CGII
Centro de Gestión de
Incidentes Informáticos

AGETIC
agencia de gobierno electrónico y
tecnologías de información y comunicación

ESTADO PLURINACIONAL DE BOLIVIA
MINISTERIO DE LA
PRESIDENCIA

PATRICIA LOPEZ

Responsable de Auditoría Informática

Centro de Gestión de Incidentes Informáticos – CGII

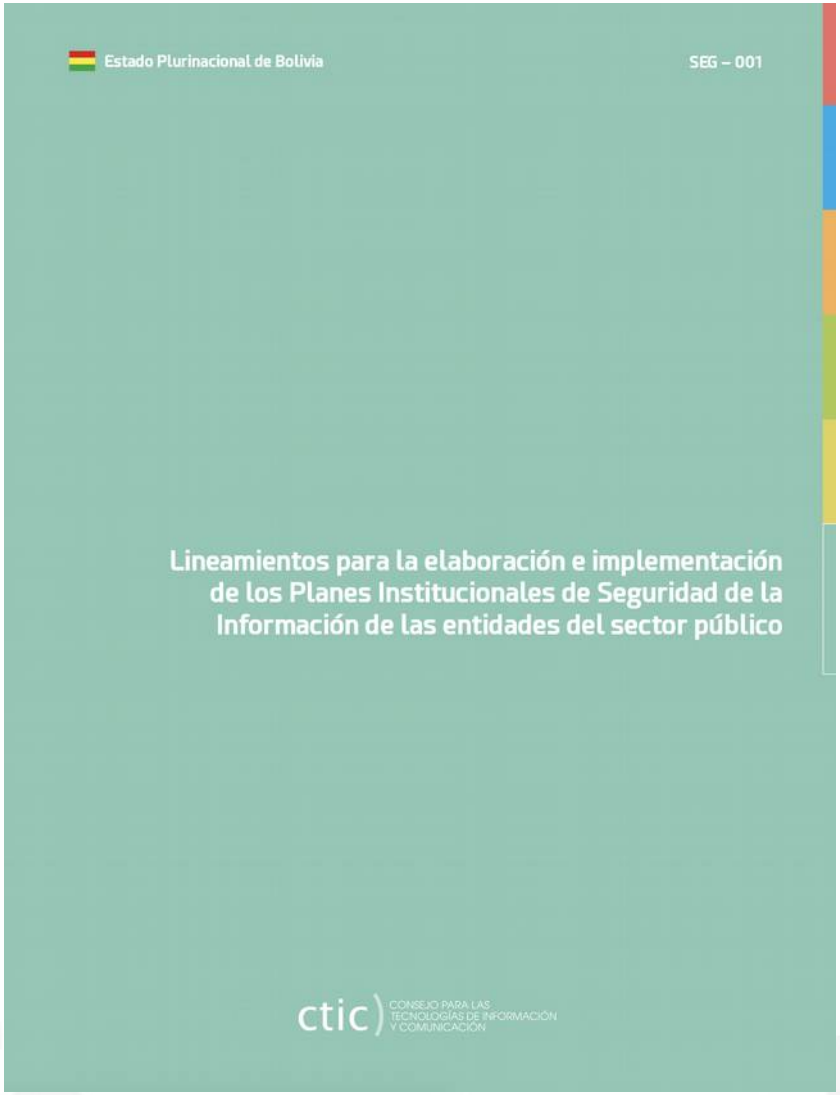
plopez@agetic.gob.bo

Algunas Definiciones

- **Seguridad de la Información**. La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.
- **Seguridad Informática.** Es el conjunto de normas, procedimientos y herramientas, las que se enfocan en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

- **Política de Seguridad de la Información (PSI).** Acciones o directrices que establecen la postura institucional en relación a la seguridad de la información, incluidas dentro del Plan Institucional de Seguridad de la Información.
- **Comité de Seguridad de la Información (CSI).** Equipo de trabajo conformado para gestionar, promover e impulsar iniciativas en seguridad de la información.
- **Responsable de Seguridad de la Información (RSI)**. Servidor publico responsable de gestionar, planificar, desarrollar e implementar el Plan Institucional de Seguridad de la Información.

Plan Institucional de Seguridad de la Información - PISI



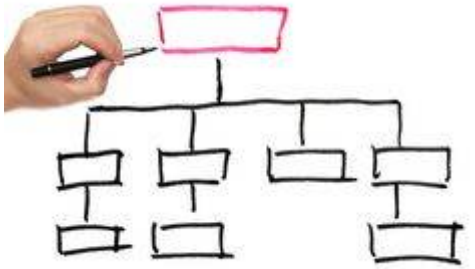
AGETIC/RA/0051/2017
19 de septiembre de 2017

OBJETIVO

Establecer los lineamientos para que las entidades del sector público del Estado Plurinacional de Bolivia puedan elaborar e implementar sus Planes Institucionales de Seguridad de la Información, en concordancia con la normativa vigente..

