| Acción formativa | 24/CIFOFSE/702/0187187/049 |
| --- | --- |
| Número y nombre del curso | [IFCT103] Ciberseguridad: prevención, análisis y respuesta a incidentes de seguridad |
| Módulo Formativo que se evalúa | MF1. Ciberseguridad: prevención, análisis y respuesta a incidentes de seguridad |

| Miembros del equipo | Nombre y Apellidos |
| --- | --- |
| 1 | MIRIAN MOLINAS MERELES |
| 2 | FRANCISCO TROVATO |
| 3 | DANIEL VALERO PICART |
| 4 |  |

| **INSTRUCCIONES DE LA ACTIVIDAD** |
| --- |
| * *En esta hoja encontrará la información necesaria para la realización de la actividad.* * *Antes de resolver la práctica lea con atención el enunciado del ejercicio y compruebe que tiene todos los materiales y equipamiento necesario.* * *Para cualquier aclaración consulte al evaluador/ y/o formador/a.* * *La prueba se realizará en grupos que conformarán equipos de investigación de 3 a 4 personas que entregarán un informe final por equipo.* |

**Enunciado**

Por grupos de tres o cuatro personas realizáis el plan director de seguridad simplificado de una organización de vuestra elección. Se recomienda utilizar las herramientas que INCIBE pone a disposición de los usuarios:

* Guía para la elaboración del plan director de seguridad
* Guía de análisis de riesgos
* Guía de inventariado de activos

**Actividad FSE49 - GRUPO 3**

**Elaboración de un Plan Director de Seguridad para el Estudio de Doblaje y Grabación "Voces y Ecos S.L."**

**ÍNDICE**

**Introducción**

La empresa "Voces y Ecos S.L." es un estudio de doblaje y grabación que fue fundado hace diez años. Se especializa en la producción de audio para diversos medios como cine, televisión y publicidad, utilizando equipos de grabación de alta tecnología y software especializado.

El estudio trabaja principalmente con productoras, agencias de publicidad y otros clientes directos interesados en servicios de doblaje y producción de audio. Además de su actividad principal, el estudio también opera una academia para formar nuevos talentos en el campo del doblaje, lo que refuerza su compromiso con el crecimiento del sector.

Las operaciones del estudio incluyen la gestión de datos sensibles como guiones, grabaciones originales y contratos, lo que requiere una interacción continua con clientes y proveedores, incluidos actores de doblaje, técnicos de sonido, y especialistas en derechos de autor, entre otros.

Actualmente, el estudio mantiene un portal web que sirve como punto de contacto e información sobre sus servicios y cursos ofrecidos. Este sitio ha sido desarrollado y es mantenido por un proveedor de servicios informáticos especializado, asegurando su funcionamiento eficiente y seguro.

"Voces y Ecos S.L." utiliza un sistema híbrido de almacenamiento de datos, con ciertos datos almacenados en la nube para facilitar el acceso remoto y la colaboración, mientras que los archivos más sensibles se almacenan localmente en sistemas seguros. Además, cuentan con un ERP adaptado para gestionar sus operaciones específicas de doblaje y producción de audio.

Tanto los clientes como los proveedores confían en que "Voces y Ecos S.L." proteja adecuadamente su información, permitiéndoles llevar a cabo las gestiones necesarias de manera segura y eficiente.

Desde "Voces y Ecos S.L.", se espera que todos los servicios contratados cumplan con las condiciones acordadas, asegurando que las necesidades del estudio sean adecuadamente cubiertas y que las garantías ofrecidas por los proveedores sean suficientes para soportar sus operaciones diarias y posibles imprevistos.

Finalmente, la empresa, al ser pequeña y no disponer a veces de la suficiente capacidad de producción para alcanzar las fechas de entrega, se alía con otros dos estudios de doblaje pequeños y se distribuyen la tarea de grabación ocasionalmente.

**Marco Legal Aplicable**

* **Ley Orgánica de Protección de Datos Personales (LOPDGDD):** Protección de datos personales de clientes y empleados.
* **Reglamento General de Protección de Datos (RGPD):** Protección de datos personales en el ámbito europeo.
* **Ley de Propiedad Intelectual:** Protección de derechos de autor sobre las grabaciones y producciones.
* **Convenio Colectivo Profesionales de Doblaje y Sonorización (Rama Artística).**

**1. Situación Actual del Plan Director de Seguridad**

En la actualidad, "Voces y Ecos S.L." no cuenta con un departamento dedicado exclusivamente a la seguridad ni ha subcontratado a una empresa externa para manejar estas tareas de forma específica. La supervisión de las actividades relacionadas con la seguridad está integrada dentro de las funciones de la gerencia y una persona del departamento administrativo-financiero, quienes reciben asesoramiento de la empresa de TI contratada para el mantenimiento informático. Esta supervisión se realiza de forma informal, reaccionando ante incidentes a medida que ocurren.

No existe un Plan Director de Seguridad (PDS) formalmente definido, ni se ha realizado un análisis de riesgos detallado más allá del cumplimiento de la normativa de protección de datos personales (LOPD), cuya documentación está desactualizada y fue elaborada externamente con el fin de cumplir estrictamente con dicha normativa para evitar sanciones.

Hasta la fecha, los requerimientos de seguridad, políticas y procedimientos de gestión de riesgos no están formalmente documentados. Sin embargo, la dirección del estudio es plenamente consciente de la necesidad de implementar un PDS, reconociendo los potenciales riesgos e impactos que podría enfrentar la empresa, tanto desde un punto de vista económico como reputacional.

La implementación de un Plan Director de Seguridad (PDS) es fundamental para el proceso de mejora continua en seguridad, permitiendo a la empresa establecer un punto de partida claro, evaluar el nivel de seguridad actual y desarrollar acciones para mitigar los riesgos identificados. Conforme a los estándares del Esquema Nacional de Seguridad (ENS), se pretende evaluar y mejorar el grado de implantación de un PDS, marcando así el inicio formal del fortalecimiento de las prácticas de seguridad en 'Voces y Ecos S.L.'.

**1.1 Estructura de la empresa**

"Voces y Ecos S.L." organiza su estructura en torno a roles clave que gestionan tanto las operaciones creativas como administrativas del estudio.

**Departamentos y roles:**

* **Gerencia:**
  + **CEO / Director de doblaje principal y socio fundador:** Supervisa todas las operaciones del estudio, dirige sesiones de doblaje importantes y participa como talento en proyectos selectos. Define la estrategia a largo plazo y las relaciones con los principales clientes y proveedores.
  + **Dueño del estudio de doblaje / Contador y socio fundador:** Responsable de la gestión financiera y contable del estudio. Supervisa la administración financiera, incluyendo presupuestos, reportes financieros y cumplimiento fiscal.
* **Producción de Doblaje:**
  + **Director de doblaje secundario y profesor de doblaje:** Participa en la dirección de proyectos de doblaje y lidera la formación de nuevos talentos en la academia. Actúa también como talento de doblaje.
  + **Director de doblaje secundario:** Dirige sesiones de doblaje y asiste en la planificación y ejecución de proyectos, asegurando el cumplimiento de los estándares de calidad del audio.
  + **Project Manager:** Coordina los proyectos de doblaje desde la planificación hasta la entrega final, asegurando que se respeten los tiempos y presupuestos establecidos.
  + **Guionista:** Desarrolla y adapta los guiones para asegurar que el contenido sea adecuado para el público objetivo y esté en línea con las especificaciones del cliente.
* **Departamento Técnico:**
  + **Técnico de Sonido en jefe:** Supervisa el equipo técnico de sonido, gestiona la configuración y mantenimiento del equipo de grabación y asegura la calidad técnica de todas las producciones.
  + **Técnicos de Sonido (2):** Operan el equipo de grabación durante las sesiones de doblaje, editan y mezclan pistas de audio, y contribuyen a la creación de efectos sonoros especiales según sea necesario.
* **Administración y Finanzas:**
  + Esta área sigue bajo la supervisión del dueño/contador, con soporte de servicios externos para tareas especializadas como auditorías o asesoría legal.
* **Recursos Humanos y Formación:**
  + Administrado por el Director de doblaje secundario/profesor, quien también se encarga de la selección y capacitación de nuevos talentos, además de su rol de instructor en la academia.

