ITBOY
NIT. 891. 801. 069-8

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUTO DE TRÁNSITO DE BOYACÁ

Oficina de Planeación y Sistemas

VIGENCIA 2025 – V2
15/01/2025

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA APROBACIÓN
1	Creación del PTRSPI.	25-01-2024
2	Actualización	15-01-2025

CONTENIDO

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto de Transito de Boyacá, se encuentra enfocado en vigilar de una manera eficaz la gestión integral de todo tipo de riesgo en la información. Esta es una entidad de carácter público y de asistencia al habitante donde se encuentra en constante intercambio de información con entes públicos y privados, así mismo como la ciudadanía en general. Toda esta información que se recibe es la materia para el buen desarrollo de sus funciones y con base en ella se toman decisiones y se ejecutan acciones que pueden generar comunicados, resoluciones, oficios, etc.

Esta información puede ser de carácter público para conocimiento de la ciudadanía en general o puede tratarse de investigaciones de mayor confidencialidad dentro del desarrollo de los procesos. Dado lo anterior, es de suma importancia tener en cuenta claramente el tipo de información que se está procesando para determinar los riesgos a los que está expuesta con el fin de protegerla debidamente.

Para la toma de decisiones con base en la información de altos estándares de calidad, en materia de políticas y gestión de seguridad de la información que permita tomar una disposición y prestar servicios a las personas y funcionarios(as) del Instituto, es necesario que la información sea real, oportuna y de acceso a las personas que lo requieren.

Internacionalmente la norma ISO 31000 ayuda a establecer un sistema de Gestión de Riesgos de cualquier tipo, incluyendo riesgos asociados a la información, esto permite reducir las falencias propias de la información a través de un tratamiento continuo y apropiado de los controles que mitiguen las posibles afectaciones a la Entidad.

La metodología MAGERIT nos ayuda a realizar un análisis y gestión de riesgos y así mismo se puede implementar medidas de control adecuadas que permitan tener los riesgos mitigados.

Basado en la norma ISO 31000 y la metodología MAGERIT, el Instituto de Transito de Boyacá, establece el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para identificar, valorar y gestionar los riesgos de seguridad de la información.

2. ALCANCE

La gestión de riesgos de seguridad y privacidad de la información junto con su tratamiento se aplicará a todas las dependencias del Instituto de Transito de Boyacá, lo que incluye a todos sus funcionarios, contratistas, a toda la ciudadanía en general y a aquellas personas que por cumplimiento de los compromisos contractuales o en ejercicio de sus funciones realicen tratamiento de la información de la cual el Instituto es responsable; así como a los diferentes activos de información que hacen parte del sistema de información.

Para lograr alcanzarlo es importante habilitar inicialmente las funciones de liderazgo para asesorar y apoyar el proceso de diseño, implementación y mantenimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información, seguido de una capacitación y generación de una cultura en la entidad para la gestión integral del riego.

3. OBJETIVO

3.1. Objetivo General:

Diseñar, consolidar e implementar el plan de tratamiento de riesgos de seguridad y privacidad de la información para cada uno de los procesos del Instituto de Transito de Boyacá y establecer un plan de trabajo para identificar y gestionar los riesgos de la información durante el periodo actual cumpliendo la norma ISO 31000 y la metodología MAGERIT.

3.2. Objetivos Específicos:

- Determinar el alcance de la gestión integral del riesgo encaminados a la seguridad y privacidad de la información.
- Establecer las fases para la gestión integral del riesgo asociados a los procesos.
- Definir a través de una adecuada administración del riesgo, una base confiable para la toma de decisiones.
- Generar conciencia y cultura enfocada a la identificación de los riesgos de seguridad y privacidad de la información.

4. DEFINICIONES

Activo: Cualquier elemento que tenga valor para la organización.

Controles: Procesos, políticas y/o actividades que pueden modificar el riesgo.

Riesgo: efecto de la incertidumbre sobre los objetivos.

Gestión del Riesgo: actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

5. DESARROLLO DEL PLAN

5.1. Actividades a Desarrollar

El Instituto de Transito de Boyacá da cumplimiento a las políticas de Seguridad de la Información y para mejorar y conservar los niveles de confidencialidad, integridad y disponibilidad de la información institucional, se apoya en las normas, estándares, políticas y directrices establecidas por los entes competentes para el adecuado manejo de la información mediante la identificación y gestión de los riesgos de seguridad de la información.

A continuación, se relaciona el plan de actividades que se deben desarrollar:

CICLO PHVA	META	ACTIVIDAD
Planear	Definir estado actual y estado deseado. Valoración del Riesgo.	Planificación del Tratamiento del Riesgo.
Hacer	Mitigar y controlar riesgos en seguridad de la información.	Implementación del Plan de Tratamiento de Riesgo
Verificar	Examinar si el plan de tratamiento está siendo efectivo.	Monitoreo y Revisión Continuo de los Riesgos.
Actuar	Identificar vulnerabilidades.	Mantener y Mejorar el Proceso de

		Gestión del Riesgo en la Seguridad de la Información.

