico centralizada (es decir, un controlador inalámbrico) que avise a los administradores cuando se detecten puntos de acceso inalámbrico invasores, cuando sea posible. |
| DS-5.0 | Seguridad del dispositivo I/O | Designe sistemas específicos que se deben usar para el ingreso o salida (input/output, I/O) de contenidos. | | * Implemente **ACL** para posibilitar el tráfico entre la **red de contenidos/producción** y los sistemas empleados para I/O a fin de ubicar **direcciones IP** de fuente o destino específicos. |
| DS-5.1 | Bloquee ingreso o salida (I/O), almacenamiento masivo, almacenamiento externo y dispositivos de almacenamiento móvil (por ej., **USB**, **FireWire**, Thunderbolt, SATA, **SCSI**, etc.) y quemadores de medios ópticos (por ej., DVD, Blu-ray, CD, etc.) en todos los sistemas que gestionan o almacenan contenidos, salvo los sistemas usados para I/O de contenidos. | | * Considere lo siguiente para bloquear los **dispositivos de I/O**: * Cambie la configuración de registros a fin de restringir el acceso con escritura a los **dispositivos de I/O** en los sistemas MS Windows. * Elimine el archivo de almacenamiento masivo para controlar el acceso con escritura en las estaciones de producción en los sistemas Mac. * Deshabilite los **dispositivos de I/O** usando Group Policy en los sistemas que emplean Microsoft Active Directory o Apple Open Directory. * Use software de vigilancia de puertos de I/O para detectar el uso de puertos si no es posible bloquear los dispositivos de salida. |
| DS-6.0 | Seguridad del sistema | Instale software de antivirus y antimalware en todas las estaciones de trabajo, servidores y en cualquier dispositivo que se conecta a sistemas SAN/NAS. | | * Instale una solución empresarial antivirus y antimalware con una consola de gestión centralizada. * Considere la instalación de un punto endpoint protection. |
| DS-6.1 | Actualice todas las definiciones de antivirus y antimalware en forma diaria o más frecuente. | | * Configure la consola de gestión centralizada de antivirus y antimalware para descargar y forzar actualizaciones de definiciones al menos una vez al día. |
| DS-6.2 | Escanee todos los contenidos para detectar virus y malware antes de ingresar a la **red de contenidos/producción.** | | * Escanee los sistemas que no estén conectados a la **red de contenidos/producción.** |
| DS-6.3 | Seguridad del sistema | Busque virus de la siguiente manera:   * Habilite la función normal de escaneo total del sistema para detectar virus y malware en todas las estaciones de trabajo. * Habilite la función de escaneo total del sistema para detectar virus y malware en servidores y sistemas que conectan a SAN/NAS. | | * Configure el software antivirus y antimalware de modo que escanee totalmente el sistema según la estrategia antivirus y antimalware. * Configure el software antivirus y antimalware de modo que se ejecute durante los períodos de inactividad. |
| DS-6.4 | Implemente un proceso para actualizar los sistemas en forma regular (por ej., sistemas de transferencia de archivos, sistemas operativos, bases de datos, aplicaciones, dispositivos de red) con parches/actualizaciones que remedian las vulnerabilidades en la seguridad. | | * Cuando sea posible, implemente una herramienta de gestión de parches centralizada (por ej., WSUS, Shavlik, Altiris) de modo que se apliquen automáticamente los parches en todos los sistemas. * Busque parches ofrecidos por proveedores y otras entidades. * Ponga a prueba los parches antes de aplicarlos. * Implemente un proceso de excepción y medidas de control compensatorias para casos en los cuales exista una razón comercial legítima para no aplicar parches en los sistemas. |
| DS-6.5 | Prohíba que los usuarios sean administrados de sus propias estaciones de trabajo, a menos que se requiera para el software (por ej., ProTools, Clipster y software de edición, como Blu-Print, Scenarist y Toshiba). La documentación del proveedor del software debe establecer explícitamente que se requieren derechos administrativos. | | * Asegúrese de que la cuenta de usuario empleada para ingresar a la estación de trabajo no tenga privilegios de administrador del sistema. |
| DS-6.6 | Use candados con cable en todos los dispositivos informáticos portátiles que se usen para gestionar contenidos (por ej., computadoras portátiles, tabletas, torres) cuando estén desatendidos. | | * Fije el candado con cable a un objeto fijo (por ej., una mesa). |
| DS-6.7 | Seguridad del sistema | Implemente controles de seguridad adicionales para computadoras portátiles y dispositivos informáticos de almacenamiento portátiles o información confidencial relacionada con proyectos de clientes. Codifique todas las computadoras portátiles. Use dispositivos informáticos de almacenamiento portátiles cifrados en hardware. Instale software de eliminación a distancia en todos los dispositivos móviles/computadoras portátiles que se empleen para gestionar contenidos de modo que se pueda eliminar a distancia información de los discos duros y otros dispositivos de almacenamiento. | | * Conecte pantallas de privacidad a las computadoras portátiles si se deben usar en ubicaciones no seguras. * No conecte computadoras portátiles a ninguna ubicación inalámbrica pública. * Apague las computadoras portátiles cuando no se usen y no use los modos de suspensión o hibernación. |
| DS-6.8 | Restrinja los privilegios de instalación de software de la gerencia de TI. | | * Prohíba la instalación y el uso de software no autorizado, incluso software invasor (por ej., software ilegal o malicioso). * Escanee todos los sistemas para un inventario de aplicaciones instaladas al menos en forma trimestral. |
| DS-6.9 | Implemente referencias y estándares de seguridad para configurar sistemas (por ej., computadoras portátiles, estaciones de trabajo, servidores, SAN/NAS) que se instalan internamente. | | * Elabore una arquitectura estándar segura que se deberá emplear en todos los sistemas. |
| DS-6.10 | Se deben desinstalar los servicios y las aplicaciones innecesarios en los servidores para transferencia de contenidos. | | * Revise el listado de servicios instalados (por ej., services. msc) en todos los servidores para transferencia de contenidos y desinstale o inhabilite los que no se necesiten. * Revise el listado de aplicaciones instaladas en todos los servidores para transferencia de contenidos y desinstale las que no se necesiten. * Revise el listado de aplicaciones de inicio para asegurarse de que no se esté ejecutando ninguna aplicación que no sea esencial. |
| DS-6.11 | Conserve un inventario de sistemas y componentes de sistema. | | * Actualice el inventario al menos en forma mensual. |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| DS-6.12 | Seguridad del sistema | Documente la topología de red y actualice el diagrama de forma anual o cuando se realizan modificaciones significativas en la infraestructura. | * Incluya WAN, Zona desmilitarizada (Demilitarized Zone, DMZ), LAN, WLAN (inalámbrica), Red local de área virtual (Virtual Local Area Network, VLAN), cortafuegos y topología de servidor/red. |
