Hoja 1: Resumen de Auditoría

Esta hoja proporciona una visión general del nivel de cumplimiento de las cinco funciones principales del NIST Cybersecurity Framework (CSF):

- **Identificación** (Identificar activos y riesgos).
- **Protección** (Control de acceso, gestión de activos, etc.).
- **Detección** (Monitoreo de seguridad).
- **Respuesta** (Planes para incidentes de ciberseguridad).
- **Recuperación** (Planificación de recuperación de desastres y continuidad del negocio).

Aquí, el equipo de auditoría de XFlight puede hacer una evaluación rápida del estado actual de ciberseguridad. En este caso:

- **Cumple Totalmente**: Si el área cumple con todos los requisitos.
- **Cumple Parcialmente**: Cumple, pero requiere ajustes o mejoras.
- **No Cumple**: No hay evidencia o los controles son insuficientes.

Ejemplo de uso en XFlight:

- **Identificación**: Cumple totalmente porque hay un inventario actualizado de los activos.
- **Protección**: Cumple totalmente, ya que se utilizan controles de acceso y autenticación multifactor (MFA).
- **Recuperación**: No cumple, ya que XFlight no ha desarrollado un plan formal de recuperación ante incidentes.

Razón de la hoja: Esta hoja es útil para presentar rápidamente el estado general a los directivos y facilitar la toma de decisiones estratégicas.

Área Evaluada	Cumple Totalmente	Cumple Parcialmente	No Cumple	Comentario
Identificación	✔			Cumple en su mayoría
Protección	✔			Cumple todas las medidas
Detección		✔		Falta mejorar en X área
Respuesta		✔		Se requiere plan de mejora
Recuperación			✔	No existen planes formales

Hoja 2: Detalle de Controles por Categoría del NIST CSF

Esta hoja proporciona un análisis más detallado de las subcategorías de cada función del NIST CSF. Aquí es donde los auditores pueden ver cómo XFlight se desempeña en controles específicos dentro de las cinco funciones clave. Cada control se evalúa de forma cualitativa con una escala de 1 a 5 (1 = No cumple, 5 = Cumple totalmente).

Ejemplo de uso en XFlight:

- **Función: Identificar**
  Subcategoría: **ID.AM-1** (Identificación y gestión de activos).
    - **Cumplimiento: 4**
    - **Evidencia: Inventario de activos actualizado**
    - **Acción Correctiva: Mejorar el control de dispositivos de IoT y periféricos**.
- **Función: Responder**
  Subcategoría: **RS.RP-1** (Planificación de respuesta a incidentes).
    - **Cumplimiento: 2**
    - **Evidencia: No existen pruebas documentadas**
    - **Acción Correctiva: Realizar simulacros trimestrales**.

Razón de la hoja: Proporciona una evaluación detallada y permite identificar áreas específicas donde XFlight debe mejorar o ajustar sus controles.

Función	Categoría	Subcategoría	Descripción	Nivel de Cumplimiento (1-5)	Evidencia	Acción Correctiva/Recomendación
Identificar	Gestión de activos	ID.AM-1	Los activos físicos están identificados y gestionados	4	Inventario de activos actualizado	Mejorar el control de dispositivos
Identificar	Gestión de riesgos	ID.RA-1	Los riesgos de ciberseguridad están identificados y priorizados	3	Matriz de riesgos	Realizar evaluación de riesgos cada 6 meses
Proteger	Control de acceso	PR.AC-1	Los usuarios son autenticados y autorizados para acceder a los activos	5	MFA habilitado para usuarios	N/A
Detectar	Monitoreo continuo	DE.CM-1	Se implementan	3	Logs SIEM	Mejorar la cobertura de

Función	Categoría	Subcategoría	Descripción	Nivel de Cumplimiento (1-5)	Evidencia	Acción Correctiva/Recomendación
			sistemas de monitoreo continuo para detectar actividades anómalas			monitoreo en el 100% de los sistemas
Responder	Planificación de respuesta	RS.RP-1	El plan de respuesta a incidentes está formalizado y probado	2	No existen pruebas documentadas	Realizar simulacros trimestrales
Recuperar	Plan de recuperación	RC.RP-1	Planes de recuperación ante incidentes están desarrollados	1	No hay plan formal	Crear plan de recuperación y pruebas de resiliencia

Hoja 3: Detalle de Controles NIST SP 800-53 (Familias de Control)

Esta hoja profundiza en los controles de seguridad específicos basados en el estándar NIST SP 800-53, que es un marco de controles más técnico y específico. Los controles se agrupan por "Familias de Control" (como gestión de acceso, auditoría, configuraciones, etc.). Este nivel de detalle es importante para XFlight ya que maneja datos sensibles y críticos.

Ejemplo de uso en XFlight:

- **Familia de Control: Acceso a la Información (AC)**
  Control Específico: **AC-2**
  - **Descripción del Control**: Control de acceso basado en roles.
  - **Cumplimiento: 4**
  - **Evidencia: Roles definidos y revisados mensualmente**
  - **Acción Correctiva: Revisar acceso de usuarios cada 3 meses**.
- **Familia de Control: Conciencia y Entrenamiento (AT)**
  Control Específico: **AT-2**
  - **Descripción del Control**: Capacitación en ciberseguridad para empleados.
  - **Cumplimiento: 2**
  - **Evidencia: Solo hay capacitación anual**

- **Acción Correctiva: Implementar capacitaciones trimestrales**.

Razón de la hoja: Sirve para cumplir con las normativas de seguridad más detalladas y técnicas, especialmente en áreas críticas como el control de acceso y la gestión de configuraciones.

Familia de Control	Control Específico	Descripción del Control	Nivel de Cumplimiento (1-5)	Evidencia	Acción Correctiva
Acceso a la Información (AC)	AC-2	Control de acceso basado en roles	4	Roles definidos	Revisar acceso de usuarios cada 3 meses
Auditoría y Responsabilidad (AU)	AU-6	Revisión y análisis de registros de auditoría	3	Logs revisados mensualmente	Implementar revisiones automáticas
Conciencia y Entrenamiento (AT)	AT-2	Capacitación en ciberseguridad para empleados	2	Solo hay capacitación anual	Implementar capacitaciones trimestrales
Gestión de Configuraciones (CM)	CM-6	Monitoreo continuo de las configuraciones del sistema	3	Herramienta de monitoreo parcial	Ampliar monitoreo a sistemas críticos