**1.2 Objetivo del plan**

En un estudio de doblaje y grabación, el único objetivo principal de cualquier estrategia de seguridad de la información debe ser proteger la integridad, confidencialidad y disponibilidad de los datos y sistemas críticos. Esto se logra mediante la reducción de los riesgos a niveles que la organización considere aceptables, asegurando así la continuidad del negocio y la confianza de los clientes y colaboradores. Aquí detallamos cómo se podría abordar esto en un estudio de doblaje y grabación:

1. **Proteger la Integridad de los Datos:** Asegurar que la información, como grabaciones originales, guiones, y datos contractuales, no sea alterada inapropiadamente, ya sea por accidente o de forma malintencionada.
2. **Mantener la confidencialidad:** Garantizar que la información sensible sólo sea accesible para aquellos que tienen autorización para accederla, como parte de su rol en el estudio. Esto es crucial no solo para cumplir con las leyes de privacidad y protección de datos, sino también para proteger la propiedad intelectual de los clientes.
3. **Asegurar la Disponibilidad:** Garantizar que los sistemas de información y los datos estén disponibles cuando sean necesarios para las operaciones del estudio, minimizando el tiempo de inactividad y asegurando que los procesos de negocio puedan continuar sin interrupciones significativas.

#### **Procesos Clave**

* **Producción y Postproducción de Audio**: Este proceso incluye la grabación, edición y mezcla de audio. Es fundamental porque manipula directamente los datos sensibles del cliente, como grabaciones originales y guiones adaptados.
* **Gestión de Datos y Archivos**: El manejo y almacenamiento de datos relacionados con proyectos, incluyendo contratos, datos personales de actores y guiones, son esenciales para la operación y requieren protección rigurosa.

#### **Departamentos Clave**

* **Departamento de Producción de Doblaje**: Este departamento maneja directamente la producción de contenidos y es donde se genera y accede a la mayoría de los datos sensibles.
* **Departamento Legal y de Recursos Humanos**: Manejan información sensible relacionada con contratos, cumplimiento legal y datos personales de empleados y colaboradores externos.

#### **Sistemas Clave**

* **Sistemas de Almacenamiento de Datos**: Tanto locales como en la nube, donde se almacenan grabaciones y documentos importantes.
* **Sistemas de Comunicación y Colaboración**: Incluyendo correo electrónico y plataformas de gestión de proyectos que facilitan la coordinación dentro y fuera del estudio.

**1.3 Aspectos técnicos**

Los aspectos técnicos del estudio "Voces y Ecos S.L." describen los elementos de TI (Tecnologías de la información) que respaldan las operaciones del estudio. El estudio posee una sede central donde se encuentran todos los departamentos técnicos y creativos.

**1.4 Estructura técnica:**

* **Conectividad:** El estudio mantiene una conexión a internet de alta velocidad a través de fibra óptica proporcionada por la empresa VodaTel (nombre ficticio). Esta conexión es esencial para el manejo de datos grandes y el trabajo colaborativo en tiempo real.
* **Software especializado:** Dependiendo del departamento, se utilizan diversos softwares especializados. El departamento técnico utiliza software avanzado de edición y mezcla de sonido como Pro Tools, mientras que el departamento de guionistas utiliza software de procesamiento de texto y software de guionización como Guionando.
* **Software común:** Todas las estaciones de trabajo tienen acceso a software ofimático básico, proporcionado como servicio en la nube (SaaS), lo que permite el acceso desde cualquier dispositivo con conexión a internet.
* **Equipamiento de TI:**
  + **Servidor:** Un servidor en nube administrado por CloudFlare
  + **Workstations:** Estaciones de trabajo de alta capacidad, de marca Apple. Año 2020, configuración estándar. (iMac 2020)
  + **Portátiles:** Para uso flexible dentro y fuera del estudio, especialmente útiles durante sesiones externas o viajes.
* **Infraestructura de red:** La sede cuenta con una red LAN robusta y Wi-Fi que cubre todas las áreas, facilitando el acceso y la colaboración entre los diferentes departamentos.
* **Seguridad y copias de seguridad:** No se implementan copias de seguridad de manera rigurosa. Existen discos duros extraíbles de backup, no hechos a tiempos o intervalos oficiales.
* **Herramientas de colaboración y comunicación:** Se utilizan servicios de correo electrónico externo con dominios propios del estudio, y dispositivos móviles para mantener al equipo conectado y operativo en cualquier lugar.
* **Portal web:** El estudio mantiene un portal web que no solo sirve para promocionar sus servicios y cursos, sino también como punto de contacto para clientes potenciales. Este sitio es desarrollado y mantenido por un proveedor especializado para asegurar la mejor experiencia de usuario y seguridad.

Con los aspectos técnicos de "Voces y Ecos S.L.", podemos desarrollar un análisis técnico de seguridad más concreto que evalúe los controles de seguridad en torno a la infraestructura de TI y software especializado, identificando posibles vulnerabilidades y recomendando mejoras.

### Tabla de Mejoras en los Controles de Seguridad para 'Voces y Ecos S.L.'

### 

| **Aspecto Tecnológico** | **Control de Seguridad Actual** | **Vulnerabilidades Identificadas** | **Recomendaciones de Mejora** |
| --- | --- | --- | --- |
| **Conectividad** | **Conexión de fibra óptica de alta velocidad** | **Dependencia de un solo proveedor** | **Añadir una conexión secundaria; implementar VPN y firewalls avanzados.** |
| **Software Especializado** | **Uso de Pro Tools, Adobe Audition, Final Draft** | **Software posiblemente no actualizado** | **Establecer políticas de actualización y gestión de parches automáticos.** |
| **Software Común** | **Aplicaciones SaaS para ofimática** | **Riesgo de ataques en la nube y acceso no autorizado** | **Mejorar políticas de seguridad cibernética; implementar MFA.** |
| **Servidores** | **Servidores Dell PowerEdge con redundancia** | **Riesgo de ataques dirigidos y fallo del hardware** | **Mejorar la redundancia del servidor; implementar encriptación de datos.** |
| **Workstations y Desktops** | **Equipos con alta capacidad de procesamiento** | **No hay antivirus; susceptibles a malware y ataques cibernéticos** | **Instalar soluciones robustas de antivirus y antimalware; fortalecer defensas contra intrusiones.** |
| **Portátiles** | **Uso para tareas externas y de viaje** | **Alta exposición a pérdidas y robos** | **Aplicar cifrado de disco completo y sistemas de rastreo de dispositivos.** |
| **Infraestructura de Red** | **Red LAN robusta y Wi-Fi extendido** | **Vulnerabilidades en la seguridad de la red y Wi-Fi** | **Implementar segmentación de red avanzada; usar WPA3 para Wi-Fi; aplicar DPI.** |
| **Seguridad y Copias de Seguridad** | **Políticas gestionadas por terceros** | **Dependencia y potencial falta de control sobre datos sensibles** | **Auditar regularmente a proveedores; implementar estrategias de copias de seguridad 3-2-1.** |
| **Herramientas de Comunicación** | **Uso de correo electrónico y dispositivos móviles** | **Susceptibles a phishing y otros ataques de ingeniería social** | **Establecer políticas de seguridad robustas; capacitar a empleados en seguridad.** |
| **Portal Web** | **Mantenido por un proveedor externo** | **Riesgos de seguridad web como inyecciones SQL y DDoS** | **Realizar pruebas de penetración regularmente; mantener el portal actualizado y seguro.** |

### 

La implementación de estas mejoras debe ser planificada y gestionada de manera que priorice las áreas de mayor riesgo y vulnerabilidad, asegurando que los recursos se utilicen de manera eficiente para maximizar la protección. Además, es crucial realizar revisiones periódicas y pruebas de los controles para adaptarse a las nuevas amenazas y cambios tecnológicos.

La ausencia de un antivirus como un riesgo significativo, lo que convierte la implementación de una solución antivirus en una prioridad urgente para proteger contra malware y ataques cibernéticos.

Estas recomendaciones y mejoras ayudarán a 'Voces y Ecos S.L.' a fortalecer su infraestructura de seguridad y asegurar el cumplimiento con normativas legales relevantes, como el ENS y GDPR, manteniendo su competitividad y reputación en el mercado.

**2. Catálogo General de Activos**

En 'Voces y Ecos S.L.', los activos incluyen equipos técnicos como micrófonos, computadoras, software de edición, así como archivos digitales de proyectos y datos de clientes. La interrupción en la disponibilidad o el deterioro de cualquiera de estos activos podría significar un retraso en las entregas de proyectos, pérdida de datos de clientes o fallos en la producción, afectando directamente la operatividad y reputación de la empresa.