| DS-7.0 | Gestión de cuentas | Establezca e implemente un proceso de gestión de cuentas para las cuentas de administradores, usuarios y cuentas de servicios para todos los **sistemas informáticos** y las aplicaciones que gestionan contenidos. | * Documente políticas y procedimientos para la gestión de cuentas que aborden lo siguiente: * Solicitudes de nuevos usuarios * Modificaciones de acceso de los usuarios * Habilitación y deshabilitación de cuentas de usuarios * Cierre de cuentas de usuarios * Caducidad de cuentas * Licencias * No permita que usuarios múltiples compartan alguna cuenta de usuario. * Restrinja el uso de las cuentas de servicio a solo las aplicaciones que las requieran. * Habilite el ingreso en los siguientes sistemas y dispositivos de infraestructura como mínimo: * Componentes de infraestructura (por ej., **cortafuegos**, servidores de autenticación, sistemas operativos de redes, mecanismos de acceso remoto, incluso **VPN**). * Sistemas operativos de producción. * Componentes de la gestión de contenidos (por ej., dispositivos de almacenamiento, servidores de contenidos, herramientas de almacenamiento de contenidos, herramientas de transporte de contenidos). * Sistemas con acceso a Internet. * Implemente un servidor que se haga cargo de las bitácoras en un depósito central (por ej., servidor de gestión syslog/log, la herramienta **Security Information and Event Management [SIEM]**). |
| DS-7.1 | Gestión de cuentas | Mantenga evidencia rastreable de las actividades de la gestión de cuentas (por ej., mensajes de correo electrónico de aprobación, formularios para solicitar cambios). | * Guarde la evidencia de las aprobaciones de la gerencia y las acciones relacionadas de todas las actividades de gestión de cuentas, si es posible. |
| DS-7.2 | Asigne credenciales únicas según las necesidades usando principios de privilegio mínimo. | * Asigne credenciales, según las necesidades, para los siguientes **sistemas informáticos**, como mínimo: * Sistemas de producción * Herramientas de gestión de contenidos * **Herramientas de transferencia** de contenidos * Dispositivos de infraestructura de redes * Sistemas de ingreso y vigilancia * Portal web del cliente * Sistemas de gestión de cuentas (por ej., Active Directory, Open Directory, protocolo ligero de acceso a directorios [Lightweight Directory Access Protocol, LDAP]). * **Permisos remotos de VPN**, los cuales solo se pueden otorgar cuando sea absolutamente necesario. |
| DS-7.3 | Modifique los nombres de las cuentas de administradores y otras cuentas asignadas por defecto y restrinja el uso de estas cuentas a situaciones especiales que requieren dichas credenciales (por ej., actualizaciones de sistemas operativos, instalaciones de parches, actualizaciones de software). | * Consulte la documentación de todo el hardware y software para identificar todas las cuentas asignadas por defecto. * Cambie la contraseña de todas las cuentas asignadas por defecto. * De ser posible, cambie el nombre de usuario de cada cuenta. * Inhabilite las cuentas de administradores cuando no se usen. |
| DS-7.4 | Separe las responsabilidades para asegurarse de que las personas responsables de otorgar acceso a los sistemas informáticos no sean usuarios finales de los sistemas (es decir, el personal no debe tener la facultad de otorgarse acceso). | * Asigne un equipo independiente que otorgue acceso a sistemas informáticos cuando sea posible. * Implemente formas de control compensatorias cuando no se pueda realizar la separación, como por ejemplo: * Vigile la actividad del personal de la empresa y de los empleados de agencias externas. * Retenga y revise las bitácoras de fiscalizaciones. * Implemente una separación física. * Haga cumplir la supervisión de la gestión. |
| DS-7.5 | Gestión de cuentas | Vigile y fiscalice las actividades de las cuentas de administradores y servicios. | * Habilite los controles de vigilancia de sistemas y aplicaciones que respaldan el ingreso al sistema. * Configure los sistemas y las aplicaciones de modo que registren las actividades de los administradores y dejen evidencia, como mínimo, de la siguiente información: * Nombre de usuario * Hora * Actividad * Información adicional (parámetros de actividades) * Vigile las cuentas de servicios para asegurar que se empleen para los fines deseados únicamente (por ej., consultas a las bases de datos, comunicaciones entre aplicaciones). * Implemente un proceso mensual para revisar la actividad de las cuentas de administradores y servicios para identificar conductas poco usuales o sospechosas, e investigue los posibles usos inadecuados. |
| DS-7.6 | Implemente un proceso para revisar el acceso de usuarios en todos los **sistemas informáticos** que gestionan contenidos, y elimine cuentas de usuarios que ya no requieran acceso trimestral. | * Elimine los **derechos de acceso** a los **sistemas informáticos** de usuarios que ya no necesitan acceso debido a cambios en las funciones laborales o por cesación de actividades del **personal de la empresa** y/o **empleados de agencias externas.** * Elimine o inhabilite las cuentas que no hayan sido usadas en más de 90 días. |
| DS-7.7 | Restrinja el acceso de usuarios a contenidos según los tipos de proyectos. | * Elimine los **derechos de acceso** a los **sistemas informáticos** a los usuarios que ya no necesiten tener acceso debido a la finalización de proyectos. |
| DS-7.8 | Gestión de cuentas | Inhabilite o elimine las cuentas locales en los sistemas que gestionan contenidos cuando sea técnicamente posible. | * Implemente un servidor centralizado de gestión de cuentas (es decir, un servidor de directorios como LDAP o Active Directory) para autenticar el acceso como usuario a los **sistemas informáticos.** * Para los dispositivos de infraestructura de red, implemente el protocolo de Autenticación, Autorización y Contabilización (Authentication, Authorization, and Accounting, AAA) para gestionar cuentas. * Deshabilite la cuenta de invitado. * Si se deben usar cuentas locales, si es posible, cambie el nombre de usuario y contraseña para cada cuenta asignada por defecto y deshabilite la capacidad de ingreso en el sistema mediante la red usando cuentas locales. |
| DS-8.0 | Autenticación | Exija el uso de **nombres de usuario** y de contraseñas únicos para acceder a los **sistemas informáticos.** | * Establezca políticas para exigir el uso de **nombres de usuario** y contraseñas únicos para todos los **sistemas informáticos.** * Configure los **sistemas informáticos** de modo que soliciten autenticación con **nombres de usuario únicos** y contraseñas únicas como mínimo. |