5.2. Método de Análisis de Riesgo

Para realizar un análisis de riesgos, la metodología MAGERIT nos pauta los siguientes pasos:

1. Determinar los activos relevantes para el Instituto de Transito de Boyacá, su interrelación y su valor, en el sentido de qué perjuicio (costo) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué procedimientos o mecanismos tecnológicos que reducen el riesgo hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

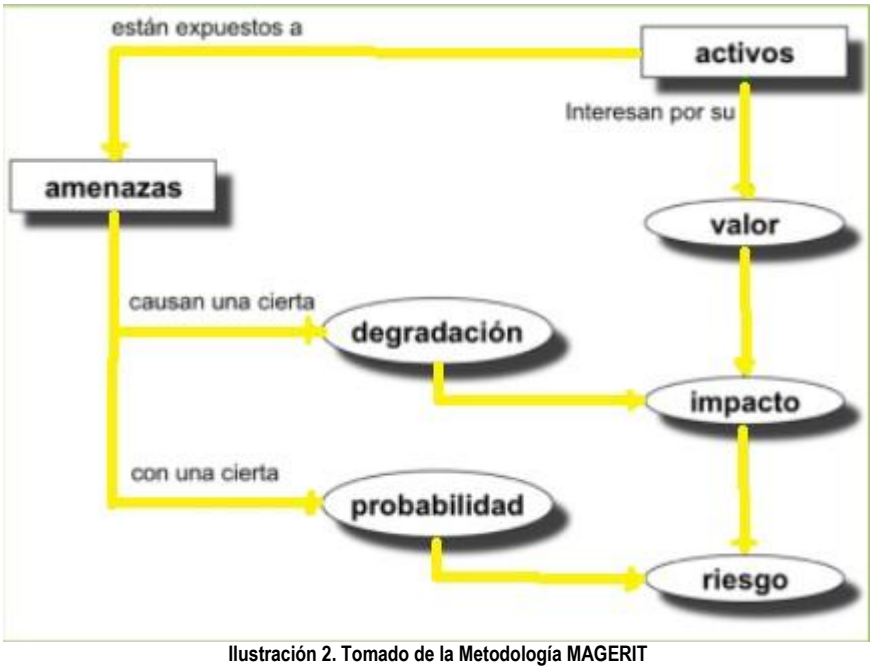


Ilustración 2. Tomado de la Metodología MAGERIT

Activos: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Amenazas: Consiste en determinar e identificar las amenazas que pueden afectar un o los activos, se define como amenaza una causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

En las amenazas, típicamente existen 5 tipos como lo son:

- De origen natural: se debe tener en cuenta que puede suceder accidentes naturales tales como terremotos, inundaciones, etc.
- Del entorno: existen desastres tales como contaminación, fallos en la red eléctrica o de comunicaciones, etc. donde la información es víctima pasiva.
- Defectos de las aplicaciones: hay problemas que nacen por defecto en el diseño o implementación, frecuentemente se conocen como vulneraciones.
- Causadas por las personas de forma accidental: las personas con acceso a los sistemas de información pueden causar problemas sin ningún tipo de intención.
- Causadas por las personas de forma deliberada: las personas con acceso al sistema de información pueden realizar problemas intencionalmente tales como: para beneficiarse indebidamente, con ánimo de causar daño y perjuicios a la entidad.

El análisis de riesgo permite determinar la degradación de este a partir de cuan es perjudicado resultaría el activo y la probabilidad de su ocurrencia, así como también determinar el riesgo inherente de cada activo y asignar el responsable.

La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela cualitativamente por medio de alguna escala nominal:

MA	Muy Alta	Case Seguro	Fácil
A	Alta	Muy alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco probable	Muy difícil
MB	Muy baja	Muy raro	Extremadamente difícil

Tabla 2. Degradación del Valor Fuente: Metodología MAGERIT

A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra. Son valores típicos:

MA	100	Muy Fuerte	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios año
MB	1/100	Muy poco frecuente	Siglos

Tabla 3. Probabilidad de Ocurrencia Fuente: Metodología MAGERIT

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

1. Caracterización de los activos del Instituto de Transito de Boyacá
   a) Identificación de los activos
   b) Dependencia entre activos
   c) Valoración de los activos
2. Caracterización de las amenazas del Instituto de Transito de Boyacá

a) Identificación de las amenazas
b) Valoración de las amenazas

3. Caracterización de las protecciones del Instituto de Transito de Boyacá
   a) Identificación de las protecciones pertinentes
   b) Valoración de las protecciones
4. Estimación del estado del riesgo
   a) Estimación del impacto
   b) Estimación del riesgo

Las tareas se formalizan como lo ilustra el siguiente proceso:

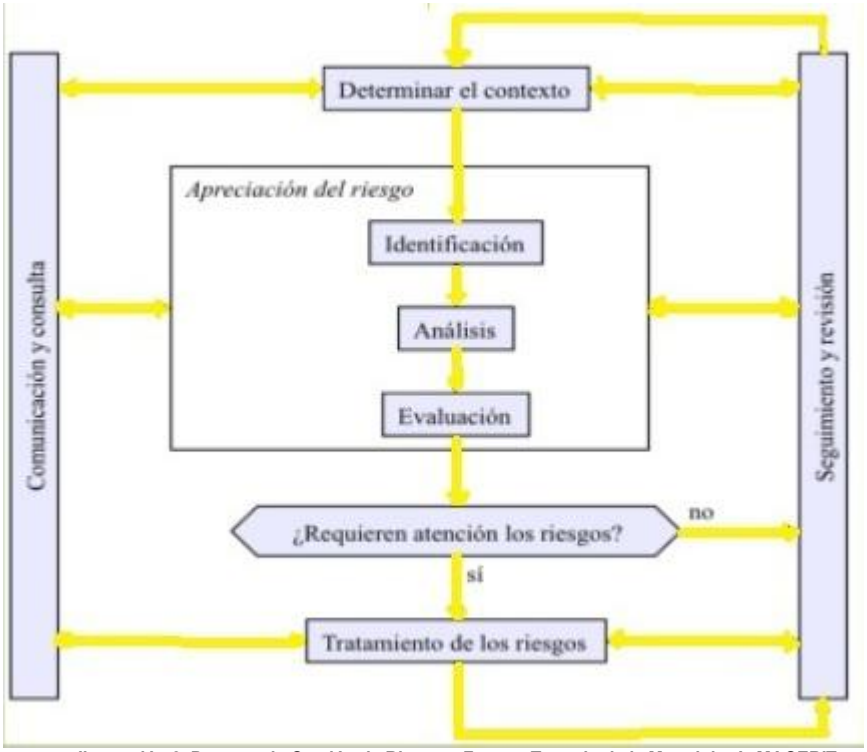


Ilustración 2. Proceso de Gestión de Riesgos. Fuente: Tomado de la Metodología MAGERIT

5.3. Tipo De Protección

Es habitual hablar de diferentes tipos de protección prestados por los procedimientos o mecanismos tecnológicos que reducen el riesgo, tales como:

- **Preventivo:** cuando se reduce las oportunidades de que un incidente ocurra.
- **Disuasión:** cuando se tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar.
- **Eliminación:** cuando se impide que éste tenga lugar.
- **Minimización/limitación del impacto:** cuando se acota las consecuencias de un incidente.
- **Corrección:** cuando se produce un daño, este se repara.

- **Recuperación:** cuando se permite regresar al estado anterior al incidente.
- **Monitorización:** cuando se vigila lo que está ocurriendo o lo que ha ocurrido.
- **Detección:** cuando se informa de que el ataque está ocurriendo en el momento preciso.
- **Concienciación:** son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él.
- **Administración:** son los componentes de seguridad relacionados al sistema.

La tabla a continuación relaciona cada uno de estos tipos de protección con el modelo anterior de reducción de la degradación y de la probabilidad:

Efecto	Tipo
Preventiva: reducen la probabilidad	PR preventiva DR Disuasorias EL eliminatorias
Acotan la degradación	IM minimizadoras CR correctivas RC recuperativas
Consolidan el efecto de las demás	MN de monitorización DC de detección AW de concientización AD administrativa

Tabla 3. Relación de Tipos de Protección Fuente: Metodología MAGERIT

5.4. Clasificación del Riesgo

1. **Riesgo Estratégico:** se enfoca en asuntos globales relacionados con la misión, la visión y el plan de desarrollo vigente, la clara definición de políticas, diseño y conceptualización de la entidad por parte del gerente y su equipo.
2. **Riesgo Operativo:** comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y la articulación entre áreas.
3. **Riesgo Financiero:** se relacionan con el manejo de los recursos de la entidad, que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
4. **Riesgo de Cumplimiento:** se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
5. **Riesgo de Infraestructura Física y Tecnológica:** están relacionados con la capacidad de infraestructura física y tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión, visión y el plan de desarrollo vigente.

5.5. Análisis de Riesgos

Para el Instituto de Transito de Boyacá es muy importante documentar y especificar cada una de las etapas surtidas para el plan. A continuación, se presenta una serie de etapas propuestas para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

5.5.1. Identificación del Riesgo

Se debe plasmar cuales son los riesgos eminentes para la ADC

5.5.2. Identificación de los Activos

Un activo es todo aquello que tiene valor para el Instituto de Transito de Boyacá, se plasmar la manera de como identificaremos los activos.

5.5.3. Identificación de las Amenazas

Las amenazas más comunes:
D= Deliberadas, A= Accidentales, E= Ambientales

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	E
	Perdida de suministro de energía	E
	Falla en equipo de telecomunicaciones	
Perturbación debida a la radiación	Radiación electromagnética	
	Radiación térmica	
	Impulsos electromagnéticos	
Compromiso de la información	Interceptación de señales de interferencia Comprometida	
	Espionaje remoto	
	Escucha encubierta	
	Hurto de medios o documentos	
	Hurto de equipo	
	Recuperación de medios reciclados o desechados	
	Divulgación	
	Datos provenientes de fuentes no confiables	

	Manipulación con hardware	
	Manipulación con software	
	Detección de la posición	
	Fallas del equipo	
	Saturación del sistema de información	
	Saturación del sistema de información	
	Incumplimiento en el mantenimiento del sistema de información.	
Acciones no autorizadas	Uso no autorizado del equipo	
	Copia fraudulenta del software	
	Uso de software falso o copiado	
	Corrupción de los datos	
	Procesamiento ilegal de datos	
Compromiso de las funciones	Error en el uso	
	Abuso de derechos	
	Falsificación de derechos	
	Negación de acciones	
	Incumplimiento en la disponibilidad del personal	

