https://learn.microsoft.com/es-es/security/zero-trust/adopt/identify-protect-sensitive-business-data   
  
Grupo 3: Describir las actividades clave en cada fase y su relevancia para la seguridad de la información.

JuanC

* Ciclo de Adopción de Confianza Cero (Introducción)

El ciclo de adopción para la protección de datos empresariales críticos en el enlace de Microsoft describe un enfoque en varias etapas. Comienza identificando datos sensibles y críticos dentro de la organización. Luego, se implementan medidas de protección basadas en riesgos para asegurar estos datos. Posteriormente, se pasa a monitorear y mejorar continuamente la protección a través de herramientas y políticas de seguridad

* Fase de definición de la estrategia

En la **Fase de definición de la estrategia**, las empresas deben establecer una visión y objetivos claros para la protección de datos críticos. Esta etapa incluye:

* **Análisis del Panorama de Riesgos**: Se evalúan las amenazas y vulnerabilidades relevantes que pueden afectar los datos sensibles.
* **Identificación de Datos Sensibles**: Se clasifica la información según su importancia y riesgo asociado, priorizando los activos más críticos.
* **Desarrollo de Políticas de Protección**: Se crean políticas que definan cómo proteger los datos, alineadas con los principios de Confianza Cero, garantizando el acceso controlado y verificado.
* **Alineación Organizacional**: Es fundamental asegurar que las políticas estén alineadas con los objetivos estratégicos generales de la organización, promoviendo una cultura de seguridad.

En esta fase, se establecen las bases para las siguientes etapas del ciclo de adopción, proporcionando un enfoque estructurado para la protección de datos.

* Fase de planeamiento

En la **Fase de planeamiento**, se traduce la estrategia de protección de datos en un conjunto de acciones prácticas. Esta fase comienza con la identificación de recursos necesarios, que incluyen:

1. **Tecnología**: Selección de herramientas como software de cifrado, sistemas de detección de intrusiones y soluciones de gestión de identidades.
2. **Recursos Humanos**: Asignación de roles y responsabilidades a equipos específicos para asegurar que todos entiendan sus funciones en la implementación.
3. **Finanzas**: Evaluación del presupuesto necesario para adquirir las herramientas y capacitar al personal.

* 1. \*\*Desarrollo de un Plan de Acción\*\*:

- Crear un plan detallado que incluya pasos concretos para implementar las políticas y procedimientos de seguridad establecidos en la fase de definición.

- Establecer un cronograma que defina plazos para cada etapa del proceso.

* 2. \*\*Asignación de Recursos\*\*:

- Identificar y asignar los recursos necesarios, incluyendo personal, presupuesto y tecnología.

- Determinar roles y responsabilidades dentro del equipo de seguridad y los equipos de datos e IA.

* 3. \*\*Integración de Equipos\*\*:

- Facilitar la colaboración entre los equipos de IT, seguridad, datos y desarrollo de IA para asegurar que todos estén alineados con la estrategia de confianza cero.

- Establecer canales de comunicación efectivos para compartir información y actualizaciones.

* 4. \*\*Definición de Controles de Seguridad\*\*:

- Especificar los controles de seguridad que se implementarán, como cifrado, autenticación, monitoreo y segmentación de datos.

- Detallar cómo se aplicarán estos controles en cada etapa del ciclo de vida de los datos y los modelos de IA.

* 5. \*\*Establecimiento de Métricas y KPIs\*\*:

- Definir métricas claras para evaluar la efectividad de las medidas de seguridad implementadas.

- Establecer indicadores clave de rendimiento (KPIs) que permitan medir el progreso y el éxito de la estrategia.

* 6. \*\*Plan de Capacitación y Concienciación\*\*:

- Desarrollar un programa de capacitación que asegure que todos los empleados comprendan su rol en la implementación de la estrategia de confianza cero.

- Incluir módulos sobre mejores prácticas en la gestión de datos y uso ético de IA.

* 7. \*\*Simulaciones y Pruebas\*\*:

- Planificar simulaciones y pruebas de incidentes para evaluar la efectividad de los planes de respuesta a incidentes.

- Asegurar que el personal esté preparado para actuar ante situaciones de riesgo.

* 8. \*\*cc\*\*:

- Crear documentación exhaustiva que detalle cada aspecto del plan, incluyendo políticas, procedimientos y protocolos de seguridad.

- Establecer un sistema de seguimiento para monitorear la implementación y ajustar el plan según sea necesario

Además, se elabora un cronograma con hitos claros que guíen la implementación, estableciendo un plan de acción que abarque pruebas, implementación y revisión. Este enfoque sistemático permite que la organización se adapte a cambios en el entorno de amenazas, garantizando una respuesta proactiva y ágil.