Plan Institucional de Seguridad de la Información

PROCESO DE ELABORACIÓN DEL PISI			
Etapa	**Objetivo**	**Actividades**	**Responsables**
Inicial	Organización Interna	Designación del Responsable de Seguridad de la Información Conformación del Comité de Seguridad de la Información	Máxima Autoridad Ejecutiva
Desarrollo	Estructura y contenido del Plan Institucional de Seguridad de la Información - PISI	Introducción, Objetivos, Alcances Declaración Institucional Metodología de gestión de riesgos Política de Seguridad de la Información Cronograma de implementación	Responsable de Seguridad de la Información
	Aprobación del PISI	Revisión y aprobación del PISI	Comité de Seguridad de la Información Máxima Autoridad Ejecutiva



Plan Institucional de Seguridad de la Información

PROCESO DE IMPLEMENTACIÓN DEL PISI			
Etapa	**Objetivo**	**Actividades**	**Responsables**
Implementación	Implementar el PISI	Aplicación de controles Capacitación e inducción Evaluación y mejora contínua Gestión de incidentes	Responsable de Seguridad de la Información Comité de Seguridad de la Información

Definición de Alcances del PISI

La entidad o institución pública definirá, dentro de su PISI, los alcances relacionados a proyectos, procesos y operaciones considerados prioritarios para cumplir con la misión, visión y objetivos estratégicos de la entidad

Gestión de Riesgos

Esta guía toma como referencia la Metodología de Análisis y Gestión de Riesgos MAGERIT. Sin embargo, la entidad o institución pública es libre de elegir el método o metodología que considere adecuada para realizar la gestión de riesgos siempre y cuando esta se encuentre bajo algún estándar nacional o internacional.

a) Identificación, clasificación y valoración de activos de información

b) Evaluación del riesgo

c) Tratamiento del riesgo

d) Controles implementados y por implementar

Identificación, Clasificación y Valoración de Activos de Información

- **Identificación**

El Responsable de Seguridad de la Información debe orientar la correcta identificación de los mismos conjuntamente con los responsables o dueños de los procesos institucionales.

Se debe identificar a los responsables y custodios de la información asociada al activo; esto es importante porque a través de la identificación se realizará una mejor valoración para resguardar la información.

Los custodios podrían ser los mismos servidores públicos o en otros casos una persona ajena a la entidad o institución

Identificación, Clasificación y Valoración de Activos de Información

- **Valoración**

Las características o atributos se utilizan para valorar las consecuencias de la materialización de una amenaza.

La valoración la debe dar el responsable del activo de información. Estas pueden ser en base a percepción, eventos anteriores relacionados a las propiedades de la información y otros.

Escala de Valoración	
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

Identificación, Clasificación y Valoración de Activos de Información

- **Valoración**

Disponibilidad

Un activo tiene gran valor, desde el punto de vista de disponibilidad, si es que una amenaza afectase su disponibilidad con consecuencias graves para el normal desarrollo de las actividades. Por el contrario, un activo carece de un valor apreciable cuando puede no estar disponible por largos periodos de tiempo sin afectar o causar daño a las actividades de la entidad o institución pública.

Integridad

Una valoración alta de esta propiedad se da por el grado de afectación (daño grave) causado por la alteración voluntaria o no intencionada de los datos. Por el contrario, una valoración menor se da cuando su modificación no supone preocupación alguna.

Confidencialidad

La valoración de esta característica está en función del grado de afectación que ocasionaría la revelación o divulgación de información a personas no autorizadas.

Disponibilidad	¿Qué importancia tendría que el activo no estuviera disponible?
Integridad	¿Qué importancia tendría que la información asociada al activo fuera modificada sin control?
Confidencialidad	¿Qué importancia tendría que la información asociada al activo fuera conocida por personas no autorizadas?

Identificación, Clasificación y Valoración de Activos de Información

- Matriz de Inventario y Valoración

	A	B	C	D	E	F	G	H	I	K	M	P	Q	R
1		INSTITUCIÓN:												
2		FECHA ELABORACIÓN:												
3		FECHA APROBACIÓN:												
4														
5														
6		INVENTARIO DE ACTIVOS IDENTIFICADOS							VALORACIÓN DE ACTIVOS			VALORACION FINAL	GESTIÓN	
7		#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad	Integridad	Confidencialidad		Fecha de Ingreso	Fecha de Salida
8															
9															
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															
24															
25															
26															
27		Elaborado por:				Aprobado por:									
28		Firma:				Firma:									
29		Cargo				Cargo:									
30															

Identificación, Clasificación y Valoración de Activos de Información

- **Revisión y Actualización**

El inventario puede ser revisado o validado en cualquier momento a solicitud del responsable de seguridad de la información.