| DS-8.1 | Exija una política sobre contraseñas muy seguras para tener acceso a los **sistemas informáticos.** | * Elabore una política sobre contraseñas que incluya lo siguiente: * La longitud mínima de la contraseña debe ser de 8 caracteres. * Al menos debe cumplir con 3 de los siguientes parámetros: mayúsculas, minúsculas, números y caracteres especiales. * La antigüedad máxima de las contraseñas es de 90 días. * Un día de antigüedad mínima de las contraseñas. * Máximo de entre 3 y 5 intentos inválidos de ingreso a los sistemas. * Se deben habilitar manualmente las cuentas de usuario bloqueadas después de intentos de ingreso inválidos y no se deben habilitar automáticamente después de que haya transcurrido una determinada cantidad de tiempo. * Historial de las diez últimas contraseñas. |
| DS-8.2 | Autenticación | Implemente la autenticación con dos factores (por ej., nombre de usuario/contraseña e identificadores “hard token”) para lograr acceso remoto (por ej., **VPN**) a las redes. | * Exija que las personas proporcionen dos de las siguientes opciones para lograr acceso remoto: * Información que la persona conoce (por ej., contraseña, nombre de usuario). * Un artículo físico único que la persona tenga (por ej., ficha, **tarjetas de acceso**, teléfono inteligente, certificado). * Una biometría/cualidad física única de la persona (por ej., huella digital, retina). * Use la autenticación con dos factores y una conexión de **VPN** con un AES de 128 bits o más para llevar a cabo funciones de administración remota. |
| DS-8.3 | Implemente salvapantallas o software de bloqueo de pantallas con contraseñas en los servidores y estaciones de trabajo. | * Configure los servidores y las estaciones de trabajo en forma manual o a través de una política (como las políticas grupales de Active Directory) para activar un salvapantallas con contraseña después de 10 minutos de inactividad. |
| DS-8.4 | Considere implementar mecanismos de autenticación adicionales para proporcionar una estrategia de autenticación de capas para un acceso de WAN y LAN/Red interna. | * Considere agregar uno o más de los siguientes: * Autenticación con múltiples factores. * Sistema de gestión de acceso e identidad. * Inicio de sesión único en sistema. * Estándares de federación de identidad. |
| DS-9.0 | Ingreso y vigilancia | Implemente sistemas de ingreso y de informes en tiempo real para registrar e informar eventos de seguridad; recaba la siguiente información como mínimo:   * Cuándo (hora) * Dónde (fuente) * Quién (nombre de usuario) * Qué (contenido) | * Habilite el ingreso en los siguientes sistemas y dispositivos de infraestructura como mínimo: * Componentes de infraestructura (por ej., **cortafuegos**, servidores de autenticación, sistemas operativos de redes, mecanismos de acceso remoto (por ej., sistemas de **VPN**). * Sistemas operativos de producción. * Componentes de la gestión de contenidos (por ej., dispositivos de almacenamiento, servidores de contenidos, herramientas de almacenamiento de contenidos, herramientas de transporte de contenidos). * Sistemas con acceso a Internet. * Aplicaciones |
| DS-9.1 | Implemente un servidor que se haga cargo de las bitácoras en un depósito central (por ej., servidor de gestión syslog/log, la herramienta **Security Information and Event Management [SIEM]**). |  |
| DS-9.2 | Configure los sistemas de ingreso de modo que envíen notificaciones automáticas cuando se detecten eventos de seguridad para facilitar la respuesta activa a los incidentes. | * Defina los eventos que requieran investigación y habilite los mecanismos de notificación automática al personal correspondiente; considere los siguientes eventos: * Intentos exitosos e infructuosos por conectarse a la **red de contenidos/producción.** * Tamaño inusual de archivo u hora del día del transporte de contenidos. * Intentos reiterados de acceso no autorizado a archivos. * Intentos de escalada de privilegios. * Implemente un servidor para agregar bitácoras en un depósito central (por ej., servidor de gestión syslog/log, la herramienta Security Information and Event Management [**SIEM**]). |
| DS-9.3 | Investigue cualquier actividad inusual informada por los sistemas de registro y notificación. | * Incorpore los procedimientos de **respuesta a incidentes** para gestionar eventos de seguridad detectados. |
| DS-9.4 | Ingreso y vigilancia | Implemente mecanismos de ingreso en todos los sistemas que se emplean para lo siguiente:   * Generación de claves criptográficas. * **Administración de claves criptográficas.** * Gestión de certificados de proveedores. | * Asegúrese de que todas las claves criptográficas generadas y los certificados adjuntados puedan ser rastreados a un usuario único. |
| DS-9.4 | Revise todas las bitácoras en forma semanal y revise las críticas y de alto riesgo en forma diaria. | * Investigue toda actividad inusual que pueda indicar un incidente de seguridad grave. * Identifique los eventos inusuales adicionales de los que no exista notificación y configure los sistemas de registro y notificación para que envíen alertas sobre los mismos. * Correlacione las bitácoras de distintos sistemas para identificar patrones de actividad inusual. * Según los hallazgos de las revisiones de bitácoras, actualice las configuraciones **SIEM** como corresponda. |
| DS-9.5 | Habilite el registro de movimientos internos y externos y de transferencia de contenidos, e incluya la siguiente información como mínimo:   * Nombre de usuario * Hora * Nombre del archivo * **Dirección IP** de origen * **Dirección IP** de destino * Evento (por ej., descarga, inspección) |  |
| DS-9.6 | Ingreso y vigilancia | Guarde las bitácoras como mínimo un año. | * Solicite asesoría legal para determinar los requisitos normativos con respecto a la conservación de las bitácoras. * Guarde las bitácoras de contenidos en un servidor centralizado al que solo puedan acceder usuarios específicos y que esté seguro en una habitación de acceso controlado. |
| DS-9.7 | Limite el acceso a las bitácoras solo al personal correspondiente. | * Mantenga las Listas de control de acceso para asegurarse de que solo el personal responsable de vigilar y revisar las bitácoras tenga permiso de inspeccionarlas. * Separe las responsabilidades para asegurarse de que nadie esté a cargo de vigilar sus propias actividades. * Proteja las bitácoras de la eliminación o modificación no autorizada usando **derechos de acceso** adecuados en las bitácoras de registro. |
| DS-10.0 | Seguridad en telefonía móvil | Desarrolle una política de "Traiga su propio dispositivo" (Bring Your Own Device, BYOD) para los dispositivos móviles que acceden o almacenan contenido. | * Considere implementar protección antivirus/antimalware para dispositivos móviles, incluso: * Actualizar definiciones incluidas. * Escanear en forma diaria. |
| DS-10.1 | Elabore una lista de aplicaciones aprobadas, tiendas de aplicaciones y programas adicionales de aplicaciones/extensiones para dispositivos móviles que acceden o almacenan contenidos. | * Prohíba la instalación de aplicaciones no aprobadas o aprobadas que no se obtuvieron mediante una tienda de aplicaciones preaprobadas. * Considere un sistema de gestión de dispositivos móviles. |