Las amenazas a estos activos podrían ser ataques cibernéticos que busquen acceder o corromper información, errores humanos que resulten en la pérdida de datos, o desastres físicos como incendios o inundaciones que dañen el equipo físico. La ampliación del concepto de amenaza a "suceso" enfatiza la necesidad de considerar cualquier circunstancia desfavorable que pueda ocurrir.

Las vulnerabilidades en 'Voces y Ecos S.L.' podrían incluir sistemas de seguridad de TI desactualizados, falta de formación en seguridad para los empleados, o infraestructura física inadecuada para proteger los equipos en caso de desastres naturales.

El impacto de la materialización de una amenaza puede variar. Por ejemplo, un ataque cibernético exitoso podría resultar en la pérdida total de datos críticos del cliente (100% de degradación), mientras que un error humano que cause la pérdida de un archivo de proyecto podría ser parcialmente mitigado mediante recuperación de backups, representando un impacto menor.

La probabilidad de cada suceso puede estimarse basándose en la experiencia previa, como la frecuencia de ataques cibernéticos sufridos en el pasado, o mediante consultas con expertos en seguridad de TI que puedan evaluar la efectividad de las medidas de seguridad actuales de la empresa.

En esta sección, se desarrolla la lista de elementos a proteger en el sistema de información de "Voces y Ecos S.L." Estos elementos son fundamentales para la organización, y su pérdida o deterioro podría causar un perjuicio significativo. Por tanto, es esencial aplicarles medidas de seguridad adecuadas.

Utilizando el ENS y la información de la empresa 'Voces y Ecos S.L.', podemos elaborar un análisis detallado y proporcionar recomendaciones para mejorar las medidas de seguridad de la información y avanzar en la implementación del PDS.

**Ver planilla “DeclaracionDeAplicabilidad.xlsx”**

[**https://docs.google.com/spreadsheets/d/1ZqE7kXHv0\_AsfJVjBw-kec-Rkf8b5QGG/edit?gid=1199151556#gid=1199151556**](https://docs.google.com/spreadsheets/d/1ZqE7kXHv0_AsfJVjBw-kec-Rkf8b5QGG/edit?gid=1199151556#gid=1199151556)

