Decreto 612 de 2018

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Alcaldía municipal de San Bernardo del Viento

2024

Contenido

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI	
Nombre del documento	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
Versión del documento	5.0
Fecha	29/01/2024
Resumen	El presente documento define las medidas de seguridad identificadas para desarrollar e implementar al 31 de diciembre del 2024 el plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios en la alcaldía municipal de San Bernardo del Viento.

Control de Cambios		
Control de Cambios		
Fecha	**Versión**	**Descripción**
31/01/2020	1.0	Creación
29/01/2021	2.0	Seguimiento
29/01/2022	3.0	Seguimiento
29/01/2023	4.0	Seguimiento
29/01/2024	4.0	Seguimiento

1. RESUMEN EJECUTIVO

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos de la alcaldía municipal de San Bernardo del Viento.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad, la alcaldía municipal de San Bernardo del Viento define medidas que serán aplicadas en el segundo semestre del año 2024. Las anteriores medidas se definieron teniendo en cuenta la información del análisis de riesgos, el cual brindó información acerca de las necesidades del Proceso de Tecnología de la alcaldía municipal de San Bernardo del Viento en cuanto a la seguridad y privacidad de la información y proporcionó las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

2. INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios de la alcaldía municipal de San Bernardo del Viento, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia establece que la seguridad de la información es un elemento que apoya a las entidades de manera trasversal, habilitando el desarrollo de los componentes de la política de Gobierno Digital, desarrollado a través de lineamientos en materia de seguridad y privacidad de la información, así como de gestión de riesgos de seguridad digital, lo cuales soportan las acciones establecidas por cada entidad para proteger los activos de información, preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos. El Manual de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones entre sus propósitos pretende lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información, que consiste en desarrollar procesos y procedimientos que hagan uso de las tecnologías de la información, a través de la incorporación de esquemas de manejo seguro de la información y de la alineación con la arquitectura institucional de la

entidad (Arquitectura misional y Arquitectura de TI), a fin de apoyar el logro de las metas y objetivos de la entidad. En ese sentido, teniendo en cuenta el nuevo concepto de Gobierno Digital y la alineación de la Política de Gobierno Digital, acorde con lo establecido en el Modelo de Seguridad y Privacidad de la Información – MSPI, Controles de Seguridad y Privacidad de la Información, se estipulan los lineamientos del presente plan.

3. DEFINICIONES

Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Impacto: son las consecuencias que genera un riesgo una vez se materialice.

Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos. Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

4. OBJETIVOS

- Establecer el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, como un instrumento que permita adoptar medidas y acciones encaminadas a controlar y minimizar los riesgos de seguridad y privacidad de la información de la Alcaldía de San Bernardo de viento.

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios que la alcaldía municipal de San Bernardo del Viento pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

- Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, de acuerdo con los contextos establecidos en la Entidad.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios de la alcaldía municipal de San Bernardo del Viento.

5. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Junto con Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016): se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la alcaldía municipal de San Bernardo del Viento.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Moderado, Alto y Extremo acorde con los lineamientos definidos por la alcaldía municipal de San Bernardo del Viento, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

Creando así una línea base del tratamiento de riesgos en la alcaldía municipal de San Bernardo del viento, facilitando la identificación de los riesgos que se encuentran presentes en la entidad; de la misma manera los funcionarios conozca el proceso de mitigación de riesgos para lograr minimizar la pérdida de información o daños en los equipos.

6. MARCO DE REFERENCIA

La alcaldía municipal de San Bernardo del Viento a través de su Modelo Integrado de Gestión se orienta hacia una cultura de la gestión del riesgo asociados en el desarrollo de sus procesos, en aras de cumplir con su responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC que contribuyen al desarrollo social y económico del país, al desarrollo integral de los ciudadanos y la mejora en su calidad de vida.

El objetivo de la política es establecer los parámetros necesarios para una adecuada gestión de los riesgos de gestión, corrupción, Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de los servicios de la alcaldía municipal de San Bernardo del Viento procurando que no se materialicen, atendiendo los lineamientos establecidos en Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de interés.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

6.1. Política de administración de riesgos

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

- Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles

apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

- ➔ Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

- ➔ Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

La gestión de riesgos de Seguridad y privacidad de la Información, seguridad digital y continuidad de la operación de los servicios le permite a la alcaldía realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La administración de riesgos de seguridad y privacidad de la información se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas.

