SITia

Sistema Integrado de Teleprotección con Inteligencia Artificial

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Subsecretaría del Interior
Gobierno de Chile

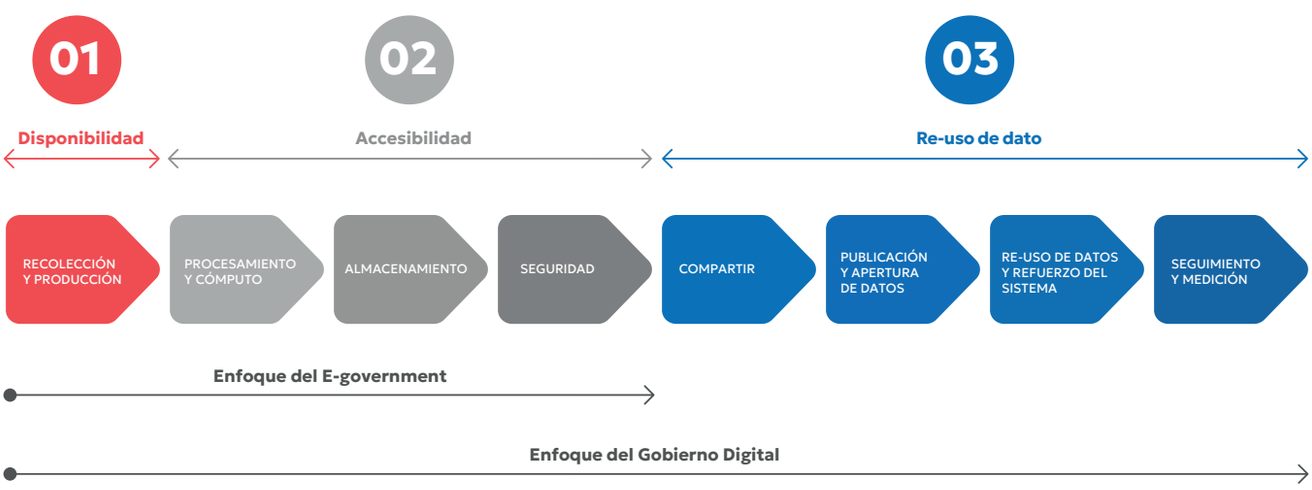
Subsecretaría de Prevención del Delito
Gobierno de Chile

CICLO DE VIDA DEL DATO
SITIA- PATENTE

El adecuado entendimiento del ciclo de vida del dato es esencial para llevar a cabo una gestión eficiente de la información dentro de una organización. Esta comprensión no solo promueve una mejora en la calidad de los datos, sino que también facilita el cumplimiento de regulaciones, fortalece la seguridad de la información, optimiza la operatividad de los procesos y respalda la toma de decisiones fundamentadas.

En este informe, se abordará específicamente el ciclo de vida de datos relacionado con la solución SITIA- PATENTE, parte integral del proyecto piloto conocido como Sistema de Teleprotección con IA (SITIA). Mediante este análisis detallado, se buscará identificar los diferentes momentos y procesos que atraviesa la información dentro de la solución Vtracker, con el propósito de comprender cómo se capturan, almacenan, procesan y utilizan los datos en este contexto particular.

Para el respectivo análisis, utilizaremos el siguiente diagrama de ciclo de vida del dato elaborado por la La Organización para la Cooperación y el Desarrollo Económicos (OCDE).



SITia

Sistema Integrado de Teleprotección con Inteligencia Artificial

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Subsecretaría del Interior
Gobierno de Chile

Subsecretaría de Prevención del Delito
Gobierno de Chile

01 Disponibilidad

Recolección e ingesta de datos

Herramientas de recolección de datos o ingesta de datos

Uso de pipelines: Un pipeline de datos es un sistema esencial en la gestión eficiente de información, actuando como una tubería que dirige y transforma datos desde su origen hasta su destino final de manera automatizada y eficaz. En nuestro contexto, donde recibimos datos de entidades colaboradoras, nuestro enfoque no radica en recolectarlos, sino en ingestarlos a través de servicios web, específicamente utilizando protocolos abiertos como REST para la comunicación y autorización.

Además de estas fuentes externas, contamos con el Sistema Único de Encargos de Vehículos (SUEV), el cual nos proporciona eventos relacionados con los encargos realizados. Estos eventos también se reciben a través de servicios web REST, garantizando una comunicación fluida y segura.

EL PIPELINE DE DATOS CONSTA DE LAS SIGUIENTES ETAPAS:

Adquisición de datos: En esta etapa, los datos se recopilan desde diversas fuentes, como bases de datos, archivos de registro, aplicaciones web, dispositivos IoT (Internet de las cosas), entre otros.

Procesamiento de datos: Los datos adquiridos pueden estar en formatos diferentes y pueden requerir limpieza, filtrado, transformación o enriquecimiento para ser útiles para su análisis posterior. Esta etapa implica procesos como la normalización de datos, la deduplicación y la detección de errores.