| **Medidas de Seguridad** |  | **Por categoría o dimensión(es)** | **Nivel de las dimensiones de seguridad** |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **BAJO** |  |  |  |
|  |  |  | **Categoría de seguridad del sistema** |  |  |  |
|  |  |  | **BÁSICA** |  |  |  |
| **org** | **Marco organizativo** |  |  | ¿Controles aplicados satisfactorios? | Controles a aplicar | Soluciones sugeridas |
| org.1 | Política de seguridad | Categoría | aplica | No | - | La empresa debe desarrollar una política de seguridad, aprobada por el responsable de seguridad, que detalle los objetivos de la organización, que mencione el marco legal y regulatorio aplicable, que claramente separe los roles y sus responsabilidades, y que definan un comité de seguridad con su acta de conformación. Debe además existir una guía para la estructuración de la documentación de seguridad y su gestión. |
| org.2 | Normativa de seguridad | Categoría | aplica | Sí | - | La empresa debe desarrollar documentación que describa el uso correcto de equipos, servicios e instalaciones, marcando lo que se considere uso indebido, y las responsabilidades del personal con respecto a esto. |
| org.3 | Procedimientos de seguridad | Categoría | aplica | No | - | La empresa deberá redactar documentos que detalles cómo operar los elementos del sistema de información, y quiénes serán los responsables de hacerlo. |
| org.4 | Proceso de autorización | Categoría | aplica | No | - | La empresa contiene controles de seguridad para ciertas partes, pero no para todas. Se debe aplicar un proceso global de autorizaciones a todos los elementos del sistema. |
| **op** | **Marco operacional** |  |  |  |  |  |
| op.pl | Planificación |  |  | No |  |  |
| op.pl.1 | Análisis de riesgos | Categoría | aplica | No |  | La empresa no ha realizado un análisis de riesgos en ninguna medida. Deberá realizar al menos un análisis de riesgos informal en el que detallen sus activos más valiosos (los guioones de doblaje y los vídeos, en este caso) y sus riesgos más probables. |
| op.pl.2 | Arquitectura de Seguridad | Categoría | aplica | No |  | La empresa no dispone de conocimiento de su arquitectura de seguridad, y aplicau na política BYOD (trae tu propio dispositivo) para mucha de ela, lo que genera una mayor dificultad a la hora de conocer todos los puntos de la red. Se debe realizar un mapeo para conocer la arquitectura de seguridad, y se recomienda deshacerse de la política BYOD. |
| op.pl.3 | Adquisición de nuevos componentes | Categoría | aplica | Sí |  | Se dispone de un proceso formal de adquisición de nuevos componentes, pero se debe hacer más énfasis en el análisis de riesgos antes de poner estos componentes en marcha. |
| op.pl.4 | Dimensionamiento/gestión de la capacidad | D | aplica | Sí |  | Se han considerado las necesidades de la empresa y se han preparado los equipos y software de manera acorde. |
| op.pl.5 | Componentes certificados | Categoría | n.a. | Sí |  |  |
| op.acc | Control de acceso |  |  |  |  |  |
| op.acc.1 | Identificación | T A | aplica | No |  | Las cuentas de usuario no están asignadas a un identificador único a través de todos los programas y plataformas, y no existe trazabilidad de las acciones. Se recomienda implementar un sistema de gestión de usuarios único al iniciar sesión, o cambiar las aplicaciones por aquellas que permitan un control más granular de permisos, aunque no sea una solución centralizada. |
| op.acc.2 | Requisitos de acceso | C I T A | aplica | No |  | Se conocen los responsables de cada parte del sistema, pero el control de accesos no es global, fallando en algunas aplicaciones, si bien no en todas. Se recomienda cambiar aquellas aplicaciones donde no se pueden ajustar estos controles. |
| op.acc.3 | Segregación de funciones y tareas | C I T A | n.a. | Sí |  |  |
| op.acc.4 | Proceso de gestión de derechos de acceso | C I T A | aplica | No |  | Los derechos de acceso están presentes, pero no se respeta la política de mínimo privilegio por falta de capacidades de configuración de algunas de las plataformas utilizadas. El problema surge de compartir cuentas. Se recomienda utilizar una cuenta para cada usuario con acceso. |
| op.acc.5 | Mecanismo de autenticación (usuarios externos) | C I T A | + [R1 o R2 o R3 o R4] | Sí |  | Solo contraseña. |
| op.acc.6 | Mecanismo de autenticación (usuarios de la organización) | C I T A | + [R1 o R2 o R3 o R4] + R8 + R9 | No |  | Los miembros se registran con contraseñas, pero no existe doble factor (R9) ni controles al acceso remoto (R10). |
| op.exp | Explotación |  |  |  |  |  |
| op.exp.1 | Inventario de activos | Categoría | aplica | No |  | Existe un inventario de activos físicos, pero no activos intangibles. Se debe realizar el inventario de activos intangibles (cada proyecto y programa). |
| op.exp.2 | Configuración de seguridad | Categoría | aplica | No |  | Se quitan las contraseñas por defecto, pero no se respeta la mínima funcionalidad. Se deben retirar los programas que no cumplen con esto. |
| op.exp.3 | Gestión de la configuración de seguridad | Categoría | aplica | No |  | No existe una gestión de seguridad luego de la puesta en marcha inicial. Agregar en la política de seguridad un intervalo regular donde se revisará la seguridad. |
| op.exp.4 | Mantenimiento y actualizaciones de seguridad | Categoría | aplica | No |  | Implementar un procedimiento para actualizar y mantener todos los equipos, no solamente al recibir notificaciones de actualización del desarrollador. |
| op.exp.5 | Gestión de cambios | Categoría | n.a. | - |  |  |
| op.exp.6 | Protección frente a código dañino | Categoría | aplica | Sí |  | Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo a las recomendaciones del fabricante. |
| op.exp.7 | Gestión de incidentes | Categoría | aplica | No |  | Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación. |
| op.exp.8 | Registro de la actividad | T | aplica | No |  | Se generará un registro de auditoría, que incluirá, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma. |
| op.exp.9 | Registro de la gestión de incidentes | Categoría | aplica | Sí |  | Se registrarán los reportes iniciales, intermedios y finales de los incidentes, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente, también se registrará aquella evidencia que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado. |
| op.exp.10 | Protección de claves criptográficas | Categoría | aplica | No |  | Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final. |
| op.ext | Recursos externos |  |  |  |  |  |
| op.ext.1 | Contratación y acuerdos de nivel de servicio | Categoría | n.a. | - |  |  |
| op.ext.2 | Gestión diaria | Categoría | n.a. | - |  |  |
| op.ext.3 | Protección de la cadena de suministro | Categoría | n.a. | - |  |  |
| op.ext.4 | Interconexión de sistemas | Categoría | n.a. | - |  |  |
| op.nub | Servicios en la nube |  |  |  |  |  |
| op.nub.1 | Protección de servicios en la nube | Categoría | aplica | No |  | Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (Software as a Service, SaaS), Plataforma como Servicio (Platform as a Service, PaaS) e Infraestructura como Servicio (Infrastructure as a Service, IaaS) definidas en las guías CCN-STIC que sean de aplicación. Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a: |
| op.cont | Continuidad del servicio |  |  |  |  |  |
| op.cont.1 | Análisis de impacto | D | n.a. | - |  |  |
| op.cont.2 | Plan de continuidad | D | n.a. | - |  |  |
| op.cont.3 | Pruebas periódicas | D | n.a. | - |  |  |
| op.cont.4 | Medios alternativos | D | n.a. | - |  |  |
| op.mon | Monitorización del sistema |  |  |  |  |  |
| op.mon.1 | Detección de intrusión | Categoría | aplica | No |  | Se dispondrá de herramientas de detección o prevención de intrusiones. (PDI y PAS) |
| op.mon.2 | Sistema de métricas | Categoría | aplica | No |  | Atendiendo a la categoría de seguridad del sistema, se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad que resulten aplicables y, en su caso, para proveer el informe anual requerido por el artículo 32. |
| op.mon.3 | Vigilancia | Categoría | aplica | No |  | Se dispondrá de un sistema automático de recolección de eventos de seguridad. |
| mp | Medidas de protección |  |  |  |  |  |
| mp.if | Protección de las instalaciones e infraestructuras |  |  |  |  |  |
| mp.if.1 | Áreas separadas y con control de acceso | Categoría | aplica | No | Separadas sí, sin control de acceso | El equipamiento del Centro de Proceso de Datos (CPD) se instalará, en la medida de lo posible, en áreas separadas, específicas para su función. Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas. |
| mp.if.2 | Identificación de las personas | Categoría | aplica | Sí |  | El procedimiento de control de acceso identificará a las personas que accedan a los locales donde hay equipamiento esencial que forme parte del sistema de información del CPD, registrando las correspondientes entradas y salidas. |
| mp.if.3 | Acondicionamiento de los locales | Categoría | aplica | Sí |  | Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado, y, en especial, para asegurar: Las condiciones de temperatura y humedad, la protección frente a las amenazas y la protección del cableado frente a incidentes fortuitos o deliberados.identificadas en el análisis de riesgos, |
| mp.if.4 | Energía eléctrica | D | aplica | Sí |  | En caso de fallo del suministro principal, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información. |
| mp.if.5 | Protección frente a incendios | D | aplica | Sí |  | Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incendios atendiendo, al menos, a la normativa industrial de aplicación. |
| mp.if.6 | Protección frente a inundaciones | D | n.a. | - |  |  |
| mp.if.7 | Registro de entrada y salida de equipamiento | Categoría | aplica | Sí |  | Se llevará un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento. |
| mp.per | Gestión del personal |  |  |  |  |  |
| mp.per.1 | Caracterización del puesto de trabajo | Categoría | n.a. | - |  |  |
| mp.per.2 | Deberes y obligaciones | Categoría | aplica | No |  | Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, contemplando: 1. Las medidas disciplinarias a que haya lugar. 2. Contemplando tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo. 3. El deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación. En caso de personal contratado a través de un tercero: 1. Se establecerán los deberes y obligaciones de cada parte y del personal contratado. 2. Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones. |
| mp.per.3 | Concienciación | Categoría | aplica | No |  | Crear e implementar un programa continuo de concienciación sobre seguridad de la información que incluya sesiones regulares, boletines informativos y comunicados sobre las últimas amenazas y vulnerabilidades. Esto debería formar parte de la inducción de nuevos empleados y un requisito anual para todos los empleados. |
| mp.per.4 | Formación | Categoría | aplica | No |  | Implementar sesiones de capacitación que sean específicas para los diferentes roles dentro de la empresa, asegurando que cada empleado entienda los riesgos y controles de seguridad pertinentes a su trabajo específico. Asegurar que las capacitaciones se actualicen regularmente para reflejar nuevas amenazas, tecnologías y prácticas de seguridad. Planificar sesiones de refresco anuales para mantener a todos al día. Fomentar y facilitar que el personal clave en seguridad obtenga certificaciones reconocidas en la industria, como CISSP, CISM, o cursos específicos relacionados con la seguridad en entornos de producción y post-producción. |
| mp.eq | Protección de los equipos |  |  |  |  |  |
| mp.eq.1 | Puesto de trabajo despejado | Categoría | aplica | Sí |  | Establecer y hacer cumplir políticas que requieran a los empleados mantener sus áreas de trabajo despejadas de documentos confidenciales y dispositivos sensibles cuando no estén en uso. Esto reduce la posibilidad de que información sensible sea vista accidentalmente por personal no autorizado o visitantes.  Formación y Concienciación: Educar a los empleados sobre la importancia de mantener un espacio de trabajo organizado y seguro para proteger la información y los activos de la empresa. |
| mp.eq.2 | Bloqueo de puesto de trabajo | A | n.a. | Sí |  | Implementar políticas de seguridad que requieran bloqueo automático de las estaciones de trabajo después de un período de inactividad. Esto asegura que los equipos no queden desprotegidos si el empleado se aleja sin bloquear su estación manualmente. Promover el uso de métodos de autenticación robustos como contraseñas complejas, autenticación de dos factores, o reconocimiento biométrico para acceder a las estaciones de trabajo. |
| mp.eq.3 | Protección de dispositivos portátiles | Categoría | aplica | Sí |  | Asegurar que todos los dispositivos portátiles como laptops, tablets y discos duros externos estén cifrados para proteger la información almacenada en caso de pérdida o robo (Cifrado de Datos:). Control de Acceso y Gestión de Dispositivos; utilizar soluciones de gestión de dispositivos móviles para controlar el acceso a los dispositivos, aplicar políticas de seguridad, y realizar borrado remoto en caso necesario. |
| mp.eq.4 | Otros dispositivos conectados a la red | C | aplica | No |  | Implementar segmentación de red para controlar el acceso a diferentes partes de la red. Usar firewalls para bloquear tráfico no autorizado hacia o desde estos dispositivos. Mantener todos los dispositivos conectados a la red actualizados con los últimos parches de seguridad para proteger contra vulnerabilidades conocidas. Y, mantener un inventario actualizado de todos los dispositivos conectados y realizar revisiones de seguridad regulares para asegurar que solo los dispositivos autorizados estén conectados y configurados adecuadamente. |
| mp.com | Protección de las comunicaciones |  |  |  |  |  |
| mp.com.1 | Perímetro seguro | Categoría | aplica | No |  | Implementar firewalls que ofrezcan inspección profunda de paquetes y capacidades avanzadas de prevención de intrusiones para proteger contra ataques externos. Utilizar redes privadas virtuales (VPN) para asegurar las conexiones remotas al entorno de la red corporativa. |
| mp.com.2 | Protección de la confidencialidad | C | aplica | No |  | Asegurar que toda la información que se transmita esté encriptada utilizando protocolos seguros. Controlar el acceso a la información mediante políticas de seguridad que determinen quién puede acceder a qué datos y en qué circunstancias. |
| mp.com.3 | Protección de la integridad y de la autenticidad | I A | aplica | Sí |  | Utilizar firmas digitales y mecanismos de sellado de tiempo para asegurar la integridad y la autenticidad de los documentos y las comunicaciones. Implementar sistemas de autenticación de múltiples factores para verificar la identidad de los usuarios y asegurar que solo las partes autorizadas puedan acceder a la información. |
| mp.com.4 | Separación de flujos de información en la red | Categoría | n.a. | No |  | Esta medida es crucial para prevenir interferencias o fugas de información entre distintas áreas de la red que podrían tener diferentes niveles de sensibilidad o seguridad. Definir políticas claras que regulen cómo deben separarse y tratarse los flujos de información, basándose en los niveles de seguridad requeridos y los roles de acceso. Establecer sistemas de monitorización para controlar continuamente los flujos de datos en la red y asegurar que se mantienen las políticas de separación. |
| mp.si | Protección de los soportes de información |  |  |  |  |  |
| mp.si.1 | Marcado de soportes | C | n.a. | No |  | Implementar un sistema de etiquetado claro y efectivo para todos los soportes de datos, como discos duros externos, USBs y otros medios removibles. Esto debería incluir información sobre la sensibilidad de los datos y las restricciones de acceso. |
| mp.si.2 | Criptografía | C I | n.a. | No |  | Utilizar cifrado fuerte para proteger la información almacenada en dispositivos portátiles y en tránsito. Asegurarse de que las claves de cifrado se manejen y almacenen de manera segura. |
| mp.si.3 | Custodia | Categoría | aplica | No |  | Establecer procedimientos estrictos de custodia para todos los soportes de información, asegurando que solo el personal autorizado tenga acceso a ellos y que exista un registro detallado de su uso y ubicación. |
| mp.si.4 | Transporte | Categoría | aplica | No |  | Desarrollar políticas y procedimientos para el transporte seguro de soportes de información, incluyendo el uso de contenedores seguros y la minimización de la transferencia física de datos sensibles. |
| mp.si.5 | Borrado y destrucción | C | aplica | No |  | Implementar métodos de borrado seguro y verificable para dispositivos de almacenamiento que serán descartados o reasignados. Considerar la destrucción física para soportes que contienen datos altamente confidenciales. |
| mp.sw | Protección de las aplicaciones informáticas |  |  |  |  |  |
| mp.sw.1 | Desarrollo de aplicaciones | Categoría | n.a. | - |  | Seguir un proceso de desarrollo de software que incorpore la seguridad desde el diseño, utilizando prácticas como la revisión de código, las pruebas de penetración y la integración continua de medidas de seguridad. |
| mp.sw.2 | Aceptación y puesta en servicio | Categoría | aplica | No |  | Establecer un protocolo de aceptación riguroso que incluya pruebas de seguridad exhaustivas antes de desplegar cualquier aplicación. Asegurar que las aplicaciones cumplan con todos los requisitos de seguridad antes de su implementación oficial. |
| mp.info | Protección de la información |  |  |  |  |  |
| mp.info.1 | Datos personales | Categoría | aplica | No |  | Adoptar y hacer cumplir políticas estrictas de protección de datos personales, alineadas con normativas como el GDPR, para gestionar adecuadamente la recolección, almacenamiento, procesamiento y eliminación de datos personales. Realizar auditorías regulares y establecer controles de acceso robustos para garantizar que solo el personal autorizado tenga acceso a datos personales. |
| mp.info.2 | Calificación de la información | C | n.a. | - |  | Establecer un sistema de clasificación que identifique claramente la sensibilidad y la importancia de la información, permitiendo aplicar medidas de seguridad adecuadas a cada tipo de dato. Capacitación sobre la Importancia de la Clasificación: Educar a todos los empleados sobre la importancia de la clasificación de la información y cómo deben manejar cada tipo de dato según su clasificación. |
| mp.info.3 | Firma electrónica | I A | aplica | Sí |  | Utilizar soluciones de firma electrónica para asegurar la autenticidad e integridad de documentos electrónicos, especialmente en comunicaciones externas y contratos. Asegurarse de que las firmas electrónicas utilizadas cumplan con los estándares legales y de seguridad pertinentes. |
| mp.info.4 | Sellos de tiempo | T | n.a. | - |  | Implementar sellado de tiempo en documentos importantes para proporcionar una prueba verificable de la existencia y el estado de un documento en un momento específico. Integrar la tecnología de sellado de tiempo en los sistemas de gestión documental para mejorar la trazabilidad y la auditoría de documentos. |
| mp.info.5 | Limpieza de documentos | C | aplica | No |  | Establecer políticas claras de retención y destrucción de documentos que definan cuándo y cómo deben eliminarse los documentos según su clasificación y relevancia legal. |
| mp.info.6 | Copias de seguridad | D | aplica | Sí |  | Implementar una estrategia de copias de seguridad que incluya respaldos regulares, almacenamiento en ubicaciones seguras (tanto on-site como off-site) y pruebas periódicas de recuperación de datos. |
| mp.s | Protección de los servicios |  |  |  |  |  |
| mp.s.1 | Protección del correo electrónico | Categoría | aplica | No |  | Implementar soluciones avanzadas de filtrado de correo electrónico que detecten y bloqueen correos no deseados, phishing y malware antes de que lleguen a los buzones de los usuarios. Educar a los empleados sobre los riesgos asociados con el correo electrónico, incluyendo el reconocimiento de intentos de phishing y la importancia de no abrir adjuntos sospechosos. Asegurar que los mensajes de correo electrónico que contienen información sensible sean cifrados durante su envío y recepción para proteger la confidencialidad de la información. |
| mp.s.2 | Protección de servicios y aplicaciones web | Categoría | + [R1 o R2] | No |  | Realizar pruebas regulares de seguridad en las aplicaciones web para identificar y corregir vulnerabilidades antes de que puedan ser explotadas. Asegurar que se implementen controles de acceso robustos, con autenticación de dos factores donde sea posible, para gestionar el acceso a aplicaciones y servicios web. |
| mp.s.3 | Protección de la navegación web | Categoría | aplica | No |  | Promover el uso de redes privadas virtuales (VPN) cuando los empleados accedan a la red corporativa desde ubicaciones externas, asegurando una navegación segura y protegida. Implementar soluciones de filtrado web para bloquear el acceso a sitios web maliciosos o no autorizados y evitar que el malware ingrese a la red. |
| mp.s.4 | Protección frente a denegación de servicio | D | n.a. | - |  | Desarrollar y practicar un plan de respuesta ante incidentes para asegurar una reacción rápida y eficaz en caso de un ataque. Implementar redundancia en los servidores y balanceo de carga para distribuir el tráfico uniformemente y minimizar el impacto de un ataque. Contratar servicios de mitigación que puedan absorber y neutralizar ataques de gran volumen antes de que afecten las operaciones de la empresa. |