| DS-10.2 | Conserve un inventario de todos los dispositivos móviles que acceden o almacenan contenido. | * Incluya sistema operativo, niveles de parches, aplicaciones instaladas. |
| DS-10.3 | Solicite codificación para el dispositivo completo o para las áreas del dispositivo en donde se manejará o almacenará contenidos. | * Considere un sistema de gestión de dispositivos móviles. |
| DS-10.4 | Evite la evasión de controles de seguridad. | * Evite el uso de evasión, ruteo, etc. |
| DS-10.5 | Seguridad en telefonía móvil | Implemente un sistema para realizar un borrado remoto de un dispositivo móvil ya sea que se haya extraviado/robado/comprometido o sea necesario por otro motivo. | * Recuerde a los empleados que no se deben extraviar los datos que no sean de la compañía en caso de que se realice un borrado remoto de un dispositivo. |
| DS-10.6 | Implemente un bloqueo automático del dispositivo después de que no se use durante 10 minutos. |  |
| DS-10.7 | Administre todos los parches del sistema operativo de dispositivos móviles y actualizaciones de aplicaciones. | * Aplique los últimos parches/actualizaciones relacionados con seguridad disponibles al momento del lanzamiento general del fabricante, transportista o creador del dispositivo. |
| DS-10.8 | Haga cumplir las políticas de contraseñas. | * Consulte DS-8.1. |
| DS-10.9 | Implemente un sistema para realizar una copia de seguridad y restauración de dispositivos móviles. | * Codifique las copias de seguridad y almacénelas en una ubicación segura. |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| DS-11.0 | Técnicas de seguridad | Asegúrese de contar con técnicas de seguridad (por ej., baja calidad, **filigranas** invisibles o visibles) y que se empleen cuando así se instruya. |  |
| DS-11.1 | Codifique contenidos en discos duros o codifique discos duros completos usando un mínimo de **codificación** **AES** de 128 bits o más a través de:   * **Codificación** en archivos: (es decir, codificar los contenidos mismos). * **Codificación** en disco: (es decir, codificar el disco duro). | * Para discos duros externos, considere adquirir discos codificados previamente (por ej., Rocstor Rocsafe, LaCie Rugged Safe). * Codifique todo el contenido en discos duros, incluso: * SAN/NAS * Servidores * Estaciones de trabajo * Computadoras de escritorio * Computadoras portátiles * Dispositivos móviles * Unidades de almacenamiento externas * Implemente una o más de las siguientes medidas: * **Codificación** en archivo, como por ejemplo, DMG codificados o archivos ZIP codificados. * **Codificación** en disco usando software. |
| DS-11.2 | Envíe claves o contraseñas de decodificación usando un protocolo de comunicación fuera de banda (es decir, no en el mismo **medio** de almacenamiento que el contenido mismo). | * Envíe las claves o contraseñas de decodificación usando un método distinto al usado para transmitir contenidos. * Asegúrese de que los nombres de las claves y las contraseñas no tengan relación con el proyecto o los contenidos. |
| DS-11.3 | Técnicas de seguridad | Implemente y documente políticas y procedimientos de administración de claves criptográficas:   * Uso de protocolos de codificación para la protección de contenidos o datos delicados, independientemente de su ubicación (por ej., servidores, bases de datos, estaciones de trabajo, computadoras portátiles, dispositivos móviles, datos en tránsito, correo electrónico). * Aprobación y revocación de dispositivos confiables. * Generación, renovación y revocación de las claves criptográficas de los contenidos. * Distribución interna y externa de las claves criptográficas de los contenidos. * Claves codificadas vinculantes a responsables identificables. * Separar las responsabilidades para separar la administración de claves del uso de claves. * Procedimientos de almacenamiento de claves. * Procedimientos de respaldo de claves. | * Considere la creación de claves codificadas únicas por cliente y activos críticos. * Evite la sustitución no autorizada de claves criptográficas. * Solicite que los custodios de claves criptográficas reconozcan formalmente que comprenden y aceptan sus responsabilidades como custodios de claves. |
| DS-11.4 | Codifique contenidos en reposo y activos, incluso en instancias de servidor virtual, usando una **codificación** mínima de **AES** de 128 bits o más. | * [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 seguridad | Almacene claves secretas y privadas (no claves públicas) usadas para cifrar datos/contenidos de una o más de las siguientes formas en todo momento:   * Cifrado con una clave de codificación de clave que es al menos tan sólida como la clave de codificación de datos y se almacena de forma separada a la clave de codificación de datos. * Dentro de un dispositivo criptográfico seguro (por ejemplo, módulo de seguridad de host [Host Security Module, HSM] o un dispositivo de punto de contacto de seguridad de transacciones de PIN [Pin Transaction Security, PTS]). * Tiene al menos dos componentes de clave o funciones de compartir clave de formato largo, conforme a un método de seguridad aceptado por la industria. |  |
| DS-11.6 | Confirme que los dispositivos de la **Lista de dispositivos confiables (Trusted Devices List, TDL)** son adecuados según la aprobación de los propietarios de los derechos. | * Solicite a los clientes que entreguen una lista de dispositivos confiables para la reproducción de contenidos. * Solo debe crear Mensajes de entrega de claves (Key Delivery Messages, KDM) para los dispositivos incluidos en la **TDL**. |
| DS-11.7 | Confirme la validez de las claves criptográficas de contenidos y asegúrese de que las fechas de caducidad concuerdan con las instrucciones del cliente. | * Solicite a los clientes que entreguen fechas de caducidad para las claves criptográficas de contenidos. * Especifique una fecha de finalización para cuando las claves criptográficas caduquen para restringir el tiempo durante el cual se puede visualizar los contenidos. |
| DS-12.0 | Seguimiento de contenidos | Implemente un sistema de gestión de contenidos digitales para brindar un seguimiento detallado de contenidos digitales. | * Registre todo el contenido digital que sea sacado o devuelto. * Registe la ubicación digital de todo el contenido. * Registre la duración esperada de cada préstamo. * Registre la fecha y hora de cada transacción. |
| DS-12.1 | Seguimiento de contenidos | Retenga las bitácoras de transacción de movimiento de contenido digital por un año. | * Incluya lo siguiente: * Hora y fecha del préstamo o de la devolución. * Nombre y número de identificación único de la persona que sacó un activo * Motivo de la salida * Ubicación del contenido |
| DS-12.2 | Revise las bitácoras del sistema de gestión de contenidos digitales e investigue las anormalidades. |  |
| DS-12.3 | Use sobrenombres (“alias”) de los clientes cuando sea oportuno en sistemas de seguimiento de activos digitales. | * Limite el conocimiento de los sobrenombres de los clientes al personal involucrado en procesar los activos de clientes. |