Almacenamiento de datos: Después de ser procesados, los datos se almacenan en un repositorio adecuado para su posterior acceso y análisis. Esto puede ser en una base de datos relacional, un almacén de datos, un sistema de archivos distribuido o incluso en la nube.

Análisis de datos: Una vez almacenados, los datos están listos para ser analizados para extraer información significativa. Esto puede implicar la ejecución de consultas SQL, la aplicación de algoritmos de aprendizaje automático o la generación de informes y visualizaciones.

Entrega de datos: Finalmente, los resultados del análisis se entregan a los usuarios finales a través de diferentes canales, como aplicaciones web, paneles de control, informes automatizados o incluso integraciones con otras aplicaciones.

SITia

Sistema Integrado de Teleprotección con Inteligencia Artificial

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Subsecretaría del Interior
Gobierno de Chile

Subsecretaría de Prevención del Delito
Gobierno de Chile

01 Disponibilidad

Fuentes de datos (Internas y externas)

Fuentes de datos externas

El objetivo de este apartado es presentar los principales hallazgos derivados del análisis de las bases de datos relacionadas con las alertas generadas por patentes con órdenes de encargo vigentes, y que han sido detectadas por pórticos o cámaras lectoras de placas patente.

El propósito del análisis es proporcionar pautas para mejorar el modelo de datos actual, con el fin de optimizar la utilización de la información disponible. Para llevar a cabo este análisis, se utilizaron las siguientes fuentes de información:

Base de datos que contiene información sobre las patentes con órdenes de encargo vigentes.

Base de datos que recopila datos sobre los pórticos o cámaras lectoras de placas patente.

Base de datos de coincidencias entre patentes con órdenes de encargo vigentes y pórticos o cámaras lectoras de placas patente.

BASE DE DATOS DE PATENTES QUE POSEEN ORDEN DE ENCARGO VIGENTE.

Descripción: base de datos que posee las patentes que presentan algún tipo de orden de encargo vigente, ya sea por robo, por haber participado en algún delito o alguna orden judicial.

Número de registros: 229.148 relacionadas al registro histórico.

Descripción de las variables e información general:
La siguiente tabla presenta la información general vinculada a la base de datos, exponiendo el nombre de las variables, tipo de dato, número de casos nulos y número de casos inválidos.

SITia

Sistema Integrado de Teleprotección con Inteligencia Artificial

Ministerio del Interior y Seguridad Pública Gobierno de Chile | Subsecretaría del Interior Gobierno de Chile | Subsecretaría de Prevención del Delito Gobierno de Chile

01 Disponibilidad

Tabla 1. Resumen general de las variables.

Variable	Descripción	Tipo dato	Estructurado	Nulos		Inválidos	
				Frecu.	%	Frecu.	%
Id	Identificador del registro	numérico		0	0,00	0	0,00
Patente	Patente vehicular	texto	No	32	0,00	23	0,00
Marca	Marca del vehículo vinculado a la patente	texto	No	15.875	6,90	0	0,00
Modelo	Modelo del vehículo vinculado a la patente	texto	No	4.357	1,90	81	0,00
Color	Color del vehículo vinculado a la patente	texto	No	15.440	6,70	8	0,00
Estado	Estado de la patente, sí es vigente corresponde a su búsqueda	texto	Si	1.120	0,50	0	0,00
Tipo_encargo	Tipo de encargo vinculada a la patente	texto	Si	3.655	1,60	0	0,00
Delito	Clasificación del delito vinculada a la patente que posea encargo	texto	Si	62.834	27,40	22	0,00
Fecha	Fecha de creación del registro	fecha		1.120	0,50	0	0,00
Created_at	Fecha y hora de creación del registro	fecha		0	0,00	0	0,00
Updated_at	Fecha y hora de actualización del registro	fecha		0	0,00	0	0,00

* Por información nula se hace referencia a registros que no poseen información, es decir, valores en blanco.
*Por información inválida se hace referencia a registros que se encuentran fuera de los valores referentes a cada variable.
*El porcentaje expuesto se realiza en base al total de registros existentes.
*Los porcentajes que posean casos en frecuencia y valor 0 en % se debe a que la información se encuentra delimitada a dos decimales.

01 Disponibilidad

BASE DE DATOS PÓRTICOS.

Descripción: base de datos que posee el listado individualizado hasta el nivel de pista de los pórticos financiados por la Subsecretaría de Prevención del Delito mediante el programa Sistema de Televigilancia.

Consideraciones de importancia: dentro de la base de datos de match de patentes que presentan algún tipo de encargo, se verifica la existencia de otros pórticos diferentes en la base de datos a analizar. Dentro de estos otros pórticos, las fuentes de información que han sido detectadas son:

Tabla 2. Otros suministradores de información

Fuente de información	Número de lectores
Mall Plaza	78
Parque Arauco	43
Municipalidad de Ñuñoa	28
Municipalidad de Puente Alto	10
Municipalidad de Vitacura	17
Total	176

Cabe hacer presente que estos pórticos han sido excluidos del análisis debido a que no poseen una estandarización de la información, a diferencia de los financiados por la SPD. En recomendaciones se precisará dichos antecedentes.