- **Reserva**

El inventario de activos de información debe ser un documento de carácter no público con medidas de restricción para evitar su modificación.

El Responsable de Seguridad de la Información debería tener acceso para modificar el inventario, además de ser el responsable de resguardarlo.

Evaluación del Riesgo

- Identificación

  La identificación de amenazas y vulnerabilidades sobre activos de información es importante para determinar cuáles tienden a degradar las propiedades de Disponibilidad, Integridad y Confidencialidad de la información.
- Una vulnerabilidad es toda aquella debilidad que presenta el activo de información, dada comúnmente por la inexistencia o ineficacia de un control.
- Una amenaza es todo elemento que haciendo uso o aprovechando una vulnerabilidad, atenta o puede atentar contra la seguridad de un activo de información. Las amenazas surgen a partir de la existencia de vulnerabilidades, independientemente de que se comprometa o no la seguridad de un sistema.

Evaluación del Riesgo

- Análisis y Valoración

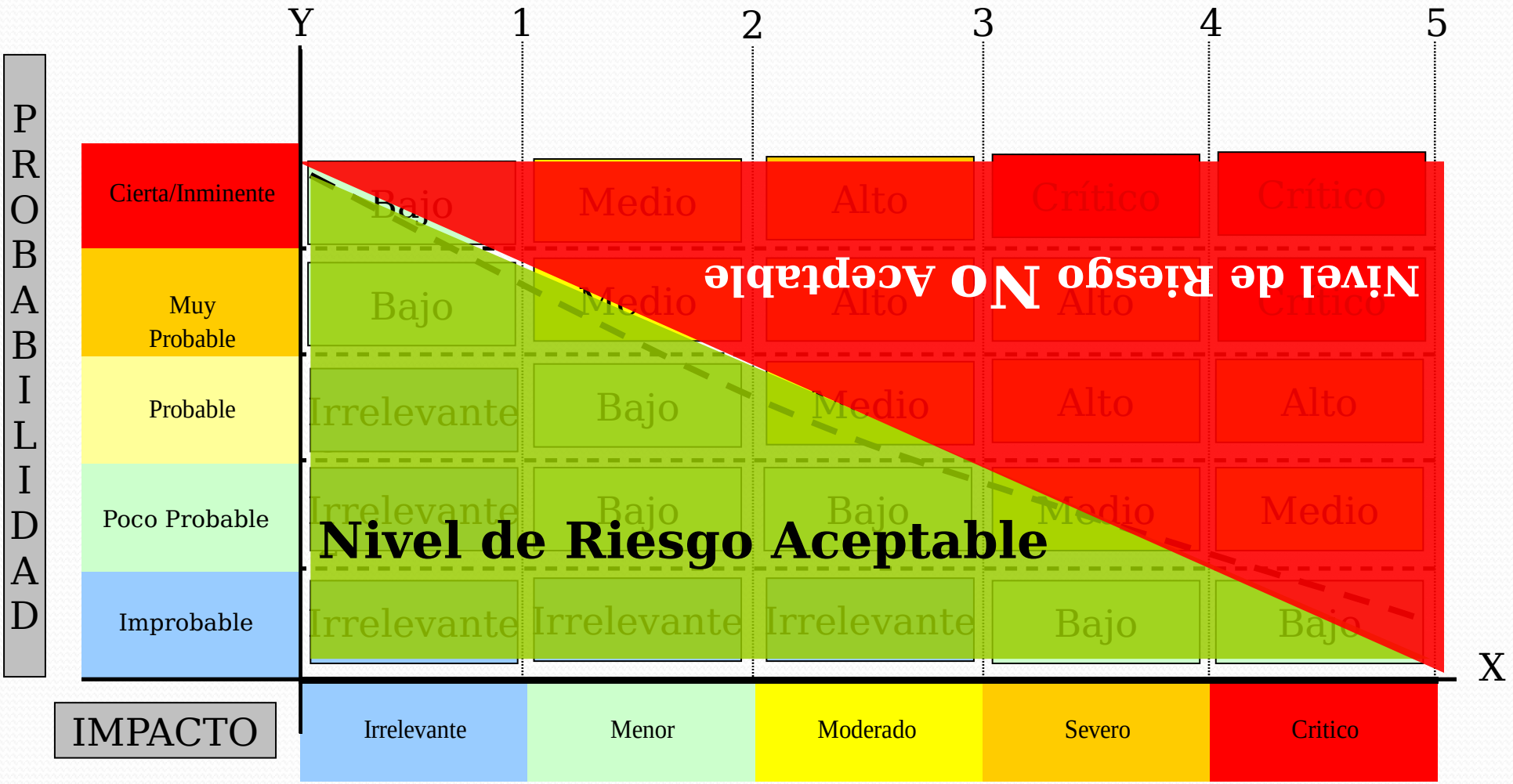
  La probabilidad de que ocurra el incidente, es decir, que la amenaza explote la vulnerabilidad.