Tabla 4. Amenazas Comunes Fuente: Metodología MAGERIT

Es recomendable tener particular atención a las fuentes de amenazas humanas:

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	Piratería Ingeniería Social Intrusión, accesos forzados al sistema Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	Crimen por computador Acto fraudulento Soborno de la información Suplantación de identidad Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	Bomba/Terrorismo Guerra de la información Ataques contra el sistema DDoS Penetración en el sistema Manipulación en el Sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Ventaja política Explotación económica Hurto de información Intrusión en privacidad

		personal Ingeniería social Penetración en el sistema Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	Asalto a un empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingreso de datos falsos o corruptos Interceptación Código malicioso Venta de información personal Errores en el sistema Intrusión al sistema Sabotaje del sistema Acceso no autorizado al sistema.

Tabla 5. Relación de Tipos de Protección Fuente: Metodología MAGERIT

5.5.4. Identificación De Controles Existentes

Se debe plasmar que controles existen actualmente en la ADC

5.5.5. Identificación de las vulnerabilidades

Se debe plasmar las vulnerabilidades existentes:

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la	Radiación

	radiación electromagnética	electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos
	Falta de cuidado en la disposición final	Hurtos medios o documentos
	Copia no controlada	Hurtos medios o documentos.
RED	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso

	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaces	Mal funcionamiento del Software
	Descarga y uso no controlado de software	Manipulación con Software
	Ausencia de copias de respaldo	Manipulación con Software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o Documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del Equipo
	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de Telecomunicaciones
	Punto único de fallas	Fallas del equipo de Telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de	Espionaje remoto

	contraseñas en claro	
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del Equipo
PERSONAL	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	
	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	
	Red energética inestable	
	Ausencia de protección física de la edificación (Puertas y ventanas)	
ORGANIZACIÓN	Ausencia de procedimiento formal	Abuso de los derechos

	para el registro y retiro de usuarios	
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal	Datos provenientes de fuentes no confiables

	para la autorización de la información disponible al público	
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o Documentos

	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado

Tabla 6. Vulnerabilidades Comunes Fuente: Metodología MAGERIT

5.5.6. Identificación de las consecuencias

Para la identificación de las consecuencias es necesario tener:

- Lista de activos de información y su relación con cada proceso de la entidad.
- Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

5.5.7. Evaluación del riesgo

Esta evaluación del riesgo se realiza dependiendo de la información obtenida de las fases anteriormente descritas.

6. VALORACION DE INCIDENTES

6.1.1. Análisis de Costos

Los incidentes de seguridad informático, es ineludible desarrollar mecanismos para gestionarlos. Para dar inicio al análisis y valoración de los incidentes de seguridad se debe partir con entender las siguientes definiciones:

- **Costo directo:** corresponde al desembolso directo de gastos para llevar a cabo una determinada actividad.

- **Costos indirectos:** equivale a la cantidad de tiempo, esfuerzo y otros recursos de la organización incurridos, pero sin que estos impliquen un gasto efectivo.
- **El Costo de oportunidad:** es el costo resultante de la pérdida de oportunidades comerciales, como consecuencia de efectos negativos en la reputación, como resultado del de la demora en informar a los clientes víctimas y públicamente a través de los medios de comunicación.
- **Costos Externos:** incluyendo la pérdida de activos de información, interrupción del negocio, daños en el equipo Y la pérdida de ingresos, se capturaron utilizando métodos de costos sombra. Los costes totales se asignaron a Nueve vectores de ataque discernibles: virus, gusanos, troyanos; Malware; Botnets; Ataques basados en la web; Phishing e ingeniería social; Miembros maliciosos; Dispositivos robados o dañados; código malicioso (Incluida la inyección de SQL); Y negación de servicios.
- **Centros de Costo:** Los centros de costos identifican cada una de las posibles fases que se deben tener en cuenta para determinar valores en la atención de incidentes de seguridad de la información según el modelo Ponemon Tomado de (Ponemon Org., 2016).

Para estimar el valor de los costos asociados a los incidentes más frecuentes, se investigaron valores de referencia de estudios realizados por las firmas Kaspersky Lab y Ponemon Institute, donde basados en encuestas realizadas a (237) empresas en 6 países, las cuales tuvieron incidentes de seguridad, se pudo obtener valores promedio que sirven de referencia para estimar el costo promedio de los incidentes para una empresa de gran tamaño.

ANÁLISIS INTERNO	TIPO DE COSTO	DESCRIPCIÓN	VALOR
Detección (Causas, víctimas probables)	Directo	Presupuesto para actividades forenses y de investigación, servicios de evaluación y auditoría, gestión de equipo de crisis. Adicionalmente se incluyen costos por Valor de la propiedad intelectual, listas de clientes, secretos comerciales, u otros activos que fueron afectados	$ 27,542
Investigación & Escalamiento (Organizar el equipo de Respuesta)	Directo	Contratación de consultores, expertos en gestión de riesgos, abogados, consultores de seguridad físicos y especialistas en relaciones públicas	$ 10,875
Contención (Ataque y Solución al Incidente)	Directo	Actividades que se centran en detener o disminuir el Incidente	Depende de la cantidad de Recursos Físicos y Humanos requeridos para la mitigación.
Recuperación (Puesta en Marcha Sistemas Afectados)	Directo	Actividades asociadas con la reparación y reparación de los sistemas de la organización Y los procesos centrales de negocio. Estos incluyen la restauración de los activos de información dañados	$ 392,984
Respuesta a Post-Incidente (Actividades para que no Vuelva a ocurrir el Incidente).	Indirecto	Actividades para ayudar a la organización a minimizar posibles ataques futuros. Estas Incluir los	$ 118,780

		costos derivados de la interrupción del negocio y la pérdida de información, así como Tecnologías y sistemas de control. Mitigación de Secuelas.	
VALOR TOTAL INCIDENTES EN UN AÑO.			**$ 550,181**