Número de registros: 100 pórticos individualizados hasta nivel pista con coordenadas geográficas.

Descripción de las variables e información general:
La siguiente tabla presenta la información general vinculada a la base de datos, exponiendo el nombre de las variables, tipo de dato, número de casos nulos y número de casos inválidos.

01 Disponibilidad

Tabla 3. Resumen general de las variables.

Variable	Descripción	Tipo dato	Estructurado	Nulos		Inválidos	
				Frecu.	%	Frecu.	%
id	identificador del registro en la base de datos	autonumérico	No	0	0	0	0
id_portico	identificador único de pórtico	numérico	No	0	0	0	0
portico_code	identificador de pórtico	texto	No	0	0	0	0
portico_code_des	identificador de pórtico desagregado	texto	No	0	0	0	0
portico_desc	descripción general de pórtico	texto	No	0	0	0	0
descripcion	descripción de ubicación de pórtico	texto	No	0	0	0	0
longitud	coordenada geográfica de longitud vinculada al pórtico desagregado	decimal	No	0	0	0	0
latitud	coordenada geográfica de latitud vinculada al pórtico desagregado	decimal	No	0	0	0	0
geometry	geometría geográfica de posición de pórtico	texto	No	0	0	0	0
pista	pista de ubicación de la coordenada geográfica desagregada, relativa a la ubicación de cámara posicionada en pórtico	texto	Si	0	0	0	0
sentido	sentido de dirección de la vía relacionada a la ubicación de la coordenada geográfica desagregada, relativa a la ubicación de cámara posicionada en pórtico	texto	Si	0	0	0	0
comuna	comuna relacionada a la ubicación del pórtico	texto	Si	0	0	0	0
provincia	provincia relacionada a la ubicación del pórtico	texto	Si	0	0	0	0
region	región relacionada a la ubicación del pórtico	texto	Si	0	0	0	0
cod_ine	código único identificador del tipo de vía del Maestro de Calles del Instituto Nacional de Estadísticas	numérico	No	0	0	0	0
tipo_via	tipo de vía del Maestro de Calles del Instituto Nacional de Estadísticas	texto	Si	0	0	0	0
nombre_via	nombre del tipo de vía del Maestro de Calles del Instituto Nacional de Estadísticas	texto	Si	0	0	0	0

* Por información nula se hace referencia a registros que no poseen información, es decir, valores en blanco.
*Por información inválida se hace referencia a registros que se encuentran fuera de los valores referentes a cada variable.
*El porcentaje expuesto se realiza en base al total de registros existentes.
*Los porcentajes que posean casos en frecuencia y valor 0 en % se debe a que la información se encuentra delimitada a dos decimales.

01 Disponibilidad

BASE DE DATOS MATCH DE PATENTES.

Descripción: base de datos que posee el resultado final del match entre la base de datos con patentes que posean algún tipo de orden vigente y la base de datos de ubicación de pórticos. El dato resultante es la localización específica de donde fue detectada la patente de interés.

Número de registros: 25.592 detecciones.

Descripción de las variables e información general:
La siguiente tabla presenta la información general vinculada a la base de datos, exponiendo el nombre de las variables, tipo de dato, número de casos nulos y número de casos inválidos.

Tabla 4. Resumen general de las variables.

Variable	Descripción	Tipo dato	Estructurado	Nulos		Inválidos	
				Frecu.	%	Frecu.	%
id	identificador del registro en la base de datos	Autonumérico		0	0	0	0
ip	Se desconoce información sobre la variable	entero	Si	0	0	0	0
id_convenio	corresponde al nombre de la institución o programa con el que se tienen el convenio de trasmisión de datos desde cámara lectora de patente	texto	Si	0	0	0	0
id_portal	información sobre el nombre del pórtico, comuna, ubicación, sentido y pista.	texto	No	0	0	4.502	17,59
acceso	Se desconoce información sobre la variable	texto	No	25.592	100	0	0
patente	letra y número de la patente que presenta algún tipo de orden	texto	No	0	0	71	0,28
delito	información sobre el tipo de orden vinculada a la patente	texto	Si	4.951	19,35		
estado	Se desconoce información sobre la variable	texto	Si	0	0	0	0
fecha	fecha de detección de la patente en alguna de las cámaras lectoras	fecha	Si	0	0	0	0
hora	hora de detección de la patente en alguna de las cámaras lectoras	hora	Si	0	0	0	0
created_at	fecha y hora de creación de la alerta vinculada a la patente por detección en algún pórtico	fecha-hora	Si	0	0	0	0
updated_at	fecha y hora de creación de la alerta vinculada a la patente por detección en algún pórtico	fecha-hora	Si	0	0	0	0

* Por información nula se hace referencia a registros que no poseen información, es decir, valores en blanco.
*Por información inválida se hace referencia a registros que se encuentran fuera de los valores referentes a cada variable.
*El porcentaje expuesto se realiza en base al total de registros existentes.
*Los porcentajes que posean casos en frecuencia y valor 0 en % se debe a que la información se encuentra delimitada a dos decimales.