| N.º | Tema de seguridad | Mejor práctica | Guía de implementación |
| --- | --- | --- | --- |
| DS-13.0 | Sistemas de transferencia | Use solamente sistemas de **transferencia** aprobados por clientes que usen controles de acceso, un mínimo de **AES** de 128 bits o más, una codificación de contenidos en reposo y contenidos activos y use una autenticación sólida para sesiones de transferencia de contenidos. | * Permita solamente que usuarios autorizados tengan acceso al sistema de transferencia de contenidos. * Considere restringir el acceso para proyectos específicos. * Verifique con el cliente que los sistemas de transferencia de contenidos estén aprobados antes de su uso. |
| DS-13.1 | Implemente un proceso de excepción en el cual se deba obtener previamente la autorización de los clientes por escrito para abordar situaciones en las que no se usen **herramientas de transferencia** codificadas. | * Use nombres de usuarios y contraseñas originados al azar que se informen en forma segura para fines de autenticación. * Solo use herramientas de transferencia y aplicaciones aprobadas por los clientes. * Exija que los clientes aprueben las excepciones en las que no se usen **herramientas de transferencia** codificadas. * Documente y guarde las excepciones. |
| DS-14.0 | Metodología de dispositivos de transferencia | Implemente y use sistemas dedicados para las transferencias de contenidos. | * Asegúrese de que las estaciones de edición y los servidores de almacenamiento de contenidos no se usen para transferir contenidos directamente. * Deshabilite la **VPN**/acceso remoto a los sistemas de transferencia o a cualquier sistema usado para almacenar, transferir o manipular contenidos. |
| DS-14.1 | Separe los sistemas de transferencia de contenidos de las redes administrativas y de producción. | * Separe las redes de forma física o lógica. |
| DS-14.2 | Metodología de dispositivos de transferencia | Ubique los sistemas de transferencia de contenidos en una **Zona Desmilitarizada** (**DMZ)**, y no en la **red de contenidos/producción.** | * Refuerce los sistemas de transferencia de contenidos antes de colocarlos en la **DMZ**(consulte DS-1.5 en caso de sugerencias). * Implemente **Listas de control de acceso (ACL)** que restrinjan todos los puertos salvo los que emplea la **herramienta de transferencia** de contenidos. * Implemente **ACL** para restringir el tráfico entre la red interna y la **DMZ** para **direcciones IP** de origen/destino específicas. * Deshabilite el acceso a Internet desde los sistemas usados para transferir contenidos que no sea el acceso necesario para descargar contenidos del cliente o acceder a ubicaciones de transferencia de contenidos aprobados. |
| DS-14.3 | Elimine los contenidos de los dispositivos/sistemas de transferencia de contenidos inmediatamente después de la transmisión o de la recepción exitosa. | * Exija que los clientes acusen recibo de los contenidos. * Implemente un proceso para eliminar contenido de dispositivos y sistemas de transferencia, incluso de papeleras de reciclaje. * Cuando corresponda, elimine el acceso de clientes a las **herramientas de transferencia** inmediatamente después de la finalización de un proyecto. * Confirme que la conexión haya concluido tras la finalización de la sesión. |
| DS-14.4 | Envíe notificaciones automáticas a los coordinadores de producción cuando se transmitan contenidos salientes. | * Configure el sistema de transferencia de contenidos de modo que envíe una notificación automática (por ej., un mensaje de correo electrónico) a los coordinadores de producción cada vez que un usuario envíe contenidos fuera de la red. |
| DS-15.0 | Portal del cliente | Restrinja el acceso a portales web empleados para transferir contenidos, transmisión ininterrumpida de contenidos y distribución de claves a los usuarios autorizados. | * Implemente medidas de control de acceso en los portales web que transfieren contenidos, transmiten contenidos de forma ininterrumpida y distribuyen claves siguiendo una o más de estas recomendaciones: * Solicite las credenciales del usuario. * Integre las claves de la máquina o del usuario para fines de autenticación y autorización. * Administre claves codificadas usando una separación de responsabilidades adecuada (por ej., una persona debe crear las claves y otra persona debe usar las claves para cifrar el contenido). * Restrinja el acceso al portal a redes específicas, **VLAN**, subredes y/o rangos de **direcciones IP**. * Restrinja la capacidad de subir o descargar contenidos, según corresponda, desde el portal del cliente. |
| DS-15.1 | Portal del cliente | Asigne credenciales únicas (por ej., nombre de usuario y contraseña) a los usuarios del portal y distribuya credenciales a los clientes en forma segura. | * No inserte nombres de usuarios ni contraseñas en los enlaces de contenidos. * Considere distribuir las credenciales de usuarios y los enlaces de contenidos en mensajes de correo electrónico por separado. * Considere distribuir credenciales de usuarios por teléfono o mensajes de texto. * Considere distribuir claves codificadas mediante una transferencia fuera de banda. * Elabore una política sobre contraseñas que incluya lo siguiente: * La longitud mínima de la contraseña debe ser de 8 caracteres. * Al menos debe cumplir con 3 de los siguientes parámetros: mayúsculas, minúsculas, números y caracteres especiales. * La antigüedad máxima de las contraseñas es de 90 días. * Un día de antigüedad mínima de las contraseñas. * Máximo de entre 3 y 5 intentos inválidos de ingreso a los sistemas. * Se deben habilitar manualmente las cuentas de usuario bloqueadas por intentos de ingreso inválidos y no se deben habilitar automáticamente después de que haya transcurrido una determinada cantidad de tiempo. * Historial de las diez últimas contraseñas. |
| DS-15.2 | Asegúrese de que los usuarios tengan sus propios **activos digitales** (es decir, el cliente A no debe tener acceso a los contenidos del cliente B). | * Implemente un proceso para revisar los permisos de archivos y directorios al menos en forma trimestral. * Asegúrese de que el acceso esté restringido a solo quienes lo requieran. |
| DS-15.3 | Ubique el portal web en un servidor dedicado en la **DMZ** y restrinja el acceso hacia y desde direcciones **IP** y protocolos. | * Implemente **Listas de control de acceso (ACL)** que restrinjan todos los puertos salvo los que emplea el portal del cliente. * Implemente **ACL** para restringir el tráfico entre la red interna y la **DMZ** para **direcciones IP** de origen/destino específicas. * Refuerce los sistemas antes de colocarlos en la **DMZ**(consulte DS-1.5 en caso de sugerencias). |
| DS-15.4 | Portal del cliente | Prohíba el uso de software/sistemas/servicios de producción de terceros que se aloje en servidores web de Internet, a menos que el cliente lo apruebe antes. | * Considere agregar uno o más de los siguientes: * Autenticación con múltiples factores. * Sistema de gestión de acceso e identidad. * Inicio de sesión único en sistema. * Estándares de federación de identidad. * Use una conexión de **VPN** con un estándar de codificación avanzado (AES) de 128 bits o más. |
| DS-15.5 | Use **HTTPS** y exija el uso de un juego de codificación más poderoso (por ej., TLS v1) para el portal web interno o externo. |  |
| DS-15.6 | No use cookies persistentes o cookies que almacenen credenciales en texto simple. | * Revise el uso de cookies por parte de aplicaciones web existentes y asegúrese de que ninguna de ellas almacene credenciales en texto simple. * Si una aplicación se encuentra almacenando credenciales en cookies de texto simple, tome una de estas medidas: * Vuelva a configurar la aplicación. * Actualice la aplicación. * Solicite un parche de seguridad al creador de la aplicación. |
| DS-15.7 | Cuando corresponda, configure el acceso a contenidos en portales internos o externos de modo que caduque automáticamente en intervalos predeterminados. |  |
| DS-15.8 | Ponga a prueba las vulnerabilidades de aplicaciones web en forma trimestral y busque la solución a los problemas identificados. | * Use pautas de evaluación aceptadas por la industria, como las emitidas por el Proyecto de Seguridad de Aplicaciones Web Abiertas (Open Web Application Security Project, OWASP) para identificar vulnerabilidades comunes en aplicaciones web, como por ejemplo, Cross Site Request (XSS), SQL Injection y Cross Site Request Forgery (CSRF). * Una agencia independiente debe llevar a cabo las pruebas. * Consulte el Anexo G para obtener más información. |
| DS-15.9 | Portal del cliente | Realice un análisis de penetración anual de las aplicaciones web y solucione los problemas identificados. | * Use pautas de evaluación aceptadas por la industria, como las emitidas por el Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP) para identificar vulnerabilidades comunes en aplicaciones web, como por ejemplo, Cross Site Request (XSS), SQL Injection y Cross Site Request Forgery (CSRF). * Una agencia independiente debe llevar a cabo las pruebas. * Consulte el Anexo G para obtener más información. |
| DS-15.10 | Permita solo al personal autorizado solicitar el establecimiento de conexiones con el proveedor de servicios de telecomunicaciones. |  |
| DS-15.11 | Prohíba la transmisión de contenidos con correo electrónico (incluso cuentas web). | * Considere el uso de servidores exclusivos para correo electrónico para cifrar correos electrónicos y archivos adjuntos (por ej., Cisco IronPort, Sophos E-Mail Security Appliance, Symantec PGP Universal Gateway Email). |
| DS-15.12 | Evalúe el acceso al portal web del cliente al menos en forma trimestral. | * Elimine los **derechos de acceso** al portal web del cliente cuando los proyectos hayan finalizado. * Elimine todas las cuentas inactivas. * Considere enviar notificaciones por correo electrónico automáticas a una parte adecuada siempre que se transfieran datos. |