Tabla 7. Análisis Interno de Costos según Kaspersky Lab y Ponemon Institute

ANÁLISIS EXTERNO	TIPO DE COSTO	DESCRIPCIÓN	VALOR
Perdida de Información	Directo	Pérdida o robo de información sensible y confidencial como Resultado de un ataque cibernético.	Depende de la Sensibilidad de la Información
Disrupción del Negocio	De Oportunidad	El impacto económico del tiempo de inactividad o interrupciones.	$ 105,800.00
Daños en equipos	Directo	Valores ocasionados por la reparación de los equipos afectados por incidentes de seguridad.	$ 566,000.00
Pérdida de Ingresos	Indirecto	Valores asociados o que deja de recibir la compañía por comportamientos anormales de las ventas con clientes, costos asociados por las estrategias de captación de clientes, pérdida de reputación o pérdida del conocimiento del buen hacer.	$ 3,030,814
Valor Total de Incidentes en un Año			**$ 3,702,614.00**

Tabla 8. Análisis Externo de Costos según Kaspersky Lab y Ponemon Institute

El laboratorio Kaspersky junto con la empresa B2B international desarrollaron un estudio a más de 4.000 representantes de empresas de 25 países, revisando complejidad de infraestructura, presupuesto y soluciones de seguridad; permitiendo determinar cuánto invierten las empresas tanto para protegerse como para recuperarse después de un incidente de seguridad.

El análisis de costos de los incidentes de seguridad desarrollado según Kaspersky y bajo la metodología de Ponemon, establece información relevante que permite evaluar los costos generados al materializarse un riesgo ya previsto en la identificación de incidentes, esta valoración permite establecer criticidad para priorizar las medidas de mitigación de los mismos, a efectos de vislumbrar un horizonte real e un panorama de riesgos que pueden afectar de manera importante la operatividad de la organización.

En términos generales la cuantificación de estos valores, permite a la alta dirección ratificar que la inversión realizada para dar solución de incidentes hubiese sido mayor de no contemplar estos componentes y analizado

el costo de pérdidas por riesgos materializados.

Los costos internos resultados de este análisis indican que las mayores inversiones se realizan en actividades asociadas a la reparación reconstrucción y restauración ocasionada por la afectación a los activos fijos de siendo estos costos directos, que debe contemplarse en la elaboración del presupuesto asignado para la mitigación de los riesgos.

La pérdida de ingresos referente a los costos indirectos (Valores asociados o que deja de recibir la compañía por comportamientos anormales de las ventas con clientes, costos asociados por las estrategias de captación de clientes, pérdida de reputación o pérdida del conocimiento del buen hacer); son los más críticos toda vez que dejan de percibirse recursos importantes sin mencionar la imagen negativa hacia el cliente.

No deben subestimarse los costos que genera la inactividad, interrupción de las operaciones y recuperación de los equipos en el análisis externo (costo de oportunidad); ya que no controlar estos aspectos, puede afectar en el tiempo las finanzas de la organización.

7. CASO DE ESTUDIO INCIDENTES DE SEGURIDAD EN ITBOY

ANÁLISIS INTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Detección (Causas, víctimas probables) - Virus y malware causan pérdida de productividad	Virus y malware causan pérdida de productividad	Directo	4	$ 61,952	$ 247,808
Investigación & Escalamiento (Organizar el equipo de Respuesta)	Virus y malware causan pérdida de productividad	Indirecto	2	$ -	$ -
Recuperación (Puesta en Marcha Sistemas Afectados)	Virus y malware causan pérdida de productividad	Directo	2	$ 27,542	$ 123,904
Respuesta a Post-Incidente (Actividades para que no Vuelva a ocurrir el Incidente).	Virus y malware causan pérdida de productividad	Directo	2	$ 27,542	$ 123,904
Notificación (Plan de comunicaciones, divulgación)	Virus y malware causan pérdida de productividad	Directo	2	$ 27,542	$ 123,904
Valor Total Incidentes en un Año.			**12**	**$ 144,578**	**$ 619,520**

ANÁLISIS EXTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORA)	VALOR	VALOR TOTAL
Pérdida de Información	Virus y malware causan pérdida de productividad	Directo	4	$ 78,914.00	$ 315,656.00
Disrupción del Negocio	Virus y malware causan pérdida de productividad	Directo	8	$ 104,730.00	$ 837,840.00
Daños en equipos	Virus y malware causan pérdida de productividad	Directo	24	$ 104,730.00	$ 2,513,520.00