01 Disponibilidad

Cadena de licitud de tratamiento de datos

(Revisión fecha 01 de mayo de 2024)

TIPO DE DATO	FUENTE DEL DATO	FUNDAMENTO DE LA LICITUD DEL TRATAMIENTO POR LA FUENTE	FUNDAMENTO DE LICITUD DE TRATAMIENTO POR SITIA (se requiere ley y/o convenio, si se trata de un dato personal)
Patentes de vehículos con encargo de búsqueda	Carabineros de Chile (Servicio de Encargo y Búsqueda de Vehículos - SEBV)	Artículo 39, DFL 1 Fija texto refundido, coordinado y sistematizado de la Ley de Tránsito: El Servicio de Registro Civil e Identificación llevará un Registro de Vehículos Motorizados en la base de datos central de su sistema electrónico. (…) Asimismo, deberá anotarse la denuncia por la apropiación de un vehículo motorizado, especificando si ha sido objeto de robo o hurto, a requerimiento de la autoridad policial, judicial o del Ministerio Público. (…) La información sobre las denuncias incorporadas al Registro de Vehículos Motorizados se encontrará permanentemente a disposición del público, en las páginas web institucionales de Carabineros de Chile, de la Policía de Investigaciones de Chile y del Ministerio Público, especificando, entre otros datos, la placa patente única, el número de motor, número de chasis, color, año y las circunstancias en que fue apropiado. Artículo 2° bis, Ley 18961, Ley Orgánica Constitucional de Carabineros: Carabineros de Chile, como parte de la Administración del Estado, está al servicio de la comunidad y sus acciones se orientarán a la prevención de delitos, al control y restablecimiento del orden público y a la seguridad pública, así como a otras que le asignen las leyes.	Cuando exista, la actividad de la SPD puede fundarse en el art. 1 de la ley 21.332: “Artículo 1.- Establécese un Sistema Táctico de Operación Policial, en adelante el "Sistema", que será administrado por Carabineros de Chile, cuyo objetivo será transparentar y optimizar la gestión táctica policial orientada a la prevención de delitos, a través de un conjunto de acciones y estrategias, entre las que se comprenden el análisis de tendencias, volúmenes y cambios del comportamiento delictual, así como el seguimiento de las acciones que se implementen en el orden preventivo y de control del fenómeno delictual. Forman parte del Sistema, en calidad de participantes, el Ministerio del Interior y Seguridad Pública, el Ministerio Público, Carabineros de Chile y las municipalidades.”
Patentes de vehículos	Arriendo por la SPD de 35 pórticos lectores de placa patente a la empresa SISTESA	El Decreto Exento N°2409 de 17 de diciembre de 2019 aprueba el contrato de arriendo celebrado entre la Subsecretaría de Prevención del Delitos y Sistemas de Seguridad y Tecnología SpA, encuadrándolo en el “Plan Calle Segura”, iniciativa “Auto Seguro”. La orden de compra 654478-36-SE22 indica que toda la gestión que se realice con las lecturas LPR obtenidas en los pórticos, será obligatorio que el 100% de estas lecturas sea reenviado, en tiempo real, a la base de datos del SEBV de Carabineros. Se declara que el objetivo es a) Detectar vehículos con placa patente única (PPU) con encargo de búsqueda por robo; b) Activar y/o alertar al SEBV sobre vehículos detectados; c) Proveer de antecedentes y medios de prueba al Ministerio Público, con el fin de contribuir a la investigación de hechos delictivos; y d) Disuadir la comisión de estos delitos, en la medida que se demuestra la utilidad de estos pórticos, evitando así también, la realización de otros hechos delictuales.	Cuando exista, la actividad de la SPD puede fundarse en el art. 1 de la ley 21.332: “Artículo 1.- Establécese un Sistema Táctico de Operación Policial, en adelante el "Sistema", que será administrado por Carabineros de Chile, cuyo objetivo será transparentar y optimizar la gestión táctica policial orientada a la prevención de delitos, a través de un conjunto de acciones y estrategias, entre las que se comprenden el análisis de tendencias, volúmenes y cambios del comportamiento delictual, así como el seguimiento de las acciones que se implementen en el orden preventivo y de control del fenómeno delictual. Forman parte del Sistema, en calidad de participantes, el Ministerio del Interior y Seguridad Pública, el Ministerio Público, Carabineros de Chile y las municipalidades.”
Patentes de vehículos con encargo de búsqueda	Supermercados, establecimientos y centros comerciales	DFL 3, que fija texto refundido, coordinado y sistematizado de la ley N°19.496, que establece normas sobre protección de los derechos de los consumidores. “Artículo 3°.- Son derechos y deberes básicos del consumidor: (…) d) La seguridad en el consumo de bienes o servicios, la protección de la salud y el medio ambiente y el deber de evitar los riesgos que puedan afectarles” Artículo 15.- Los sistemas de seguridad y vigilancia que, en conformidad a las leyes que los regulan, mantengan los establecimientos comerciales están especialmente obligados a respetar la dignidad y derechos de las personas. Artículo 15 A.- Los proveedores que ofrezcan servicios de estacionamiento de acceso al público general, cualquiera sea el medio de pago utilizado, se regirán por las siguientes reglas: (…)5. Si, con ocasión del servicio y como consecuencia de la falta de medidas de seguridad adecuadas en la prestación de éste, se producen hurtos o robos de vehículos, o daño en éstos, el proveedor del servicio será civilmente responsable de los perjuicios causados al consumidor”.	La Subsecretaría de Prevención del Delito no tiene competencias para realizar tratamiento de datos personales en materia de seguridad pública, salvo que actúe como mandatario de un organismo con dichas competencias legales y, a la vez, tenga competencias propias para realizar operaciones de tratamiento. En este último aspecto, la SPD puede fundar su actividad en el art. 1 de la ley 21.332: “Artículo 1.- Establécese un Sistema Táctico de Operación Policial, en adelante el "Sistema", que será administrado por Carabineros de Chile, cuyo objetivo será transparentar y optimizar la gestión táctica policial orientada a la prevención de delitos, a través de un conjunto de acciones y estrategias, entre las que se comprenden el análisis de tendencias, volúmenes y cambios del comportamiento delictual, así como el seguimiento de las acciones que se implementen en el orden preventivo y de control del fenómeno delictual. Forman parte del Sistema, en calidad de participantes, el Ministerio del Interior y Seguridad Pública, el Ministerio Público, Carabineros de Chile y las municipalidades.”
Patentes de vehículos con encargo de búsqueda	Concesionarios de obras públicas	Las facultades para tratar datos arrancan tanto de los respectivos contratos de licitación como del Decreto Exento N°4110 del Ministerio del Interior y Seguridad Pública, de 23 de octubre de 2015, que “Aprueba convenio marco de cooperación ente el Ministerio del Interior y Seguridad Pública, el Ministerio de Obras Públicas, Carabineros de Chile, Policía de Investigaciones de Chile, COPSA A.G. y las sociedades concesionarias que se indican”, y cuya cláusula PRIMERA regula la transferencia de datos entre las concesionarias y Carabineros de Chile.	El convenio puede fundarse en el art. 1 de la ley 21.332: “Artículo 1.- Establécese un Sistema Táctico de Operación Policial, en adelante el "Sistema", que será administrado por Carabineros de Chile, cuyo objetivo será transparentar y optimizar la gestión táctica policial orientada a la prevención de delitos, a través de un conjunto de acciones y estrategias, entre las que se comprenden el análisis de tendencias, volúmenes y cambios del comportamiento delictual, así como el seguimiento de las acciones que se implementen en el orden preventivo y de control del fenómeno delictual. Forman parte del Sistema, en calidad de participantes, el Ministerio del Interior y Seguridad Pública, el Ministerio Público, Carabineros de Chile y las municipalidades.”