  La magnitud del impacto que el evento produce sobre el activo.

- El cómputo de la probabilidad de ocurrencia del evento adverso suele basarse en los valores históricos de frecuencia con la que ocurre (o podría ocurrir) un evento (en un periodo determinado de tiempo, por ejemplo: anual, semestral. En caso de no contar con referencias históricas, se debe tomar la percepción que da el responsable del activo.

ESCALAS	
Probabilidad	**Impacto**
Cierta/Inminente	Crítico
Muy Probable	Severo
Probable	Moderado
Poco Probable	Menor
Improbable	Irrelevante

Riesgo = Probabilidad vs. Impacto (+ Percepción)



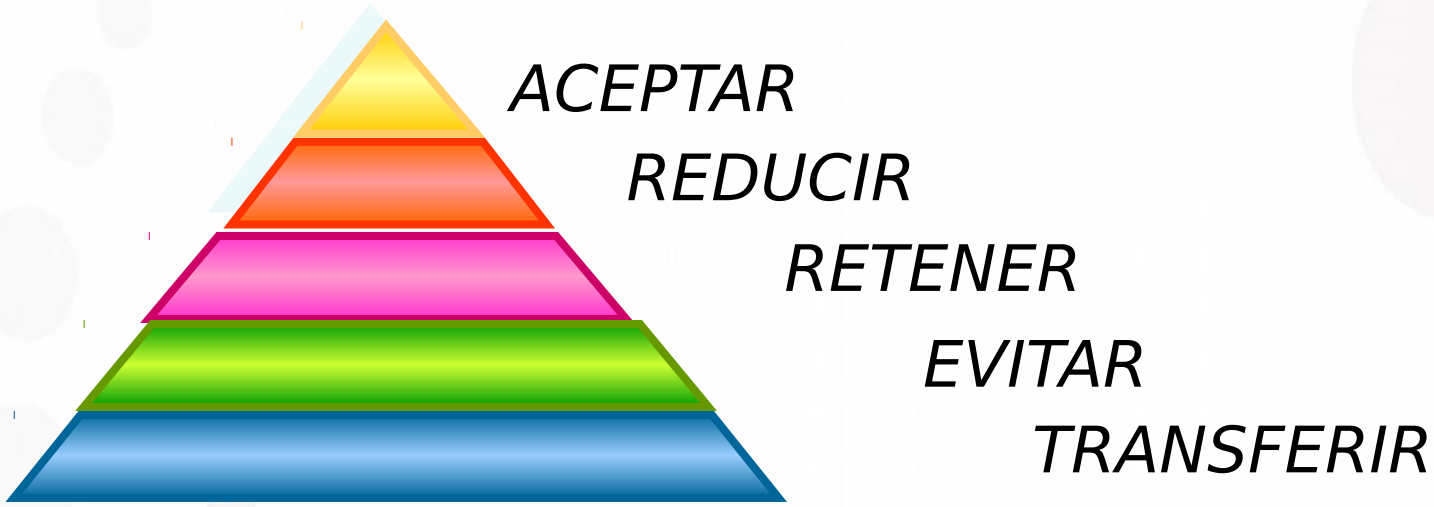
Evaluación del Riesgo

- Matriz de Valoración del Riesgo.