**2.1 Inventariado de activos**

| **Identificador** | **Nombre** | **Descripción** | **Responsable** | **Tipo** | **Ubicación** | **Crítico** |
| --- | --- | --- | --- | --- | --- | --- |
| *ID\_0001* | Router Wifi | Router Wi-Fi para las instalaciones | Dpto. Informática. | Router (físico) | Sala de CPD1 | No |
| *ID\_0002* | Servidor 02 (Web) | Servidor para la página web corporativa. | Cloudfare | Servidor (nube) | Nube | Sí |
| *ID\_0003* | Computadoras y Laptops | MacBook Pro 13 Pulgadas 2020 | Sonidista en Jefe | Ordenador (físico) | Sala de mezclas | Sí |
| *ID\_0004* | Computadoras y Laptops | iMac 2020 | Sonidista en Jefe | Ordenador (físico) | Sala de mezclas | Sí |
| *ID\_0005* | Componentes y Periféricos de Computadoras | Disco Duro Seagate 4tb | Jefe de estudio | Almacenamiento (físico) | Sala de mezclas | Sí |
| *ID\_0006* | Componentes y Periféricos de Computadoras | Disco Duro Seagate 4tb | Jefe de estudio | Almacenamiento (físico) | Sala de Mezclas | Sí |
| *ID\_0007* | Componentes y Periféricos de Computadoras | Impresora HP DeskJet | Jefe de estudio | Impresora | Recepción |  |
| *ID\_0008* | Componentes y Periféricos de Computadoras | Monitor Samsung 24" | Jefe de estudio | Periférico | Sala de Mezclas |  |
| *ID\_0009* | Componentes y Periféricos de Computadoras | Monitor Samsung 24" | Jefe de estudio | Periférico | Sala de Mezclas |  |
| *ID\_0010* | Componentes y Periféricos de Computadoras | Micrófno Profesional de Grabación con Pantalla | Jefe de estudio | Periférico | Sala de Grabación |  |
| *ID\_0011* | Componentes y Periféricos de Computadoras | Micrófno Profesional de Grabación con Pantalla | Jefe de estudio | Periférico | Sala de Grabación |  |
| *ID\_0012* | Computadoras y Laptops | ThinkPad Pro | Dueño del estudio | Ordenador (físico) | Oficina |  |
| *ID\_0013* | Componentes y Periféricos de Computadoras | Altoparlante Surround | Sonidista en Jefe | Periférico | Sala de Mezclas |  |
| *ID\_0014* | Componentes y Periféricos de Computadoras | Altoparlante Surround | Sonidista en Jefe | Periférico | Sala de Mezclas |  |
| *ID\_0015* | Componentes y Periféricos de Computadoras | Pantalla 48" LCD Samsung | Dueño del estudio | Periférico | Sala de Mezclas |  |
| *ID\_0016* | Componentes y Periféricos de Computadoras | Pantalla 48" LCD Samsung | Dueño del estudio | Periférico | Sala de Grabación |  |
| *ID\_0017* | Móviles | iPhone 13 | Jefe del estudio | Dispositivo móvil | (sin ubicación definida) | Sí |
| *ID\_0018* | Mezclador de sonido | Mezclador de sonido | Sonidista en Jefe | Periférico | Sala de mezclas |  |
| *ID\_0019* | Equipo de almacenamiento | Cloud | Jefe del estudio | Almacenamiento (nube) | Nube | Sí |
| *ID\_0020* | Aplicación | ProTools | Sonidista en Jefe | Aplicación | Macbook | Sí |
| *ID\_0021* | Aplicación | GuioNando | Jefe del estudio | Aplicación | Macbook | Sí |
| *ID\_0022* | Alarma | Sensor Infrarojo | Dueño del estudio | Alarma | Todo el estudio | - |
| *ID\_0023* | Alarma | Servicio de vigilancia | Securitas | Alarma | - | - |
| *ID\_0024* | Componentes y Periféricos de Computadoras | Altoparlante Surround | Sonidista en Jefe | Periférico | Sala de Grabación |  |
| *ID\_0025* | Componentes y Periféricos de Computadoras | Altoparlante Surround | Sonidista en Jefe | Periférico | Sala de Grabación |  |
| *ID\_0026* | Documentación | Planilla de trabajo | Jefe del estudio | Documentos | Recepción |  |
| *ID\_0027* | Documentación | Guiones | Jefe del estudio | Documentos | Sala de grabación |  |
| *ID\_0028* | Personas | Staff de la empresa | Jefe del estudio | Recursos Humanos | Sala de grabación | Sí |
| *ID\_0029* | Documentación | Directorio de talentos de doblaje | Jefe del estudio | Documentos | Estudio de grabación | Sí |