02 Accesibilidad

Procesamiento y Cómputo

Calidad de los datos

Establecer estándares de calidad de datos es fundamental para un sistema público de seguimiento de autos robados o de especial interés en Chile por varias razones clave:

1- Precisión en la Identificación: Los estándares de calidad de datos aseguran que la información sobre vehículos robados o de interés especial sea precisa y confiable. Esto es crucial para garantizar la identificación correcta de los vehículos y evitar confusiones que podrían resultar en la liberación de vehículos robados o en la retención indebida de vehículos legítimos.

2- Eficiencia en la Búsqueda y Recuperación: La calidad de los datos facilita la búsqueda y recuperación efectiva de vehículos robados. Datos precisos y bien estructurados permiten a las autoridades realizar búsquedas rápidas y precisas en el sistema, lo que aumenta las posibilidades de recuperar los vehículos perdidos y reducir el tiempo necesario para hacerlo.

3- Integración de Sistemas: Establecer estándares de calidad de datos facilita la integración de sistemas entre diferentes agencias gubernamentales y organizaciones encargadas de la seguridad pública. Esto garantiza que la información relevante se comparta de manera fluida y que los diferentes sistemas puedan trabajar juntos de manera efectiva para abordar el problema de los autos robados.

Por ello, se emplearán, de manera general y sin necesidad de certificación, dos estándares internacionales para garantizar la calidad de datos: la ISO 800-61 y la ISO 25000

ISO 800: establece un modelo de referencia de procesos de gestión de calidad de los datos. La principal característica es que, para alcanzar la mejora continua, el proceso de implementación debe ser ejecutado continuamente siguiendo el ciclo Plan-Do-Check-Act.

ISO 25000: permite a las empresas que desarrollan software conocer la calidad de sus productos y a las empresas que compran software, decidirse por una solución u otra en función de sus necesidades.

02 Accesibilidad

Interoperabilidad

Las siguientes etapas describen el proceso de interoperabilidad de la solución VTracker, diseñada para mejorar la seguridad y eficiencia en la detección y seguimiento de vehículos mediante una infraestructura avanzada de televigilancia:

Paso 1: Este proceso se inicia con el evento "Vehículo Detectado", el cual es generado por entidades colaboradoras equipadas con pórticos que cuentan con tecnología de reconocimiento de placas patentes.

Paso 2: Estos pórticos tienen la capacidad de capturar las placas de los vehículos en tránsito, y luego envían esta información de manera automática a VTracker.