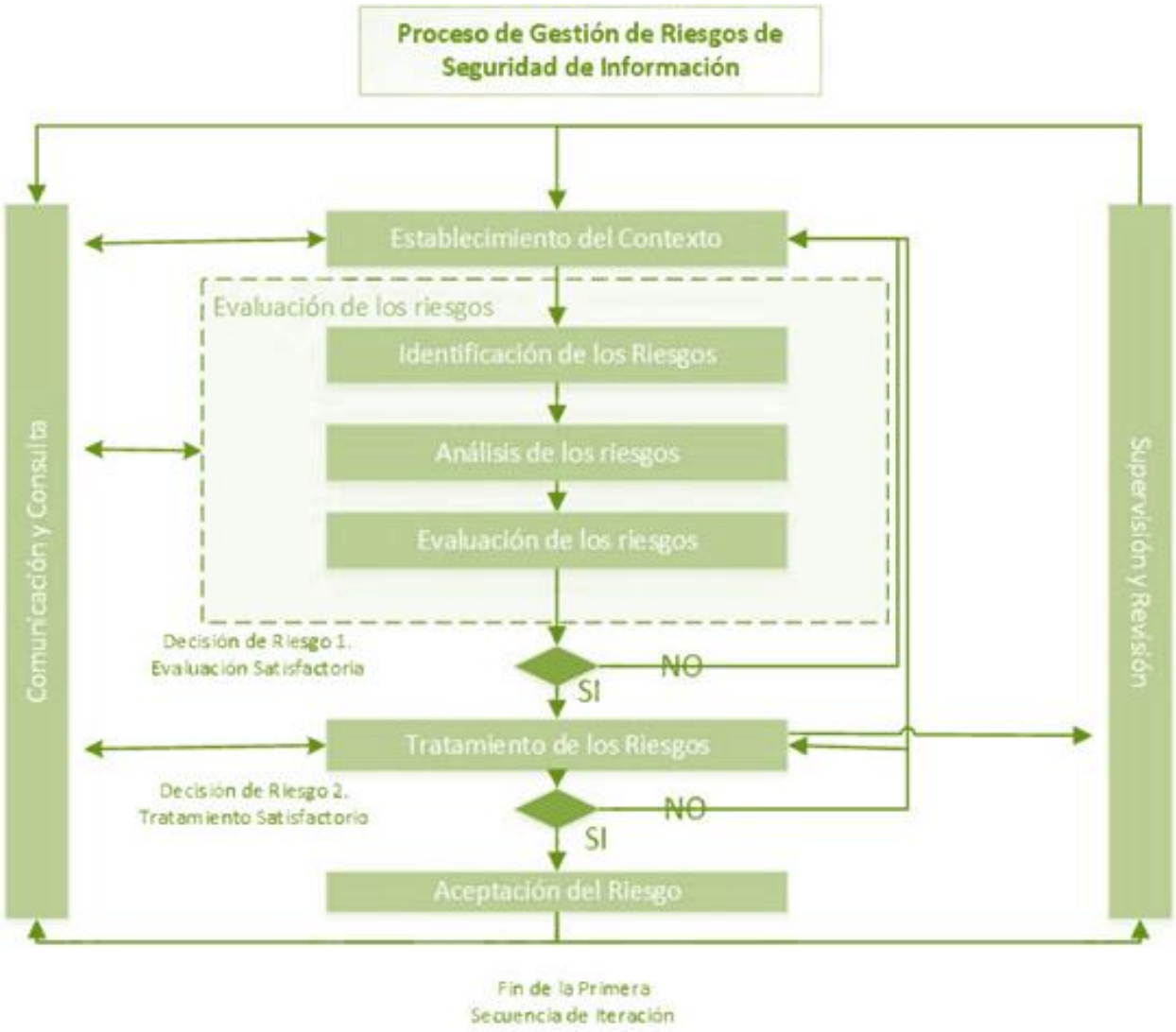
7. METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de información de los diferentes procesos de la Alcaldía de San Bernardo de viento, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información de la Alcaldía.