Anexo A: Glosario

Los términos básicos y los acrónimos de este glosario se usan con frecuencia y son remitidos en esta publicación. Estas definiciones han sido tomadas de estándares ISO relevantes (27001/27002), estándares de seguridad (es decir, NIST) y mejores prácticas de la industria. En las pautas sobre mejores prácticas, todos los términos que están incluidos en este glosario figuran resaltados en **negrita.**

| **Término o acrónimo** | **Descripción** |
| --- | --- |
| **Listas de control de acceso (ACL)** | Mecanismo que implementa el control de acceso para un recurso sistémico mostrando un listado de identidades del sistema que tienen autorización para acceder al recurso. |
| **Derechos de acceso** | Permiso para usar o modificar un objeto o sistema. |
| **Estándar de codificación avanzado (Advanced Encryption Standard, AES)** | Es un estándar NIST de codificación con clave simétrica que emplea bloques de 128 bits y cuyas claves tienen una longitud de 128, 192 o 256 bits. |
| **Gestión de activos** | El sistema por el cual los activos son rastreados en el flujo de trabajo, desde la adquisición hasta la eliminación. |
| **Circuito cerrado de televisión (CCTV)** | Cámaras de video que se usan para transmitir una señal a un lugar específico a través de un número limitado de monitores. |
| **Consola de CCTV** | Sistema central de interfaz de vigilancia de CCTV. |
| **Personal de la empresa** | Personas que trabajan directamente en los establecimientos, incluso empleados, trabajadores temporarios y pasantes. |
| **Red de contenidos/producción** | Una red informática que se usa para almacenar, transferir o procesar contenidos multimedia. |
| **Activos digitales** | Cualquier forma de contenidos y/o medios que hayan sido formateados en una fuente binaria que incluye el derecho a usarlos. |
| **Debida diligencia** | La investigación sobre un posible empleado o trabajador de una agencia externa que se realiza antes de la contratación para asegurar un buen estatus. |
| **Protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol, DHCP)** | Protocolo empleado para asignar automáticamente direcciones IP a todos los nodos de la red. |
| **Zona desmilitarizada (Demilitarized Zone, DMZ)** | Subred física o lógica que contiene y presenta los servicios externos de una organización a una red mayor no confiable, normalmente Internet. |
| **Codificación** | La conversión de datos a un formato, llamado texto cifrado, el cual no puede ser fácilmente comprendido por las personas no autorizadas. |
| **Toma de huellas dactilares** | Una técnica en la cual un software identifica, extrae y luego comprime los componentes característicos de un medio, lo cual posibilita que ese medio sea identificable en forma única por parte del formato comprimido resultante. |
| **Cortafuegos** | Puerta que restringe el acceso entre redes de conformidad con la política local de seguridad. |
| **Reglas del cortafuegos** | Conjunto de instrucciones que usa el cortafuegos para determinar cómo se deben enviar paquetes entre el origen y el destino. |
| **FireWire** | Una interfaz de alta velocidad que permite transmitir datos desde dispositivos externos a una computadora. |
| **Protocolo de transferencia de archivos (File Transfer Protocol, FTP)** | Protocolo TCP/IP que especifica la transferencia de archivos en una red sin codificación. |
| **HTTPS** | Un protocolo de comunicaciones para una comunicación segura en una red informática con una aplicación especialmente ancha en Internet. |
| **Tarjeta de identificación** | Tarjeta que se emplea para identificar personas autorizadas a ingresar a un establecimiento (por ej., empleados, proveedores, visitantes). |
| **Detección de intrusos (IDS)/Prevención de intrusos (IPS)** | Un sistema de detección de intrusos (IDS) es un dispositivo o aplicación de software que vigila actividades de red o sistema en busca de actividades maliciosas o violaciones de políticas y genera informes a una estación de administración. Un sistema de prevención de intrusos (IPS) desempeña la misma función y también intenta bloquear la actividad. |
| **Respuesta a incidentes** | La detección, el análisis y la solución de incidentes de seguridad. |
| **Sistemas informáticos** | Cualquier sistema electrónico informático utilizado por el establecimiento para procesar información. Los sistemas informáticos incluyen, entre otros, aplicaciones, dispositivos de red, servidores y estaciones de trabajo. |
| **Dispositivo I/O** | Dispositivos empleados para comunicarse con y/o entre computadoras (por ej., unidades USB y FireWire). |
| **Dirección IP** | Una identificación numérica (dirección lógica) que se asigna a dispositivos que participan en una red informática. |
| **Administración de claves criptográficas** | La creación, distribución, almacenamiento y revocación de claves codificadas que se usan para acceder a contenidos codificados. |
| **Tarjeta de acceso** | Tarjeta plástica que almacena una firma digital empleada para abrir cerraduras electrónicas de control de acceso. |
| **Red de área local (Local Area Network, LAN)** | Red informática que abarca un área física pequeña (por ej., una oficina). |
| **Filtración de dirección MAC** | Metodología de control de acceso por seguridad que se emplea para restringir el acceso a una red informática. |
| **Llaves maestras** | Llaves que ofrecen acceso a todas las puertas (interiores y exteriores) de un lugar. Las llaves que dan acceso a todas las áreas de alta seguridad también son consideradas llaves maestras. |
| **Medios** | Dispositivos físicos o superficies de grabación que incluyen, entre otros, cintas magnéticas, discos ópticos, discos magnéticos, chips de memoria LSI, en los cuales se graba, almacena o imprime información dentro de un sistema informático. |
| **Protocolo de red** | Convención o estándar que controla o posibilita la conexión, comunicación y transferencia de datos entre terminales informáticos. |
| **Tarjeta de interfaz de red (Network Interface Card, NIC)** | Un componente de hardware informático que conecta una computadora a una red informática. |
| **Red distinta a la de producción** | Todas las redes informáticas que no se usan para procesar o transferir contenidos de medios. Las redes distintas a las de producción pueden incluir la red de oficina o administrativa y la red del cliente. |
| **Evaluación de riesgos** | Identificar y establecer prioridades de riesgos con el fin de identificar posibles amenazas a un negocio. |
| **Gestión de riesgos** | La identificación, el análisis y la mitigación de riesgos a través de la evaluación de riesgos y la implementación de formas de control de seguridad. |
| **Enrutador** | Dispositivo cuyo software y hardware tienen como finalidad guiar y hacer circular información. |
| **Security information and event management (SIEM)** | Un término utilizado para servicios y productos de software que combina administración de información de seguridad (security information management, SIM) y administración de eventos de seguridad (security event management, SEM). La tecnología SIEM ofrece un análisis en tiempo real de alertas de seguridad generadas por aplicaciones y hardware de red. |
| **Separación de responsabilidades** | Un principio de seguridad por el cual ninguna persona individual debe tener la capacidad de completar una tarea por sí misma: un principio por el cual nadie debe tener la responsabilidad de más de una función relacionada. |
| **Identificador de Conjunto de Servicio (SSID)** | Un identificador único de una LAN inalámbrica, el cual generalmente es una cadena de caracteres legible para el ser humano comúnmente denominada "nombre de red". |
| **Interfaz de sistema para computadoras pequeñas (Small Computer System Interface, SCSI)** | Estándares para conectar y transferir datos físicamente entre computadoras y dispositivos periféricos. |
| **Área intermedia** | Un área en donde se almacenan los contenidos antes de ser recogidos (por ej., para entrega o ingreso). |
| **IP estático** | Configuración en la cual una computadora usa la misma dirección IP cada vez que se enciende. |
| **Conmutador** | Dispositivo de redes informáticas que conecta varias máquinas dentro de una red y dirige el tráfico hacia destinos específicos. |
| **Telnet** | Protocolo de red empleado en Internet o redes locales de área para acceder a máquinas remotas. |
| **Empleado de agencias externas** | Cualquier persona que trabaje para una empresa externa pero que es contratado por el establecimiento para prestar servicios. Los empleados de agencias externas incluyen a los contratistas, trabajadores independientes y agencias de temporarios. |
| **Mecanismos de seguimiento** | Herramientas, procesos y/o métodos empleados para darle seguimiento a los activos en el proceso de producción, incluido el registro de activos, el seguimiento del movimiento de los activos (por ej., mover un activo desde una bóveda a un estudio de edición), así como el envío y la destrucción de activos. |
| **Herramientas de transferencia** | Herramientas empleadas para la transmisión electrónica de activos digitales en una red, normalmente con codificación aceptable y mecanismos de autenticación. |
| **Protocolo de transferencia** | El procedimiento relacionado con la transmisión de archivos en una red informática o en Internet. |
| **Listado de dispositivos confiables (TDL)** | Un listado de dispositivos digitales específicos que cuentan con aprobación para reproducir contenidos. |
| **Nombre de usuario único** | Identificación de ingreso fácil de distinguir. |
| **Bus de serie universal (Universal Serial Bus, USB)** | Estándar de bus de serie para conectar dispositivos a un computador host. |
| **Gestión de acceso de usuarios** | El proceso de crear, cambiar derechos de acceso y eliminar cuentas de usuarios de un sistema o aplicación. |
| **Bóveda** | Un área dedicada para almacenar medios físicos con contenidos. |
| **Red local de área virtual (Virtual Local Area Network, VLAN)** | Red informática con atributos de una LAN/Red interna pero sin la restricción de tener una ubicación física. |
| **Red privada virtual (Virtual Private Network, VPN)** | Red informática que permite que los usuarios accedan a otra red mayor. |
| **Red de área amplia (Wide Area Network, WAN)** | Red informática que abarca un área amplia (por ej., una empresa). |
| **Uso de filigranas** | El proceso de insertar (posiblemente) en forma irreversible la información en un activo digital. |
| **Trabajo en proceso (Work in Progress, WIP)** | Cualquier bien que no se considere producto terminado. |
| **Flujo de trabajo** | La secuencia de pasos que una empresa realiza en un trabajo. |