Paso 3: Una vez que VTracker recibe los datos, procede a procesarlos para verificar si existen coincidencias con vehículos que están siendo buscados por robo u otras alertas.

Paso 4: Si se detecta una coincidencia, se genera automáticamente el evento "Vehículo con Encargo encontrado".

Paso 5: Este segundo evento activa una serie de procedimientos operativos, que incluyen el almacenamiento de la información relevante, la generación de alertas visuales y sonoras, y el envío de esta información crítica a otras aplicaciones e interesados, como fuerzas policiales y sistemas de gestión de tráfico.

Granularidad

Esquema de granularidad del dato.

Tabla 6. Resumen general de la granularidad del dato.

Dimensión patente							
Patente	Patente	Patente	Patente	Patente	Patente	Patente	Patente
	Marca	Marca	Marca	Marca	Marca	Marca	Marca
		Modelo	Modelo	Modelo	Modelo	Modelo	Modelo
			Color	Color	Color	Color	Color
				Estado	Estado	Estado	Estado
					Tipo de encargo	Tipo de encargo	Tipo de encargo
						Delito	Delito
							Creación del encargo

*Se excluyen todas aquellas variables que no aportan al enfoque de la dimensión.

02 Accesibilidad

Tabla 7. Resumen general de la granularidad del dato.

Dimensión match de patente				
patente	patente	patente	patente	patente
	pórtico	pórtico	pórtico	pórtico
		hora - fecha	hora - fecha	hora - fecha
			delito	delito
				administrador pórtico

Tabla 8. Resumen general de la granularidad del dato.

Dimensión cámara o pórtico lector de placa patente								
pórtico	pórtico	pórtico	pórtico	pórtico	pórtico	pórtico	pórtico	pórtico
	pista	pista	pista	pista	pista	pista	pista	pista
		sentido	sentido	sentido	sentido	sentido	sentido	sentido
			longitud - latitud	longitud - latitud	longitud - latitud	longitud - latitud	longitud - latitud	longitud - latitud
				tipo de vía	tipo de vía	tipo de vía	tipo de vía	tipo de vía
					nombre de la vía	nombre de la vía	nombre de la vía	nombre de la vía
						comuna	comuna	comuna
							provincia	provincia
								región

*Se excluyen todas aquellas variables que no aportan al enfoque de la dimensión.

02 Accesibilidad

Datos estructurados y no estructurados

Los datos estructurados son información organizada en un formato definido, facilitando su procesamiento automatizado. Las bases de datos específicas incluyen:

El desarrollo solo procesa datos estructurados*

Base de Datos de Patentes con Órdenes de Encargo Vigentes: Contiene detalles sobre patentes vinculadas a órdenes de encargo activas, como números de registro, fechas y estado de la orden.
Base de Datos de Pórticos o Cámaras Lectoras de Placas Patente: Almacena información sobre dispositivos de lectura de placas, como ubicación, identificadores y datos de placas patente detectadas. Base de Datos de Coincidencias entre Patentes con Órdenes de Encargo Vigentes y Pórticos o Cámaras
Lectoras de Placas Patente: Combina datos de las anteriores para identificar coincidencias entre patentes con órdenes activas y placas detectadas, registrando detalles como fechas, ubicaciones y otras información relevante.

SITia

Sistema Integrado de Teleprotección con Inteligencia Artificial

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Subsecretaría del Interior
Gobierno de Chile

Subsecretaría de Prevención del Delito
Gobierno de Chile

03 Re-uso de dato

Almacenamiento y seguridad

Objetivo

El objetivo de este apartado es establecer los cursos de acción necesarios para garantizar el resguardo efectivo del sistema de lectura de placas patentes de vehículos Vtracker entre Equipo SITIA y Carabineros. Esto se llevará a cabo en conformidad con los estándares de seguridad y confidencialidad aplicables, incluyendo el Decreto 83 y otras normativas relevantes. Además, se incorporarán prácticas de desarrollo seguro y metodologías ágiles para asegurar la integridad y seguridad del sistema a lo largo de su ciclo de vida.

Alcance

El alcance del proyecto abarcará la implementación de medidas de seguridad y controles conforme al Decreto Nr. 83 que aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos y las normas ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27034 e ISO 31000 en el sistema de alerta de placas patentes, alojado en servidores on-premise en las dependencias de Carabineros. Esto incluirá el establecimiento de controles de acceso, gestión de activos, seguridad física y del entorno, gestión de incidentes de seguridad de la información, así como evaluación y tratamiento continuo de riesgos. Además, se aplicarán prácticas de desarrollo seguro y metodologías ágiles para asegurar la integridad y seguridad del sistema a lo largo de su ciclo de vida.