**Adr**

#### **Fase de Preparación**

1. Definición de Datos Confidenciales: Asegúrese de que los datos críticos para la organización estén claramente definidos y ajuste estas definiciones conforme se avance en el análisis.
2. Mapeo de Datos y Aplicaciones: Elabore un mapa de conjuntos de datos y aplicaciones prioritarias, extendiendo gradualmente el alcance hasta abarcar toda la infraestructura digital.
3. Instrucciones Técnicas: Documente los ajustes necesarios para adaptarse al entorno de la organización.
4. Clasificación de Datos: Familiarícese con las funcionalidades de clasificación de datos (tipos, etiquetas, políticas DLP) y comience su implementación en Microsoft 365.
5. Protección en Dispositivos: Implemente políticas de DLP en dispositivos y amplíe estas funcionalidades a aplicaciones en la nube mediante Defender for Cloud Apps.
6. Detección en Entornos Locales: Use Microsoft Purview para proteger datos en entornos locales y gobernanza de datos en almacenamiento en la nube.

#### **Fase de Adopción**

* Enfoque Iterativo: Realice el proceso de detección y protección de datos confidenciales de manera iterativa, mejorando continuamente el esquema y las políticas conforme se obtienen resultados.
* Implementación Práctica: No es necesario esperar a completar una fase antes de comenzar la siguiente; los ciclos de retroalimentación mejoran la eficacia.

#### **Fases de Gobernanza y Administración**

1. Metodología de Revisión: Establezca un enfoque para revisar el esquema de clasificación y evaluar el éxito de las políticas de protección.
2. Base de Gobernanza Inicial (MVP): Comience con herramientas de gobernanza simples y efectivas.
3. Mejoras Iterativas: Agregue controles adicionales de gobernanza conforme se identifiquen riesgos.

### **Fase de Preparación**

En esta fase, se recomienda establecer un plan para identificar y proteger los datos confidenciales como parte de la estrategia de Confianza Cero. Es fundamental definir claramente qué datos son confidenciales y crear un mapa de conjuntos de datos y aplicaciones para priorizar el trabajo.

**Pasos a seguir:**

1. Familiarizarse con las funcionalidades de clasificación de datos en Microsoft 365.
2. Implementar estas funcionalidades en los datos y aplicaciones de Office.
3. Proteger datos en dispositivos usando DLP (Prevención de Pérdida de Datos).
4. Extender la protección a aplicaciones en la nube mediante Defender for Cloud Apps.
5. Utilizar herramientas como Microsoft Purview para proteger datos en entornos locales y servicios en la nube.

**Consideraciones:**

* La coordinación con Intune es necesaria para proteger datos en dispositivos.
* La protección en aplicaciones SaaS requiere Defender for Cloud Apps.

A medida que se avanza, es importante iterar en el proceso y ajustar las estrategias de protección.

### **Fase de Adopción**

Se sugiere un enfoque iterativo para detectar y proteger datos confidenciales. Comenzar la implementación de un esquema de clasificación y protección desde el inicio permite mejorar las herramientas y directivas a lo largo del proceso, facilitando ajustes según los resultados obtenidos.

### **Fases de Gobernanza y Administración**

La gobernanza de datos es un proceso continuo. Para establecer una base sólida, se recomienda:

1. Definir una metodología para revisar el esquema de clasificación y su efectividad.
2. Comenzar con un conjunto básico de herramientas de gobernanza (producto viable mínimo).
3. Mejorar progresivamente los controles de gobernanza.

Microsoft Purview ofrece funcionalidades para controlar los datos, incluidas políticas de retención y administración de registros. Además, herramientas como el explorador de actividades y Microsoft Defender for Cloud Apps proporcionan visibilidad y control sobre los datos confidenciales.

**Conjunto**

Recomendaciones en la aplicación a una empresa ficticia:

(yo resumiria con nuestras palabras por encima cada apartado)

**Fase de Definición de la Estrategia:**

* Realizar un análisis de riesgos y clasificar los datos sensibles.
* Desarrollar políticas de protección alineadas con Confianza Cero.
* Alinear a todos los equipos con los objetivos de seguridad de la empresa.

**Fase de Planeamiento:**

* Crear un plan de acción detallado con hitos y plazos.
* Asignar recursos humanos, tecnológicos y financieros necesarios.
* Fomentar la colaboración entre equipos de IT, seguridad y desarrollo.

**Fase de Preparación:**

* Implementar la clasificación de datos y proteger la información en dispositivos y aplicaciones.
* Usar herramientas como Microsoft Intune y Defender para prevenir pérdida de datos.

**Fase de Adopción:**

* Implementar un esquema de protección de datos y ajustarlo de forma iterativa.
* Mejorar continuamente herramientas y políticas según los resultados.

**Fase de Gobernanza y Administración:**

* Definir una metodología para revisar la clasificación y la efectividad de las políticas.
* Monitorear y ajustar las medidas de seguridad continuamente.