Anexo B: Definiciones de títulos y canales de distribución de la MPAA

**Tipos de título**

| **Tipo de título** | **Descripción** |
| --- | --- |
| **Película** | Un tipo de trabajo presentado en cines o directamente en video o Internet y que incluye los siguientes tipos:   |  |  | | --- | --- | | **Tipo de película** | **Descripción** | | Largometraje | Película de formato largo. | | Cortometraje | Una película más breve que el estándar de un largometraje. | | Película distinta a una película en formato largo | Otras obras, como por ejemplo, un documental. | |
| **Programas televisivos de episodios** | Un tipo de obra relacionada con la televisión, Web o dispositivos móviles y que incluye episodios de una temporada o miniserie. Un piloto también es un episodio, como lo son otras secuencias especializadas (como los “webisodios” o los “movisodios”). |
| **Programas televisivos que no tienen episodios** | Un tipo de obra relacionada con la televisión, Web o dispositivos móviles, pero que no tiene episodios (por ej., películas para televisión, eventos deportivos o programas de noticias). |
| **Promociones y publicidad** | Un tipo de obra que incluye:   * + “Promoción”: todo tipo de material promocional relacionado con medios. Esto incluye avances, sinopsis, paquetes electrónicos para la prensa y otros materiales. Las promociones son casos especiales de publicidad. |
| **Publicidad** | Cualquier forma de anuncio, incluso comerciales televisivos, infomerciales, anuncios de servicio público y promociones no incluidas en el concepto de “Promoción”. No incluye avances y sinopsis de películas aunque puedan salir al aire en forma de comerciales de televisión. |
| **Música** | Un tipo de obra que incluye tonos de timbre, videos de música y otros tipos de música. |
| **Otros** | Un tipo de obra que incluye:   |  |  | | --- | --- | | **Tipo** | **Descripción** | | Fragmento | Un activo que consta primordialmente de partes de otra obra u otras obras. | | Suplementarios | Material creado para suplementar otras obras. Por ejemplo, extras relacionados con un DVD. | | Colección | Un grupo de activos que no encaja en otra categoría. Por ejemplo, una colección de películas. | | Franquicia | Una colección o combinación de otros tipos; por ejemplo, una franquicia podría incluir varios programas de televisión o programas de televisión y películas. | |

**Canales de distribución**

| **Canal de distribución** | **Descripción** |
| --- | --- |
| **Cine** | Las películas se presentan exclusivamente en cines. |
| **Formato distinto al cine** | Una película se presenta en forma pública de otra manera que no es la televisión, el video ni el cine. Incluye la exhibición de una película (i) en aviones, trenes, barcos u otros medios de transporte comunes, (ii) en escuelas, universidades y otras instituciones educativas, bibliotecas, agencias gubernamentales, organizaciones comerciales o de servicios y clubes, iglesias y otros grupos de orientación religiosa, museos y sociedades fílmicas (incluso la transmisión por circuito cerrado dentro del área inmediata de origen de tal exhibición) y (iii) en instalaciones militares permanentes o temporales, instituciones de encierro, prisiones, centros de jubilados, plataformas petroleras, campamentos forestales y campamentos de silvicultura y construcción remotos (incluso la transmisión por circuito cerrado dentro del área inmediata de origen de tal exhibición). |
| **Video** | Una película se presenta para el alquiler y venta de bienes empaquetados a nivel mayorista; por ejemplo, en DVD o Blu-Ray. |
| **Televisión abierta** | Una película se presenta al público en ondas de difusión abierta, por lo general, según se describe en los acuerdos de licencia con cadenas de televisión, estaciones de televisión o redes de televisión por cable básico. |
| **Televisión pagada** | Una película se presenta al público en un formato que requiere pago por parte de al menos un participante en la cadena de difusión, como por ejemplo, video a pedido, cable, satélite y pago por consumo. |
| **Internet** | Una película se presenta en cualquiera de los siguientes canales de distribución en línea:   |  |  | | --- | --- | | **Tipo** | **Descripción** | | Venta electrónica directa (Electronic Sell-Through, EST) o Descargar para poseer (Download to Own, DTO) | Copias digitales permanentes que se venden en Internet. | | Alquiler por Internet o Video a pedido (Video-on-Demand, VOD) | Alquiler por Internet para visualización temporal. | | Video a pedido con suscripción (Subscription Video-on-Demand, SVOD) | Visualización por alquiler por Internet con suscripción. | | Video a pedido gratuito por Internet (Online Free Video-on-Demand, FVOD) | Visualización mediante transmisión ininterrumpida gratuita, normalmente con anuncios comerciales. | | Otros | Internet y nuevos medios, como televisión móvil o por protocolo de Internet. | |

Anexo C: ESQUEMA DE ESTABLECIMIENTOS

Los establecimientos deben revisar la leyenda que se menciona a continuación, identificar qué tipos corresponden a los servicios que presta el establecimiento e implementar las medidas de control adecuadas según la evaluación de riesgos.

|  |  |  |  |
| --- | --- | --- | --- |
| **Leyenda** | | | |
| ADS | Audio, doblaje y subtitulado | FL | Laboratorio cinematográfico |
| CA | Publicidad creativa | IFE | IFE y servicios de hospitalidad |
| CDF | Transporte, entrega y flete | PP | Posproducción |
| D | Distribución | R | Duplicación |
| DC | Cine digital | VFX | Efectos visuales |
| DS | Servicios digitales | AS | Seguridad de aplicaciones |
| DVD | Creación de DVD | CS | Seguridad de nube |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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: Esquema de medidas de control y sus referencias

La siguiente tabla ofrece un esquema general de las mejores prácticas según los estándares de las políticas ISO 27001/27002 y NIST 800-53. Estos estándares se pueden consultar para obtener mayor información sobre la implementación de las medidas de control de seguridad proporcionadas.

| **N.º** | **Tema de seguridad** | **Referencia ISO 27002 -2013** | **Referencia NIST 800-53 Rev. 4** |
| --- | --- | --- | --- |
| **MS-1.0** | Concienciación de la seguridad ejecutiva/Omisión | 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** | Gestión de riesgos | 6.1.1 | CA-1, RA-1 |
| **MS-2.1** | 5.1.2 | RA-2 |
| **MS-3.0** | Organización de la seguridad | 6.1.3 | PM-2 |
| **MS-4.0** | Políticas y procedimientos | 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** | Respuesta 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** | Continuidad del negocio y recuperación ante desastres | 17.1.1 | CP |
| **MS-6.1** | 17.1.1 | CP |
| **MS-7.0** | Control de cambio y gestión de la configuración | 14.2.2 | CM |
| **MS-8.0** | Flujo de trabajo | 11.1 |  |
| **MS-8.1** | 11.1 |  |
| **MS-9.0** | Separación de responsabilidades | 6.1.2 | AC-5 |
| **MS-10.0** | Verificación de antecedentes | 7.1.1 | PS-3 |
| **MS-11.0** | Acuerdos de confidencialidad | 7.1.2 | PL-4, PS-6, SA-9 |
| **MS-11.1** | 8.1.4 | PS-4, PS-8 |
| **MS-12.0** | Uso y verificación de agencias externas | 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** | Puntos de entrada y salida | 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 y salida de visitantes | 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** | Identificación | 11.1.2 | PE-3 |
| **PS-4.0** | Seguridad del 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** | Alarmas | 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** | Autorización | 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** | Control de acceso electrónico | 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** | Llaves | 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** | Cámaras |  | 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** | Ingreso y vigilancia | 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** | Inspecciones | 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** | Seguimiento del inventario | 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** | Recuentos de inventario | 8.1.1 | AU-6, CM-8 |
| **PS-13.1** | 6.1.2 | AC-5 |
| **PS-14.0** | Rastreo de medios vírgenes y materiales de inventario | 8.2.2 | MP-4 |
| **PS-14.1** | 8.1.1 | MP-4, PE-2, PE-3 |
| **PS-14.2** |  |  |
| **PS-15.0** | Activos 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** | Eliminación de residuos | 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** | Envío | 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** | Recepción | 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** | Etiquetado | 8.2.2 | MP-3 |
| **PS-20.0** | Embalaje | 8.3.3 | MP-5 |
| **PS-20.1** | 8.3.3 |  |
| **PS-20.2** |  |  |
| **PS-21.0** | Vehículos de transporte |  | MP-5 |
| **PS-21.1** |  |  |
| **PS-21.2** |  |  |
| **PS-21.3** |  |  |
| **DS-1.0** | Red 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/Red 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** | Inalámbrica | 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** | Seguridad del dispositivo I/O | 10.7.1 | SC-7 |
| **DS-5.1** |  | AC-19, MP-2 |
| **DS-6.0** | Seguridad del sistema | 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** | Gestión de cuentas | 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** | Autenticación | 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** | Ingreso y vigilancia | 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** | Seguridad en telefonía móvil | 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 seguridad | 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** | Seguimiento de contenidos |  |  |
| **DS-12.1** |  |  |  |
| **DS-12.2** |  |  |  |
| **DS-12.3** |  |  |  |
| **DS-13.0** | Sistemas de transferencia | 10.1, 13.2 | IA-5, SC-13 |
| **DS-13.1** | 10.1, 13.2 |  |
| **DS-14.0** | Metodología de dispositivos de transferencia | 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 del 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: Preguntas frecuentes