	A	B	C	D	E	F	G	H	I	K	M
1		INSTITUCIÓN:									
2		FECHA ELABORACIÓN:									
3		FECHA APROBACIÓN:									
4											
5											
6		VALORACIÓN DE RIESGOS							DEGRADACIÓN		
7		#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo	Disponibilidad	Integridad	Confidencialidad
8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												
21												
22												
23												
24												
25												
26												
27		Elaborado por:				Aprobado por:						
28		Firma:				Firma:						
29		Cargo				Cargo:						
30												

Tratamiento del Riesgo

- Controles del Anexo A



Controles de Seguridad de la Información

- Recursos Humanos
- Activos de Información
- Control de Accesos
- Criptografía
- Seguridad Física
- Seguridad de las Operaciones
- Comunicaciones
- Desarrollo de sistemas
- Gestión de Incidentes
- Contingencias Tecnológicas
- Cumplimiento

Controles Implementados y por Implementar

- Consecuencia de la decisión de las opciones de tratamiento de riesgos y los controles de seguridad que se decidan implementar.
-

Control de Seguridad de la Información	Inclusión del Control	Control Existente	Justificación Inclusión	Justificación Exclusión	Documentación
Acuerdo de confidencialidad	Sí	No	Control mínimo requerido. Resultados de la evaluación de riesgos.		
Control de accesos	Sí	Sí	Control mínimo requerido. Resultados de la evaluación de riesgos.		Política de control de accesos. Procedimientos de altas y bajas de
Uso de medios extraíbles	No	No		Aceptación del riesgo.	

Política de Seguridad de la Información

- Posturas respecto a :
- Protección de la información institucional ante amenazas que se originan del recurso humano.
- Uso y protección de activos de información.
- Control de accesos a recursos de red, información, sistemas y aplicaciones.
- Protección de información transmitida a través de redes de comunicaciones.
- Protección de áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y crítica.
- Seguridad en el ciclo de vida de los sistemas y/o software que se desarrolle y/o adquiera.
- Continuidad de las operaciones y procesos mediante la gestión de incidentes en seguridad de la información.
- Protección de información física documental.
- Otros.

Política de Seguridad de la Información

Introducción.

- **Términos y Definiciones**
- **Objetivo General**

El objetivo general se debe enfocar en el resguardo de los activos de información de la institución respecto a la confidencialidad, integridad y disponibilidad de la información asociada.

Política de Seguridad de la Información

- **Objetivos Específicos**

  Dentro de los objetivos se pueden identificar temas relacionados a la gestión de activos de información, gestión de riesgos, gestión de incidentes, capacitación y sensibilización de los documentos que regulan la seguridad.

- **Alcance**

  Define la trascendencia y el ámbito de aplicación de la PSI al interior de la entidad o institución

Política de Seguridad de la Información

- **Roles y Responsabilidades**
- **Desarrollo (políticas de seguridad**)

  Explicar la postura institucional respecto al PISI, los controles mínimos de seguridad contemplados, y otros requerimientos de seguridad de la información de acuerdo a los resultados del análisis de riesgo realizado

  - Ámbito de seguridad:
  - Descripción:

Política de Seguridad de la Información

- **Difusión**
- **Cumplimiento**
- **Sanciones**
- **Histórico de Cambios**

Indicadores y Métricas

- Específico.
- Medible cualitativa o cuantitativamente y/o con indicadores y atributos.
- Alcanzable.
- Relevante.
- Repetible en periodos de tiempo.

Ejemplo: Red de Datos Control Seguridad de las comunicaciones

INDICADOR: Caídas por Mes

TIPO DE INDICADOR: Disponibilidad.

Control de Seguridad	Indicador y métrica (cualitativa, cuantitativa, indicador, atributo)	Alcanzable	Relevancia	Periodo de tiempo

Cronograma de Implementación

- Fechas.
- Controles a implementarse.
- Roles y responsabilidades.
- Actividades relacionadas a capacitación, seguimiento, revisión y aplicación de controles.

Aprobación del PISI

- Revisado por el CSI.
- Aprobado por la MAE
- Plan flexible a actualizaciones

  La disposición transitoria segunda del Decreto Supremo 2514 de 9 de septiembre de 2015, establece que: “las entidades del nivel central del Estado deberán presentar a la AGETIC, en un plazo no mayor a un (1) año desde la aprobación de las políticas de seguridad de la información por la AGETIC, su Plan Institucional de Seguridad de la Información”.

CGII
Centro de Gestión de
Incidentes Informáticos

GRACIAS

Patricia Lopez. plopez@agetic.gob.bo

Humberto Bellido hbellido@agetic.gob.bo

AGETIC

agencia de gobierno electrónico y tecnologías de información y comunicación

ageticbolivia@diasp.org

@AgeticBolivia
facebook.com/ageticbolivia

mastodon.xyz/@AgeticBolivia

@AgeticBolivia
instagram.com/ageticbolivia

+591**75235634**

@AgeticBolivia
twitter.com/AgeticBolivia

@AgeticBolivia
www.t.me/AgeticBolivia

Agetic Bolivia
youtube.com/AgeticBolivia

contacto@agetic.gob.bo

(+591 -2) 2120498

www.agetic.gob.bo

blog.agetic.gob.bo