Glosario

ISO/IEC 27001: Norma para establecer un Sistema de Gestión de Seguridad de la Información (SGSI).
ISO/IEC 27002: Norma con directrices para la gestión de la seguridad de la información en una organización.
ISO/IEC 27034: Norma para la gestión de la seguridad en el desarrollo de aplicaciones.
ISO 31000: Norma que establece principios y directrices para la gestión de riesgos.
SAPP: Sistema que utiliza tecnología OCR para identificar y procesar placas patentes de vehículos.
Servidores on-premise: Infraestructura de servidores en las instalaciones de Carabineros.
Controles de acceso: Medidas para limitar el acceso a sistemas, aplicaciones o datos.
Gestión de activos: Proceso para identificar, clasificar y gestionar los activos de información de una organización.
Seguridad física y del entorno: Medidas para proteger recursos físicos como servidores y centros de datos.
Gestión de incidentes de seguridad de la información: Proceso para detectar, responder, mitigar y recuperar incidentes de seguridad de la información.
Evaluación y tratamiento de riesgos: Proceso para identificar, evaluar y mitigar riesgos de seguridad de la información.
Desarrollo seguro: Enfoque de desarrollo de software que incorpora prácticas y controles de seguridad desde el inicio del ciclo de vida del software.
Metodologías ágiles: Enfoques de desarrollo de software que priorizan la entrega rápida e incremental de funcionalidades.

SITia

Sistema Integrado de Teleprotección con Inteligencia Artificial

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Subsecretaría del Interior
Gobierno de Chile

Subsecretaría de Prevención del Delito
Gobierno de Chile

03 Re-uso de dato

Desarrollo del Decreto Nº 83

El Decreto Nº 83 establece requisitos para asegurar la confidencialidad, integridad y disponibilidad de documentos electrónicos. Incluye la implementación de controles de seguridad y una evaluación de riesgos para identificar amenazas y vulnerabilidades en el SAPP.

Desarrollo de Normas ISO

ISO/IEC 27001:
Control de acceso
Gestión de activos
Seguridad física y del entorno
Gestión de incidentes de seguridad de la información
Evaluación y tratamiento de riesgos
Gestión de cambios
Auditorías internas de seguridad de la información
Monitoreo de eventos de seguridad
Revisión de seguridad de la información

ISO/IEC 27002:
Control de acceso
Seguridad en el desarrollo de software
Concientización sobre la seguridad de la información
Entrenamiento sobre políticas y procedimientos de seguridad

ISO/IEC 27034:
Seguridad en el desarrollo de software

ISO 31000:
Evaluación y tratamiento de riesgos

Evaluación de Riesgos

El Equipo SITIA realizó una evaluación exhaustiva de riesgos del sistema anterior de Carabineros, siguiendo los principios de la norma ISO 31000. Se establecieron cursos de acción para mitigar estos riesgos, como controles de acceso estrictos, validación y sincronización de datos en tiempo real, y monitoreo y log en las plataformas de Carabineros.

SITia

Sistema Integrado de Teleprotección con Inteligencia Artificial

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Subsecretaría del Interior
Gobierno de Chile

Subsecretaría de Prevención del Delito
Gobierno de Chile

03 Re-uso de dato

Implementación de Controles de Seguridad

En el proyecto SITIA, la implementación de controles de seguridad se aplica para proteger la infraestructura crítica y los datos sensibles de los sistemas de información. Siguiendo las directrices de la norma ISO/IEC 27001, reconocida internacionalmente por su enfoque integral en la gestión de la seguridad de la información, se implementarán medidas de seguridad tecnológicas y organizativas para proteger la información del sistema. Esto incluye la identificación de activos de información, evaluación de riesgos, implementación de políticas de seguridad, controles de acceso, gestión de incidentes de seguridad y auditorías periódicas para garantizar el cumplimiento continuo de los estándares de seguridad. Este enfoque estructurado y proactivo garantiza una protección sólida y adaptable, asegurando la confidencialidad, integridad y disponibilidad de los datos en el entorno del proyecto SITIA.

Controles utilizados según ISO/IEC 27002

Carabineros ha establecido un riguroso conjunto de medidas y protocolos destinados a salvaguardar la integridad y seguridad de sus sistemas de información.

Control de acceso: Carabineros cuenta con controles de acceso físicos y lógicos en su Datacenter.
Gestión de activos: Carabineros cuenta con plataformas de control de gestión de activos para tener control de sistemas según las normas ITIL.
Seguridad física y del entorno: Carabineros cuenta con controles de acceso a edificios y dependencias, mediante CCTV y personal capacitado.
Gestión de incidentes de seguridad de la información: Carabineros cuenta con manuales y procedimientos para gestionar incidentes de seguridad y continuidad de servicios.

Desarrollo Seguro y Metodologías Ágiles

En el proyecto SITIA, se adoptarán prácticas de desarrollo seguro como piedra angular para garantizar la integridad y confidencialidad de los sistemas y datos. Esto implicará la integración de medidas de seguridad desde las etapas iniciales del ciclo de vida del desarrollo de software, asegurando que la seguridad se considere de manera proactiva en cada fase del proceso. Se llevarán a cabo revisiones continuas de código para identificar posibles vulnerabilidades y asegurar el cumplimiento de los estándares de seguridad. Las pruebas de seguridad automatizadas serán una parte fundamental del proceso, permitiendo la detección temprana de posibles fallos o brechas de seguridad.