1. **¿Mi establecimiento debe implementar todas las mejores prácticas que se presentan?**

El cumplimiento de las mejores prácticas es totalmente voluntario. Son pautas sugeridas para la planificación, implementación y modificación de procedimientos de seguridad.

1. **Si mi establecimiento ofrece múltiples servicios (por ej., laboratorio de película y posproducción), ¿qué tipo de mejores prácticas suplementarias debo aplicar?**

Los establecimientos siempre deben aplicar las mejores prácticas suplementarias más restrictivas salvo que los procesos laborales estén separados unos de otros, en cuyo caso solo se deben aplicar las mejores prácticas suplementarias al entorno de esos servicios.

1. **¿Mi establecimiento debe aplicar todos los puntos incluidos en la sección “Guía de implementación” de las mejores prácticas?**

No. La información incluida en esa sección de las pautas tiene como objetivo ayudarlo a determinar la mejor forma de estructurar una medida en particular de control de seguridad. Si en su establecimiento la MPAA realiza una evaluación de seguridad de contenidos, nuestra evaluación solo comparará las prácticas de su establecimiento con la respectiva sección sobre mejores prácticas de las pautas en un momento determinado. (Para obtener más información sobre cómo recibir una evaluación de seguridad de contenidos de la MPAA, puede comunicarse con nosotros enviando un correo electrónico a contentsecurity@mpaa.org.

1. **¿Qué sucede si mi sistema actual no permite la implementación de mejores prácticas?**

Comuníquese con el respectivo proveedor de los sistemas para buscar posibles soluciones a fin de permitir que los sistemas sigan las mejores prácticas. Las soluciones pueden incluir parches, actualizaciones de versiones e incluso cambios a sistemas más seguros. También se pueden emplear medidas alternativas de seguridad si las restricciones técnicas evitan la implementación de mejores prácticas; sin embargo, tales medidas por lo general no cubren los riesgos asociados. Se debe presentar documentación formal y la aprobación de sus clientes con respecto a excepciones a la implementación de las pautas de seguridad debido a limitaciones de sistemas.

1. **Al aplicar las mejores prácticas de estas pautas, ¿mi establecimiento igualmente deberá cumplir con los requisitos de seguridad establecidos individualmente por un miembro de la MPAA?**

La implementación de las mejores prácticas es una pauta y no sustituye las disposiciones contractuales específicas de un miembro de la MPAA. Las decisiones sobre el uso de proveedores por parte de un miembro en particular las toma cada miembro únicamente en forma unilateral. La MPAA recomienda el uso de las mejores prácticas como pauta para futuras discusiones de seguridad con sus clientes.

Anexo F: Políticas y procedimientos sugeridos

A continuación se presentan algunas áreas comunes para las cuales se deben crear e implementar políticas de seguridad y procedimientos para proteger contenidos:

1. **Políticas y procedimientos de seguridad física**

* Seguridad en puntos de entrada y salida
* Protocolo de acceso para visitantes
* Identificación y autenticación
* Protocolo de emergencias
* Medidas para el control de acceso al establecimiento
* Vigilancia del establecimiento

1. **Inventario y gestión de activos**

* Seguimiento del inventario
* Protocolos de envío
* Almacenamiento del inventario en el sitio y durante el transporte

1. **Seguridad de la tecnología informática**

* Política sobre el uso de Internet
* Autenticación y autorización
* Política sobre contraseñas
* Protección y antivirus contra códigos dañinos
* Nota: incluya todo (uso aceptable, etc.)

1. **Políticas y procedimientos de Recursos Humanos**

* Inclusión de seguridad en las responsabilidades laborales
* Verificación de personal
* Acuerdos de confidencialidad, derechos de propiedad y de protección de propiedad intelectual
* Términos y condiciones de empleo
* Separación de responsabilidades (SOD)
* Finalización de la relación laboral
* Medidas disciplinarias
* Concienciación sobre la seguridad y programa de capacitación
* Antecedentes y verificación de empleados y temporarios o trabajadores independientes
* Acuerdos de no divulgación (non-disclosure agreements, NDA) de empleados y temporarios o trabajadores independientes.
* Retención de registros

1. **Agencias externas**

* Contratos con agencias externas
* Acuerdos de no divulgación (NDA)

1. **Respuesta a incidentes**

* Identificación y análisis de incidentes
* Notificación escalada de incidentes
* Procesos y procedimientos de respuesta a incidentes
* Procedimientos de revisión a posteriori y lecciones aprendidas

Anexo G: Otros recursos y referencias

International Organization for Standardization (ISO), Standard 27001. *Information technology - Security techniques - Information security management systems – Requirements.* Octubre 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.* Julio de 2007.<http://www.27000.org/iso-27002.htm>

International Organization for Standardization (ISO), Standard 27005. *Information technology - Security technique- Information security risk management*. Junio 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*, febrero 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*, septiembre de 2006. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

National Industrial Security Program - Operating Manual (DoD 5220.22-M), febrero 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,* septiembre 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,* septiembre 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,* noviembre de 2005. <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>

Anexo H: Cómo notificar actividades de piratería a la MPAA

**Notificación por Internet a la MPAA sobre actividades de piratería**

Usted puede notificar a la MPAA directamente sobre actividades de piratería:

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

**Líneas de notificación sobre actividades de piratería de la MPAA y MPA, disponibles las 24 horas**

El siguiente listado incluye la información de contacto de la línea para notificar, disponible las 24 horas, en todos los países donde la MPAA tiene presencia con una oficina de protección de contenidos local:

|  |  |
| --- | --- |
| **Norteamérica y la región de Latinoamérica** | |
| Canadá | (800) 363-9166 |
| Estados Unidos | (800) 371-9884 |
| **Región de Europa, Medio Oriente y África (EMEA)** | |
| Bélgica | +32 2 778 2711 |
| Italia | (800) 864 120 |
| Países Bajos | (909) 747 2837 |
| Ucrania | +38 0 445 013829 |
| Reino Unido | (800) 555 111 |
| **Región Asia Pacífico (APAC)** | |
| Australia | +61 29997 8011 |
| Hong Kong | +65 6253-1033 |
| Malasia | +65 6253-1033 |
| Nueva Zelanda | +65 6253-1033 |
| Filipinas | +65 6253-1033 |
| Singapur | +65 6253-1033 |
| Taiwán | +65 6253-1033 |

En el sitio <http://www.mpaa.org/contact-us/> encontrará un listado completo con la información general de contacto de todas las oficinas regionales y nacionales para la protección de contenidos.

**Recursos en línea de la MPAA**

Se puede consultar más información sobre la MPAA en el sitio web [www.mpaa.org](http://www.mpaa.org)

También podrá obtener más información sobre programas de protección de contenidos en el todo el mundo durante la exhibición en el sitio [www.fightfilmtheft.org](http://www.fightfilmtheft.org).

**Fin del documento**