**2.2 Medidas de Seguridad**

Para proteger estos activos, "Voces y Ecos S.L." implementará las siguientes medidas de seguridad:

* **Cifrado de datos:** Para asegurar la confidencialidad y la integridad de las grabaciones, guiones y datos personales.
* **Autenticación fuerte:** Uso de autenticación multifactor (MFA) para acceder a sistemas críticos.
* **Backups regulares:** Realización de copias de seguridad diarias y semanales, tanto locales como en la nube.
* **Políticas de acceso restrictivas:** Control estricto de acceso a la información basada en roles y necesidades.
* **Formación en seguridad:** Programas de concienciación y formación continua para todos los empleados sobre las mejores prácticas de seguridad.

Este catálogo de activos, junto con las medidas de seguridad aplicables, ayudará a "Voces y Ecos S.L." a gestionar y proteger eficazmente sus recursos críticos, asegurando la continuidad de sus operaciones y la protección de su información sensible.

**3. Análisis de riesgo**

La definición moderna de riesgo como "incertidumbre en la consecución de los objetivos" refleja un enfoque más amplio y estratégico hacia la gestión de riesgos, alineando los esfuerzos de gestión de riesgos con los objetivos globales de la empresa. Este enfoque es especialmente relevante para una empresa como 'Voces y Ecos S.L.', que opera en el dinámico sector del doblaje y la grabación. Adaptar esta visión a la gestión de riesgos puede ayudar a 'Voces y Ecos S.L.' a anticipar, responder y adaptarse a cambios que podrían afectar su capacidad de alcanzar sus metas. Aquí se expone una visión adaptada:

### 3.1 Aplicación de los Conceptos de Gestión de Riesgos

#### **1. Activo (Fuente de Riesgo)**

En 'Voces y Ecos S.L.', los activos incluyen equipos técnicos como micrófonos, computadoras, software de edición, así como archivos digitales de proyectos y datos de clientes. La interrupción en la disponibilidad o el deterioro de cualquiera de estos activos podría significar un retraso en las entregas de proyectos, pérdida de datos de clientes o fallos en la producción, afectando directamente la operatividad y reputación de la empresa.

#### **2. Amenaza (Suceso)**

Las amenazas a estos activos podrían ser ataques cibernéticos que busquen acceder o corromper información, errores humanos que resulten en la pérdida de datos, o desastres físicos como incendios o inundaciones que dañen el equipo físico. La ampliación del concepto de amenaza a "suceso" enfatiza la necesidad de considerar cualquier circunstancia desfavorable que pueda ocurrir.

#### **3. Vulnerabilidad**

Las vulnerabilidades en 'Voces y Ecos S.L.' podrían incluir sistemas de seguridad de TI desactualizados, falta de formación en seguridad para los empleados, o infraestructura física inadecuada para proteger los equipos en caso de desastres naturales.

#### **4. Impacto**

El impacto de la materialización de una amenaza puede variar. Por ejemplo, un ataque cibernético exitoso podría resultar en la pérdida total de datos críticos del cliente (100% de degradación), mientras que un error humano que cause la pérdida de un archivo de proyecto podría ser parcialmente mitigado mediante recuperación de backups, representando un impacto menor.

#### **5. Probabilidad**

La probabilidad de cada suceso puede estimarse basándose en la experiencia previa, como la frecuencia de ataques cibernéticos sufridos en el pasado, o mediante consultas con expertos en seguridad de TI que puedan evaluar la efectividad de las medidas de seguridad actuales de la empresa.

Para mitigar estos riesgos, 'Voces y Ecos S.L.' podría implementar una serie de estrategias, tales como:

* **Actualizaciones de Seguridad**: Mantener todos los sistemas de seguridad informática actualizados para proteger contra vulnerabilidades conocidas.
* **Formación Continua**: Capacitar regularmente a todos los empleados en las mejores prácticas de seguridad para minimizar errores humanos y mejorar la respuesta a incidentes.
* **Planes de Recuperación de Desastres**: Establecer y mantener planes de recuperación ante desastres que incluyan soluciones de backup y contingencias operativas para garantizar la continuidad del negocio.

Al aplicar estos conceptos y estrategias, 'Voces y Ecos S.L.' podrá no solo proteger mejor sus activos sino también fortalecer su capacidad para alcanzar sus objetivos comerciales frente a incertidumbres y cambios en su entorno operativo.

### 3.2 Cálculo del Nivel de Riesgo

Multiplicamos el impacto por la probabilidad para obtener el nivel de riesgo para cada amenaza. Por ejemplo:

* Supongamos que la amenaza de un ataque de ransomware tiene un impacto estimado de 8 (pérdida significativa de datos y tiempo de inactividad) y una probabilidad de 0.2 (20% de posibilidades de que ocurra en un año). Entonces, el nivel de riesgo sería: Nivel de Riesgo=8×0.2=1.6\text{Nivel de Riesgo} = 8 \times 0.2 = 1.6Nivel de Riesgo=8×0.2=1.6

### Tabla de Nivel de Riesgo para 'Voces y Ecos S.L.'

| **ID del Activo** | **Descripción del Activo** | **Amenaza** | **Impacto Estimado** | **Probabilidad Estimada** | **Nivel de Riesgo (Impacto x Probabilidad)** |
| --- | --- | --- | --- | --- | --- |
| ID\_0003 | MacBook Pro 13" | Ataque de malware | 8 | 0.4 | 3.2 |
| ID\_0004 | iMac 2020 | Ataque de ransomware | 9 | 0.3 | 2.7 |
| ID\_0005 | Disco Duro Seagate 4tb | Fallo físico | 7 | 0.5 | 3.5 |
| ID\_0019 | Cloud Storage | Brecha de datos | 9 | 0.2 | 1.8 |
| ID\_0020 | ProTools | Pérdida de licencia | 6 | 0.1 | 0.6 |
| ID\_0022 | Sensor Infrarrojo | Desactivación por vandalismo | 5 | 0.3 | 1.5 |
| ID\_0027 | Guiones | Divulgación no autorizada | 10 | 0.4 | 4.0 |