Pérdida de Ingresos	Virus y malware causan pérdida de productividad	Directo	4	$ 78,914.00	$ 315,656.00
Valor Total de Incidentes en un Año			**40**	**$ 288,374.00**	**$ 3,667,016.00**

Tabla 9. Análisis Interno y Externo Incidente No.1

ANÁLISIS INTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Detección (Causas, víctimas probables) - Virus y malware causan pérdida de productividad	Uso inapropiado del recurso por los empleados	Indirecto	2	$ 61,952	$ 123,904
(Organizar el equipo de Respuesta)	Uso inapropiado del recurso por los empleados	Indirecto	1	$ 30,976	$ 30,976
Recuperación (Puesta en Marcha Sistemas Afectados)	Uso inapropiado del recurso por los empleados	Indirecto	2	$ 27,542	$ 55,084
Respuesta a Post-Incidente (Actividades para que no Vuelva a ocurrir el Incidente).	Uso inapropiado del recurso por los empleados	Indirecto	4	$ 27,542	$ 110,168
Notificación (Plan de comunicaciones, divulgación)	Uso inapropiado del recurso por los empleados	Indirecto	1	$ 27,542	$ 27,542
Valor Total Incidentes en un Año.			**10**	**$ 175,554**	**$ 347,674**

ANÁLISIS EXTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Pérdida de Información	Uso inapropiado del recurso por los empleados	Indirecto	8	$ 78,914.00	$ 631,312.00
Disrupción del Negocio	Uso inapropiado del recurso por los empleados	Indirecto	2	$ 104,730.00	$ 209,460.00
Daños en equipos	Uso inapropiado del recurso por los empleados	Indirecto	2	$ 104,730.00	$ 209,460.00
Pérdida de Ingresos	Uso inapropiado del recurso por los empleados	N/A			$ -
Valor Total de Incidentes en un Año			**12**	**$ 209,460.00**	**$ 418,920.00**

Tabla 10. Análisis Interno y Externo Incidente No.2

ANÁLISIS INTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Detección (Causas, víctimas probables) - Virus y malware causan pérdida de productividad	Pérdida física de dispositivos o medios que contengan datos	Directo	8	$ 72,806	$ 582,448
Investigación & Escalamiento (Organizar el equipo de Respuesta)	Pérdida física de dispositivos o medios que contengan datos	Directo	6	$ 72,806	$ 436,836

Recuperación (Puesta en Marcha Sistemas Afectados)	Pérdida física de dispositivos o medios que contengan datos	Directo	2	$ 27,542	$ 55,084
Respuesta a Post-Incidente (Actividades para que no Vuelva a ocurrir el Incidente).	Pérdida física de dispositivos o medios que contengan datos	Directo	2	$ 72,806	$ 145,612
Notificación (Plan de comunicaciones, divulgación)	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	1	$ 72,806	$ 72,806
Valor Total Incidentes en un Año.			**19**	**$ 318,766**	**$ 1,292,786**

ANÁLISIS EXTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Pérdida de Información	Pérdida física de dispositivos o medios que contengan datos	Indirecto	1	$ 72,806	$ 72,806.00
Disruption del Negocio	Pérdida física de dispositivos o medios que contengan datos	N/A			$ -
Daños en equipos	Pérdida física de dispositivos o medios que contengan datos	Directo	2	$ 72,806	$145,612.00
Pérdida de Ingresos	Pérdida física de dispositivos o medios que contengan datos	N/A			$ -
Valor Total de Incidentes en un Año			**3**	**$ 72,806.00**	**$145,612.00**

Tabla 11. Análisis Interno y Externo Incidente No.3

ANÁLISIS INTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Detección (Causas, víctimas probables) - Virus y malware causan pérdida de productividad	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	1	$ 72,806	$ 72,806
Investigación & Escalamiento (Organizar el equipo de Respuesta)	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	1	$ 72,806	$ 72,806
Recuperación (Puesta en Marcha Sistemas Afectados)	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	1	$ 72,806	$ 72,806
Respuesta a Post-Incidente (Actividades para que no Vuelva a ocurrir el Incidente).	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	1	$ 72,806	$ 72,806
Notificación (Plan de comunicaciones, divulgación)	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	1	$ 72,806	$ 72,806
Valor Total Incidentes en un Año.			**5**	**$ 364,030**	**$ 364,030**

ANÁLISIS EXTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO(HORS)	VALOR	VALOR TOTAL
Pérdida de Información	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Indirecto	0.5	$ 72,806	$ 36,403

Disrupción del Negocio	Pérdida física de dispositivos móviles que exponen riesgo a la organización	N/A			$ -
Daños en equipos	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	2	$ 72,806	$ 145,612
Pérdida de Ingresos	Pérdida física de dispositivos móviles que exponen riesgo a la organización	N/A			$ -
Valor Total de Incidentes en un Año			**2.5**	**$145,612.00**	**$182,015.00**