Además, se implementarán metodologías ágiles y de desarrollo continuo (CI/CD) para mantener un enfoque flexible y adaptable frente a los cambios del entorno. Esto permitirá una respuesta rápida a las necesidades emergentes y la implementación incremental de mejoras en la seguridad. La adopción de estas metodologías no solo agilizará el proceso de desarrollo, sino que también facilitará la integración de nuevas características y actualizaciones de seguridad de manera eficiente y sin interrupciones en el funcionamiento del sistema.

Asimismo, se priorizará la capacitación del personal en seguridad de la información, garantizando que todos los miembros del equipo estén familiarizados con las mejores prácticas de seguridad y puedan contribuir activamente a la protección de los activos y datos del proyecto SITIA. Esta combinación de prácticas de desarrollo seguro, metodologías ágiles y capacitación del personal garantizará un enfoque integral hacia la seguridad de la información en todas las etapas del proyecto, fortaleciendo su robustez y confiabilidad.

03 Re-uso de dato

Controles utilizados según ISO/IEC 27034 (desarrollo seguro)

Personal SITIA realizó análisis de las mejores prácticas a utilizar con el fin de realizar mejoras al sistema, separando cada etapa como se menciona:

Definición de requisitos de seguridad
Diseño seguro
Implementación segura
Verificación y validación de seguridad

Desarrollo de Políticas y Procedimientos

Se elaborarán políticas y procedimientos internos alineados con los requisitos del Decreto 83 y otras normativas aplicables.

Controles utilizados según ISO/IEC 27002:

Control de acceso
Seguridad en el desarrollo de software
Gestión de incidentes de seguridad de la información
Seguridad en la gestión de proveedores
Capacitación y Concientización

Se llevará a cabo capacitación regular para todos los empleados involucrados en el manejo del sistema, conforme a la norma ISO 27001.

Controles utilizados según ISO/IEC 27002:

Concientización sobre la seguridad de la información
Entrenamiento sobre políticas y procedimientos de seguridad
Capacitación en manejo seguro de datos
Auditoría y Monitoreo

Se establecerá un programa de auditoría interna para monitorear el cumplimiento de las políticas y procedimientos establecidos.

Controles utilizados según ISO/IEC 27001:

Auditorías internas de seguridad de la información
Monitoreo de eventos de seguridad
Revisión de cumplimiento normativo
Gestión de Riesgos Continua

Se realizarán evaluaciones periódicas de riesgos, conforme a la norma ISO 31000, para identificar posibles amenazas y vulnerabilidades en el sistema.

03 Re-uso de dato

Controles utilizados según ISO/IEC 27001:

Evaluación y tratamiento de riesgos
Mejora continua del SGSI
Actualización Continua

Se mantendrán actualizados los sistemas, tecnologías y procesos relacionados con la seguridad de la información.

Controles utilizados según ISO/IEC 27001:

Gestión de cambios
Revisión de seguridad de la información
Actualización de políticas y procedimientos

Versionado de Código en Github

Se utilizará Github como repositorio de control de versiones para el código del SAPP. Esto permitirá realizar un seguimiento de los cambios realizados en el código, revertir a versiones anteriores si es necesario y colaborar de manera efectiva entre los desarrolladores. Además, se establecerán políticas claras de acceso al repositorio para garantizar que solo las personas autorizadas puedan realizar cambios en el código.

Protección de la Información en Azure

Para proteger la información que se enviará a la plataforma Azure para su análisis, se implementarán las siguientes medidas:

Cifrado: La información se cifrará antes de enviarla a Azure. Esto evitará que personas no autorizadas puedan leerla si se intercepta en tránsito.
Control de acceso: Solo las personas autorizadas podrán acceder a la información en Azure. Esto se logrará mediante el uso de roles y permisos de Azure.
Monitoreo y auditoría: Se monitoreará el acceso a la información en Azure y se realizarán auditorías periódicas para garantizar que se cumplan las políticas de seguridad.

Controles utilizados según ISO/IEC 27001:

Gestión de cambios
Revisión de seguridad de la información
Actualización de políticas y procedimientos

03 Re-uso de dato

Versionado de Código en Github

Se utilizará Github como repositorio de control de versiones para el código del SAPP. Esto permitirá realizar un seguimiento de los cambios realizados en el código, revertir a versiones anteriores si es necesario y colaborar de manera efectiva entre los desarrolladores. Además, se establecerán políticas claras de acceso al repositorio para garantizar que solo las personas autorizadas puedan realizar cambios en el código.

Protección de la Información en Azure

Para proteger la información que se enviará a la plataforma Azure para su análisis, se implementarán las siguientes medidas:

Cifrado: La información se cifrará antes de enviarla a Azure. Esto evitará que personas no autorizadas puedan leerla si se intercepta en tránsito.
Control de acceso: Solo las personas autorizadas podrán acceder a la información en Azure. Esto se logrará mediante el uso de roles y permisos de Azure.
Monitoreo y auditoría: Se monitoreará el acceso a la información en Azure y se realizarán auditorías periódicas para garantizar que se cumplan las políticas de seguridad.