### Tabla de Amenazas y Activos Afectados en 'Voces y Ecos S.L.'

| **ID del Activo** | **Descripción del Activo** | **Amenazas Identificadas** | **Activos Afectados** |
| --- | --- | --- | --- |
| ID\_0003 | MacBook Pro 13" | Ataque de malware, robo físico | Datos de proyectos, software de edición |
| ID\_0004 | iMac 2020 | Ataque de ransomware, fallo de hardware | Datos de clientes, archivos de audio |
| ID\_0005 | Disco Duro Seagate 4tb | Fallo físico, robo | Backups de proyectos, datos críticos |
| ID\_0019 | Cloud Storage | Brecha de datos, interrupción del servicio | Datos de clientes, proyectos almacenados |
| ID\_0020 | ProTools | Pérdida de licencia, incompatibilidad de actualizaciones | Software de producción |
| ID\_0022 | Sensor Infrarrojo | Desactivación por vandalismo, fallos técnicos | Seguridad física del estudio |
| ID\_0027 | Guiones | Divulgación no autorizada, pérdida física | Propiedad intelectual, documentos |
| ID\_0028 | Personal del estudio | Errores humanos, baja productividad | Operaciones de grabación y edición |
| ID\_0017 | iPhone 13 | Robo de dispositivo, acceso no autorizado a datos | Comunicaciones internas, acceso a redes |

### Tabla de Vulnerabilidades de 'Voces y Ecos S.L.'

| **ID del Activo** | **Descripción del Activo** | **Vulnerabilidades Identificadas** | **Recomendaciones de Mitigación** |
| --- | --- | --- | --- |
| ID\_0003 | MacBook Pro 13" | Software desactualizado, falta de entrenamiento en seguridad | Actualizar software, programas regulares de formación |
| ID\_0004 | iMac 2020 | Configuraciones de red inseguras, vulnerabilidad a malware | Implementar políticas de seguridad de red más estrictas |
| ID\_0005 | Disco Duro Seagate 4tb | Ausencia de cifrado, almacenamiento en ubicaciones físicamente accesibles | Implementar cifrado, mejorar la seguridad física |
| ID\_0019 | Cloud Storage | Dependencia de un solo proveedor, fallos de autenticación | Diversificar almacenamiento en la nube, autenticación de dos factores |
| ID\_0020 | ProTools | Vulnerabilidades de software no parcheadas, licencias expuestas | Mantener el software actualizado, gestionar licencias de forma segura |
| ID\_0022 | Sensor Infrarrojo | Mantenimiento inadecuado, susceptibilidad a sabotajes | Mejorar mantenimiento regular, instalar alarmas anti-sabotaje |
| ID\_0027 | Guiones | Almacenamiento en locaciones no seguras, acceso no regulado | Mejorar controles de acceso, utilizar almacenamiento seguro |
| ID\_0028 | Personal del estudio | Falta de capacitación en protección de datos, errores humanos | Programas continuos de capacitación en seguridad de datos |
| ID\_0017 | iPhone 13 | Uso de redes públicas inseguras, falta de políticas de dispositivo móvil | Prohibir uso de redes inseguras, implementar políticas de seguridad móvil |

**4. Planificación del Plan Director de Seguridad PDS**

Un Plan Director de Seguridad (PDS) para "Voces y Ecos S.L." que aborde sus objetivos de transformación digital y mejore sus capacidades de seguridad de la información, para lo cual necesitamos establecer un plan estructurado y detallado que priorice las inversiones en tecnología y capacitación. Dado que la empresa busca diferenciarse en su sector aprovechando las TIC y desea implementar prácticas de trabajo innovadoras y seguras, este PDS se centrará en asegurar tanto la infraestructura tecnológica como la conciencia de seguridad de su personal.

### 4.1 Tabla de Clasificación y Priorización

| ID | Proyecto | Origen | Tipo de Acción | Esfuerzo | Impacto | Coste Temporal | Prioridad |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 01 | Política de Seguridad | Cumplimiento Normativo | Organizativa | Medio | Alto | Corto | Alta |
| 02 | Plan de Concienciación de Seguridad | Análisis de Riesgos | Organizativa | Medio | Alto | Medio | Alta |
| 03 | Gestión de Incidentes | Análisis Técnico | Técnica | Alto | Muy Alto | Largo | Media |
| 04 | Adecuación al RGPD | Cumplimiento Normativo | Regulatoria | Alto | Alto | Medio | Alta |
| 05 | Mejora de Coordinación RRHH y TIC | Análisis de Riesgos | Organizativa | Medio | Medio | Corto | Media |
| 06 | Plan de Continuidad TIC | Análisis Técnico | Técnica | Muy Alto | Muy Alto | Largo | Alta |
| 07 | Seguridad de la Red Corporativa | Análisis Técnico | Técnica | Alto | Alto | Medio | Alta |
| 08 | Política de Copias de Seguridad | Análisis de Riesgos | Técnica | Medio | Alto | Medio | Alta |
| 09 | Clasificación de la Información | Cumplimiento Normativo | Organizativa | Bajo | Alto | Corto | Alta |
| 10 | Regulación de Servicios TIC por Terceros | Cumplimiento Normativo | Regulatoria | Medio | Medio | Largo | Me |

### Los proyectos con los puntajes más altos deben ser priorizados e iniciados primero, asegurando que los recursos disponibles se utilicen de manera más efectiva para abordar los riesgos más críticos y cumplir con las normativas. Los proyectos con puntajes más bajos deben planificarse para etapas posteriores o cuando los recursos lo permitan.

### 4.2 Proyecto: Plan Director de Seguridad para "Estudio de doblaje y grabación"

#### **Duración del Proyecto:**

3 años

#### **Presupuesto General:**

Alto (a definir según las necesidades detalladas de cada fase del proyecto)

### Objetivos del Proyecto:

1. **Asegurar la transformación digital de la empresa minimizando los riesgos de** seguridad asociados.
2. Fortalecer la postura de seguridad global para proteger contra amenazas internas y externas.
3. Cumplir con todas las regulaciones pertinentes, incluido el RGPD, y otras normativas de seguridad de la información.

### Líneas Principales de Actuación y Detalles del Proyecto:

#### **1. Desarrollo e Implementación de Política de Seguridad**

* **Acciones:**
  + Crear una política de seguridad que abarque el uso de dispositivos móviles, email, internet y la protección de datos.
  + Involucrar a la dirección en el compromiso con estas políticas para asegurar su implementación y cumplimiento.
* **Presupuesto Estimado:** 20,000 euros para el desarrollo, implementación y revisión inicial.

#### **2. Plan de Concienciación en Seguridad de la Información**

* **Acciones:**
  + Desarrollar un plan de formación continua para todo el personal, incluidos los directivos, sobre las prácticas seguras y la gestión de la información.
* **Presupuesto Estimado:** 10,000 euros anuales para sesiones de formación y materiales.

#### **3. Mejora de la Gestión de Incidentes y Atención al Usuario**

* **Acciones:**
  + Establecer un proceso formal para la gestión de incidentes de seguridad que incluya protocolos de respuesta rápida.
* **Presupuesto Estimado:** 10,000 euros para el desarrollo del sistema de gestión de incidentes y capacitación del equipo de respuesta.

#### **4. Adecuación al RGPD y Otras Normativas**

* **Acciones:**
  + Realizar un proyecto específico para adaptar todos los procesos y almacenamiento de datos al RGPD.
* **Presupuesto Estimado:** 25,000 euros para consultoría legal y adaptación de sistemas.

#### **5. Desarrollo de un Plan de Continuidad y Recuperación de TI**

* **Acciones:**
  + Implementar planes de continuidad de operaciones y recuperación ante desastres que abarquen todos los aspectos críticos de TI.
* **Presupuesto Estimado:** 25,000 euros para desarrollo de plan, compra de equipamiento y pruebas regulares.

#### **6. Seguridad de la Red Corporativa**

* **Acciones:**
  + Mejorar la infraestructura de la red con segmentación avanzada y sistemas de prevención de intrusiones.
* **Presupuesto Estimado:** 20,000 euros para hardware, software y configuración.

#### **7. Política de Copias de Seguridad y Clasificación de la Información**

* **Acciones:**
  + Implementar un sistema de clasificación y etiquetado de la información, así como políticas de copias de seguridad y restauración periódicas.
* **Presupuesto Estimado:** 15,000 euros para software de clasificación, almacenamiento seguro y formación.

#### **8. Regulación de los Servicios TIC de Terceros**

* **Acciones:**
  + Evaluar y estandarizar los contratos con todos los proveedores de servicios TIC para asegurar el cumplimiento y la seguridad.
* **Presupuesto Estimado:** 25,000 euros para auditorías y renegociación de contratos.