Tabla 12. Análisis Interno y Externo Incidente No.4

ANÁLISIS INTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Detección (Causas, víctimas probables) - Virus y malware causan pérdida de productividad	Uso inadecuado de datos mediante dispositivos móviles.	Directo	2	$ 72,806	$ 145,612
Investigación & Escalamiento (Organizar el equipo de Respuesta)	Uso inadecuado de datos mediante dispositivos móviles.	Directo	2	$ 72,806	$ 145,612
Recuperación (Puesta en Marcha Sistemas Afectados)	Uso inadecuado de datos mediante dispositivos móviles.	Directo	0.5	$ 72,806	$ 36,403
Respuesta a Post-Incidente (Actividades para que no Vuelva a ocurrir el Incidente).	Uso inadecuado de datos mediante dispositivos móviles.	Directo	0.5	$ 72,806	$ 36,403
Notificación (Plan de comunicaciones, divulgación)	Uso inadecuado de datos mediante dispositivos móviles.	Directo	1	$ 72,806	$ 72,806
Valor Total Incidentes en un Año.			**6**	**$ 364,030**	**$ 436,836**

ANÁLISIS EXTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Pérdida de Información	Uso inadecuado de datos mediante dispositivos móviles.	Indirecto			0
Disrupción del Negocio	Uso inadecuado de datos mediante dispositivos móviles.	N/A			0
Daños en equipos	Uso inadecuado de datos mediante dispositivos móviles.	N/A			0
Pérdida de Ingresos	Uso inadecuado de datos mediante dispositivos móviles.	N/A			0
Valor Total de Incidentes en un Año			**0**	**$ -**	**$ -**

Tabla 13. Análisis Interno y Externo Incidente No.5

7.1. Análisis de Costos Caso de Estudio ITBOY

Para nuestro caso de estudio referente a los costos de incidentes de seguridad más frecuentes en el Instituto de Transito de Boyacá -ITBOY y apoyándonos con los resultados del estudio del laboratorio Kaspersky; se

tomaron como referencia cinco (5) incidentes: Pérdida de Información, disrupción de negocio, daños en equipos y pérdida de ingresos (incidente externo, costo directo); evidenciándose la necesidad de provisionar recursos para atender los posibles costos generados por infecciones informáticas por virus y malware que traumatizan las operaciones en la entidad.

En orden de costos, se aprecian valores ocasionados por la pérdida física de dispositivos o medios que contengan datos, estos costos directos hacen parte de incidentes internos y como bien sabido es, la información es considerada como el activo más valioso de toda organización, no deben entonces escatimarse recursos encaminados a proteger los datos, el análisis indica que igualmente inversiones importantes en la etapa de recuperación deben ser tenidos en cuenta.

Los virus informáticos y los malware son definitivamente como se observa en el cuadro de costos a los que más importancia hay que darle tanto como incidente interno como externo, pues sus constantes ataques ponen en riesgo los sistemas de información de la entidad y contrarrestar los efectos ocasionados representa valores considerables para la entidad.

Las gráficas antes relacionadas reflejan el comportamiento de los incidentes más frecuentes vs los costos de recuperación, de manera concordante con los análisis realizados en el transcurso de este capítulo se concluye la necesidad de prestar toda la atención a la protección de los datos, que son propensos de manera permanente a infecciones informáticas , de prosperar y hacerse efectivo un riesgo de este tipo, los costos en los que incurren las entidades son importantes, más si se tiene en cuenta el papel que juega las probabilidades, no siempre es posible alcanzar una recuperación total logrando desestabilizar a la organización.

Un efecto domino genera reacción sobre la disponibilidad, ocasionando pérdida de productividad e interrupción en la prestación de los servicios que lesiona seriamente la imagen y los ingresos productos de su deber ser.

El factor tiempo es determinante y uno de los actores más importantes en el cálculo de costos por la cristalización de los riesgos, “a mayor tiempo mayor pérdida”, esto lleva a sensibilizar y concientizar a la dirección a fin de enfocar esfuerzos para que en caso de prosperar y hacerse realidad un riesgo, pueda resolverse el impase en el menor tiempo posible.

7.2. Análisis Graficas Tiempos y Costos ITBOY

La Ilustración 1 y la Ilustración 2, reflejan el comportamiento de los incidentes más frecuentes Vs los costos de recuperación, de manera concordante con los análisis realizados en el transcurso de este capítulo se concluye la necesidad de prestar toda la atención a la protección de los datos, que son propensos de manera permanente a infecciones informáticas, de prosperar y hacerse efectivo un riesgo de este tipo, los costos en los que incurren las entidades son importantes, más si se tiene en cuenta el papel que juega las probabilidades, no siempre es posible alcanzar una recuperación total logrando desestabilizar a la organización.

Un efecto domino genera reacción sobre la disponibilidad, ocasionando pérdida de productividad e interrupción en la prestación de los servicios que lesiona seriamente la imagen y los ingresos productos de su deber ser.

El factor tiempo es determinante y uno de los actores más importantes en el cálculo de costos por la cristalización de los riesgos, “a mayor tiempo mayor pérdida”, esto lleva a sensibilizar y concientizar a la dirección a fin de enfocar esfuerzos para que en caso de prosperar y hacerse realidad un riesgo, pueda

resolverse el impase en el menor tiempo posible.