GESTION DE RIESGO					
FASES	**ACTIVIDAD**	**TAREA**	**RESPONSABLE**	**FECHA INICIO**	**FECHA FINAL**
Fase 1 Planeación de la gestión del riesgo	Revisar y ajustar metodología para la gestión de Riesgo de Seguridad Digital Y lineamientos de riesgo	Actualizar políticas y metodologías	Equipo de gestión de riesgos	Febrero 2024	Febrero 2024
Fase 2 Identificación y valoración de activos	Identificación de Información, clasificación de Información y Valoración de Información. - Sensibilización	Socialización guía y herramienta, gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Equipo de gestión de riesgos	Marzo de 2024	Marzo de 2024
	Identificación de riesgos y seguridad de la información, seguridad digital y continuidad de la operación	Identificación, análisis y evaluación de riesgos y seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Equipo de gestión de riesgos	abril de 2024	abril de 2024
Fase 3 identificación de amenazas y Vulnerabilidades	Aceptación de riesgos identificados y vulnerabilidad	Aceptación, aprobación de riesgos identificados y planes de tratamientos	Equipo de gestión de riesgos	mayo de 2024	junio de 2024
Fase 4 Determinación de riesgos	Determinación del Impactos de las amenazas por activo de Probabilidad de Ocurrencia	Publicación matriz de riesgos	Equipo de gestión de riesgos	julio de 2024	agosto de 2024
Fase 5 Análisis de riesgo	Seguimiento fase de tratamiento	Seguimiento estado de planes de tratamientos de riesgos identificados y verificación de evidencias	Equipo de gestión de riesgos	septiembrede 2024	Septiembre de 2024
Fase 6 Gestión de riesgos	Determinación de Controles Tratamiento de Riesgos Diseño de controles Priorización de Controles	Evaluación de riesgos residuales	Equipo de gestión de riesgos	octubre de 2024	octubre de 2024
Fase 7 Planificación de controles	Medición de la eficacia de los controles, Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Equipo de gestión de riesgos	Noviembre de2024	Noviembre de2024
		Actualización guía de gestión de riesgos, seguridad de la información de acuerdo a los cambio solicitados		Diciembre de 2024	Diciembre de2024
Fase 8 Monitoreo	Monitoreo y revisión	Generación, presentación y reportes de indicadores	Equipo de gestión de riesgos	Diciembre de 2024	N/A

7.1. Desarrollo metodológico

En la figura siguiente se presenta el modelo de gestión de riesgos de seguridad de la información basada tanto en la norma ISO/IEC 31000 como en la ISO 27005 para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:



Fuente: Tomado de Proceso de gestión de riesgos ISO 27005:2008

7.2. Oportunidad de mejora

La alcaldía municipal de San Bernardo del Viento no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

8. RECURSOS

La alcaldía municipal de San Bernardo del Viento, en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	La Oficina de Tecnologías de la información a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía de Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - octubre de 2018 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI) , ISO 27005, Magerit
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos para los controles producto de la gestión de riesgos

8.1. Presupuesto

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios identificados en la entidad, corresponderá al presupuesto Asignado por el año en vigencia del municipio, las diferentes dependencias serán responsables de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos y del plan de tratamiento.

9. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La medición se realiza con un indicador de gestión, está orientada principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicador que se alimenta de indicadores internos en el marco de la implementación del Eje de Seguridad de la Información y que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre Seguridad de la informa.

HOJA DE VIDA DEL INDICADOR

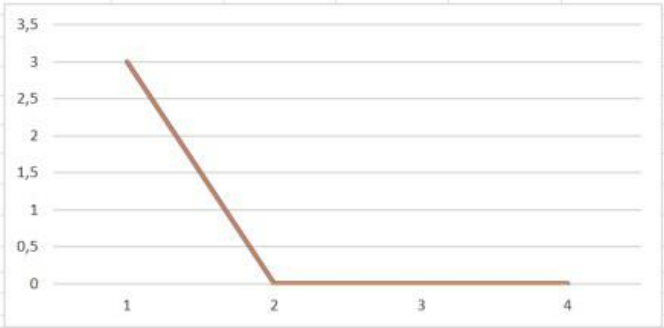
Despliegue de Objetivos	
Dimensión:	D2 Entorno del Ecosistema Digital
Objetivo:	O5 Consolidar al MINTIC como una organización centrada en la innovación, basada en procesos transversales y orientada al desarrollo potencial de las personas
Objetivo de Calidad asociado.:	Mejorar la eficiencia, eficacia y efectividad de los procesos del MinTIC / Mejorar los niveles de satisfacción de los servicios internos
Macro proceso:	Gestión de Recursos
Proceso	Gestión de Tecnologías de Información

Datos del Indicador			
Nombre del Indicador.:	Nivel de de implementación de los controles para los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Objetivo del Indicador.:	Medir el nivel de implementación de los controles para los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.
Tipo de Indicador.:	Eficacia	Frecuencia recolección de la info	Mensual
Responsable del análisis.:	Profesional encargado de coordinar el tema de Seguridad Digital	Frecuencia del análisis de la info	Trimestral
Fuentes(s) de la Información.:	Informe de seguimiento al desarrollo y mantenimiento de sistemas de información / Formatos de acuerdos de desarrollo y de requerimientos acordados	Formula (índice).:	Porcentaje de controles implementados = (#controles implementados / #controles definidos) *100

Metas:		
Rango		Calificación
Desde	Hasta	
85%	100%	Alto
60%	84%	Medio
0%	59%	Bajo

Variables	
1	Número de controles implementados
2	Número de definidos (aprobados)

Variable	Periodo 1	Periodo 2	Periodo 3	Periodo 4
1	0	0	0	0
2	0	0	0	0
Resultado	-	-	-	-



Análisis escrito del Periodo
PRIMER TRIMESTRE.
SEGUNDO TRIMESTRE
TERCER TRIMESTRE
CUARTO TRIMESTRE