### Implementación y Seguimiento:

* **Planificación Detallada:** Se establecerán planes detallados para cada línea de actuación, incluyendo cronogramas, responsables y KPIs para la evaluación de progreso.
* **Revisión y Ajustes:** Revisiones trimestrales para ajustar el plan según los avances tecnológicos y cambios en el panorama de amenazas.
* **Evaluación de Impacto:** Evaluaciones anuales para medir la efectividad del PDS y el ROI en términos de reducción de incidentes y mejoras en la seguridad.

**4.3 Tabla de Calendario de Implementación y Seguimiento del PDS**

| **Año/Trimestre** | **Actividades** | **Presupuesto Estimado** |
| --- | --- | --- |
| **Año 1 - T1** | - Lanzamiento del proyecto y reuniones iniciales. <br> - Auditoría inicial de seguridad. <br> - Desarrollo de la política de seguridad. | 15,000 € |
| **Año 1 - T2** | - Implementación de política de seguridad. <br> - Inicio del plan de concienciación en seguridad. <br> - Diseño del sistema de gestión de incidentes. | 15,000 € |
| **Año 1 - T3** | - Implementación del sistema de gestión de incidentes. <br> - Adaptación al RGPD. <br> - Desarrollo del Plan de Continuidad de TI. | 15,000 € |
| **Año 1 - T4** | - Implementación del Plan de Continuidad de TI. <br> - Revisión de políticas de seguridad. <br> - Revisión de contratos con proveedores TIC. | 15,000 € |
| **Año 2 - T1** | - Continuación del plan de concienciación en seguridad. <br> - Mejoras en seguridad de red. <br> - Implementación de políticas de copias de seguridad. | 15,000 € |
| **Año 2 - T2** | - Clasificación y políticas de acceso de información. <br> - Revisión de mejoras en la red. <br> - Segunda revisión de política de seguridad. | 15,000 € |
| **Año 2 - T3** | - Continuación de acciones de plan de continuidad y recuperación. <br> - Auditoría de seguridad de medio término. <br> - Ajustes basados en auditoría y feedback. | 15,000 € |
| **Año 2 - T4** | - Revisión de servicios TIC de terceros. <br> - Implementación de mejoras post-auditoría. <br> - Preparación para el tercer año del PDS. | 15,000 € |
| **Año 3 - T1** | - Tercera fase del plan de concienciación en seguridad. <br> - Revisión estratégica de seguridad. <br> - Ajustes en el Plan de Continuidad de TI. | 15,000 € |
| **Año 3 - T2** | - Implementación de tecnologías emergentes en seguridad. <br> - Revisión y mejora de clasificación de información. <br> - Evaluación continua de cumplimiento normativo. | 15,000 € |
| **Año 3 - T3** | - Segunda auditoría de seguridad de medio término. <br> - Ajustes en políticas de copias de seguridad. <br> - Planificación para la sostenibilidad del PDS. | 15,000 € |
| **Año 3 - T4** | - Preparación de informes finales. <br> - Evaluación final del impacto del PDS. <br> - Reuniones de cierre del proyecto y planificación para futuras actualizaciones y mantenimiento continuo del PDS. | 15,000 € |

**5. Conclusión**

La implementación del Plan Director de Seguridad en Voces y Ecos S.L. traerá múltiples beneficios que fortalecerán la posición de la empresa en un entorno cada vez más digitalizado y expuesto a ciberamenazas. Al adoptar medidas robustas de ciberseguridad, la empresa no solo protegerá su valiosa información y la de sus clientes, sino que también mejorará su resiliencia frente a posibles incidentes.

**Consecuencias Positivas de la Ciberseguridad y la IA para Voces y Ecos S.L.**

1. **Protección de Datos Sensibles**: Implementar sistemas avanzados de ciberseguridad asegura la protección de datos críticos como guiones, grabaciones originales y contratos, mitigando el riesgo de pérdidas o filtraciones que podrían tener graves consecuencias financieras y reputacionales​​​​.
2. **Eficiencia Operativa**: La automatización y optimización de procesos mediante inteligencia artificial (IA) pueden aumentar la eficiencia operativa, reduciendo tiempos y costos en tareas como la producción de doblaje y grabación​​​​.
3. **Mejora en la Calidad del Servicio**: El uso de IA puede mejorar significativamente la calidad del doblaje, permitiendo una sincronización de labios más precisa y una adaptación de voces que suena natural, lo que es crucial para la satisfacción del cliente y la competitividad en el mercado​​​​.
4. **Detección y Respuesta Rápida a Amenazas**: Los sistemas de ciberseguridad basados en IA son capaces de identificar y responder rápidamente a ciberamenazas, reduciendo el tiempo de reacción ante incidentes y limitando el impacto de posibles ataques​​.
5. **Adaptabilidad y Escalabilidad**: Las soluciones de seguridad impulsadas por IA pueden escalar y adaptarse a medida que la empresa crece, gestionando grandes volúmenes de datos y numerosos dispositivos conectados, lo cual es esencial en un entorno tecnológico en constante evolución​​​​.

**Competidores y colaboradores de Voces y Ecos S.L. en España**

En el ámbito del doblaje y grabación, Voces y Ecos S.L. se enfrenta a la competencia de varias empresas bien establecidas en España, entre ellas:

1. **SDI Media**: Una de las mayores empresas de servicios de doblaje y subtitulación a nivel mundial, con una fuerte presencia en España.
2. **Soundub**: Especializada en doblaje, mezcla de sonido y postproducción audiovisual.
3. **Deluxe Spain**: Parte de Deluxe Entertainment Services Group, ofrece servicios de doblaje, subtitulación y postproducción.
4. **Polford**: Conocida por su trabajo en doblaje de películas y series de televisión.
5. **International Sound Studio**: Provee servicios de doblaje y grabación para cine, televisión y publicidad.

Implementar un Plan Director de Seguridad eficaz permitirá a Voces y Ecos S.L. no solo cumplir con las normativas vigentes, sino también diferenciarse en el mercado mediante la garantía de seguridad y confiabilidad en sus servicios. Con ello, la empresa podrá consolidar su posición competitiva y continuar innovando en el sector del doblaje y grabación.**6. Referencias**

Estas referencias proporcionan un marco comprensivo para la creación, implementación y gestión del Plan Director de Seguridad en un estudio de doblaje y grabación, cubriendo aspectos legales, técnicos y estratégicos necesarios para proteger efectivamente los activos de información del estudio.

* **Guía para la Elaboración del Plan Director de Seguridad**
* **Guía de Análisis de Riesgos**
* **Guía de Inventariado de Activos**
* **Normativas y Estándares**
* **Esquema Nacional de Seguridad (ENS)**
* **ISO/IEC 27001:2013 - Sistema de Gestión de Seguridad de la Información**
* **ISO/IEC 27002:2013 - Código de Práctica para Controles de Seguridad de la Información**
* **ISO/IEC 27005:2018 - Gestión de Riesgos de Seguridad de la Información**
* **UNE-EN ISO/IEC 27000:2019** - Proporciona una visión general y vocabulario sobre los Sistemas de Gestión de la Seguridad de la Información (PDS), esencial para establecer y definir los marcos y términos en la gestión de la seguridad de la información.
* **Ley Orgánica 3/2018** - Importante para comprender los requisitos legales en España respecto a la protección de datos personales y garantía de los derechos digitales.
* **Reglamento (UE) 2016/679 (RGPD)** - Crítico para garantizar que el estudio cumpla con las normativas de la UE sobre la protección de datos personales, un aspecto crucial para cualquier empresa que maneje datos personales dentro de la UE.
* **MAGERIT – versión 3.0** - Esta metodología de análisis y gestión de riesgos de los sistemas de información es particularmente valiosa para estructurar cómo se identifican, analizan y gestionan los riesgos en el estudio.
* **ISO/IEC 27001:2013, ISO/IEC 27002:2017, y ISO/IEC 27005:2018** - Estas normas ofrecen guías sobre los requisitos para un PDS, prácticas de control de seguridad, y gestión de riesgos de seguridad de la información, respectivamente, proporcionando un marco robusto para la implementación de medidas de seguridad efectivas.
* **ISO 31000:2018** - Ofrece principios y directrices sobre gestión de riesgos, útil para integrar la gestión de riesgos de seguridad de la información en las prácticas de gestión de riesgos más amplias del estudio.
* **INCIBE – Colección “Protege tu empresa: Plan director de seguridad” y “Kit de concienciación para empresas”** - Estos recursos del Instituto Nacional de Ciberseguridad de España son herramientas prácticas para implementar y mejorar la concienciación sobre la seguridad en el estudio.