Ilustración 1. Análisis Costos Incidentes más Frecuentes ITBOY

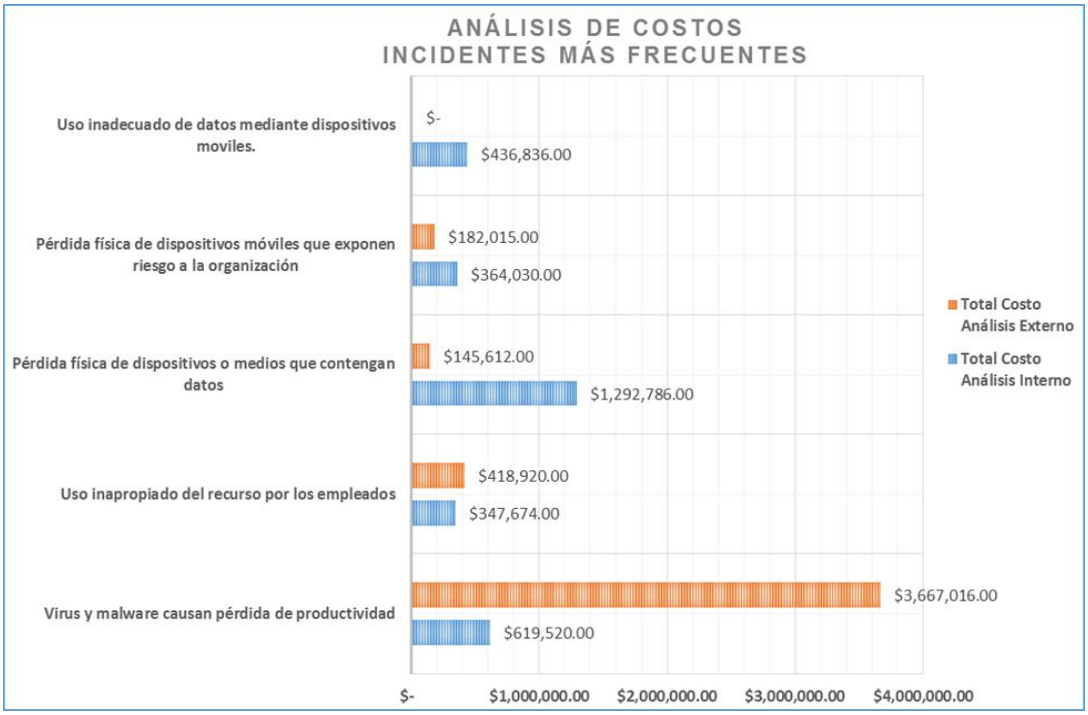
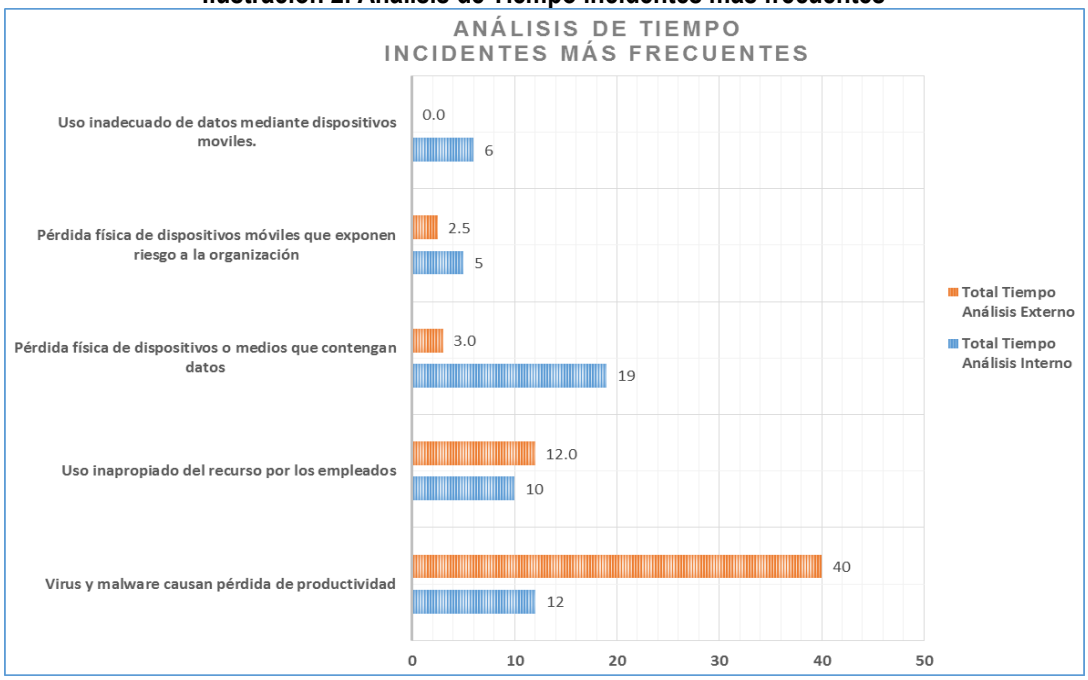


Ilustración 2. Análisis de Tiempo incidentes más frecuentes



En Tunja a los quince (15) días del mes de enero de 2025.

NIDIA CAROLINA PUENTES AGUILAR
Gerente Instituto de Transito de Boyacá

Elaborado por:
Richard Hernan Ayala Joya
Profesional Especializado
INSTITUTO DE TRANSITO DE BOYACA
2025

Revisado por:
William Rene Higuera Morales
Jefe Oficina Asesora Planeación y Sistemas
INSTITUTO DE TRANSITO DE BOYACA
2025