

## EVALUACION MATRIZ MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PERIODO 2024

**FECHA:** 20/12/2024

**ENTIDAD:** GOBERNACIÓN DE ARAUCA

**PROCESO:** TECNOLOGÍA DE LA INFORMACIÓN

**OBJETIVO DEL PROCESO:** Garantizar el funcionamiento de los Sistemas de Información y de infraestructura de Tecnología de Información de la Administración Departamental, actuando de manera eficiente, para asegurar que los servicios de soporte acordados con los procesos del negocio se cumplan de manera eficiente conforme la innovación y las soluciones de mejora tecnológica requeridas en materia de software y hardware para hacer mas competitiva la gestión de la gobernación de Arauca.

**LIDER:** XIOMARA TORRES VARGAS, Profesional Universitario SGDI.

### OBJETIVO EVALUACIÓN:

Realizar seguimiento de los riesgos y los controles implementados, asegurando que las medidas de seguridad se ajusten ante nuevos riesgos emergentes o cambios en el entorno.

### GLOSARIO:

- ✚ **Confidencialidad:** La información solo tiene que ser accesible o divulgada a aquellos que están autorizados.
- ✚ **Integridad:** La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.
- ✚ **Disponibilidad:** La información debe estar siempre accesible para aquellos que estén autorizados.
- ✚ **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- ✚ **Amenaza:** causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.
- ✚ **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.
- ✚ **Impacto:** es la consecuencia de la materialización de una amenaza sobre un activo.

- ✚ **Riesgo inherente:** Es el riesgo existente y propio de cada actividad, sin la ejecución de ningún control.
- ✚ **Riesgo residual:** El riesgo que permanece tras el tratamiento del riesgo.
- ✚ **Administración de riesgos:** Proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- ✚ **Análisis de riesgo:** Uso sistemático de la información disponible para valorar los riesgos en función de las causas o agentes que los generan, las consecuencias generadas por un incidente y/o evento, su severidad y la posibilidad de ocurrencia del mismo, con el fin de estimar la zona de riesgo inicial.
- ✚ **Causa:** Medios, circunstancias, situaciones o agentes generadores del riesgo (recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos).
- ✚ **Consecuencia:** Efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la entidad (ejemplo: una pérdida, un daño, un perjuicio, un detrimento).
- ✚ **Control:** Cualquier medida que adopte la entidad para gestionar los riesgos y proporcionar una seguridad razonable de alcanzar los objetivos y metas establecidos.
- ✚ **Evaluación del riesgo:** Determinación de las prioridades de gestión del riesgo, mediante la comparación del nivel de riesgo hallado (riesgo inherente) y la evaluación de las medidas de control existentes. Es una etapa que busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual).
- ✚ **Gestión del riesgo:** Es el proceso de su identificación y evaluación, y la creación del plan para disminuir o controlar esos riesgos junto con el efecto que podrían tener en la entidad.

## MATRÍZ INICIAL DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La siguiente es la matriz inicial de riesgos aprobada para el proceso de Tecnología de la Información (Riesgos Inherentes):

TIPO ACTIVO	VALORACION ACTIVO				CAUSAS/VULNERABILIDADES	CONSECUENCIA	ID DEL RIESGO	RIESGOS	Clasificación del Riesgo	RIESGO INHERENTE		VALORACION DEL RIESGO	EVALUACION	CONTROL ES
	CONFIDENCIAL	INTEGRIDAD	DISPONIBILIDAD	VALOR ACTIVO						PROBABILIDAD	IMPACTO			
Hardware	2	5	3	10	Falta de seguridad en el acceso al DATACENTER	Posibles daños y pérdidas de equipos	RT11	Acceso al cuarto de comunicaciones por personal no autorizado	Riesgo tecnológico	Casi seguro	Catastrófico	25	Muy Alto	Establecer y documentar una política de control de acceso a información y al DATACENTER de la Gobernación.
Servicio	3	5	3	11	Falta de una política de seguridad de la Información	Afectación de la Infraestructura Tecnológica por falta de lineamientos	RT12	Interrupción de los servicios informáticos por incidentes como cambios de voltajes, ataques cibernéticos, eventos catastróficos, errores humanos, accidentes.	Riesgo tecnológico	Casi seguro	Catastrófico	25	Muy Alto	Elaboración e implementación, verificación, revisión y evaluación del Plan de continuidad del negocio – ISO 22301, que mediante procedimientos que capacite a la Gobernación para responder a un evento de tal manera que las funciones críticas de la Gobernación continúen con los niveles planeados de interrupción o cambios esenciales



TIPO ACTIVO	VALORACION ACTIVO				CAUSAS/VULNERABILIDADES	CONSECUENCIA	ID DEL RIESGO	RIESGOS	Clasificación del Riesgo	RIESGO INHERENTE		VALORACION DEL RIESGO	EVALUACION	CONTROL ES
	CONFIDENCIAL	INTEGRIDAD	DISPONIBILIDAD	VALOR ACTIVO						PROBABILIDAD	IMPACTO			
Hardware	2	5	3	10	Falta de conciencia por parte de la entidad a cerca del perjuicio legal, economico y de imagen, el NO atender los lineamientos en Seguridad del informacion	Sanciones a la entidad por parte de los entes de control por desatención a las normas, lineamientos y políticas	RTI3	Posibles sanciones por desatención a las normas, lineamientos, políticas del orden Nacional y/o Departamental.	Riesgo normativo	Probable	Catastrófico	20	Muy Alto	Definir política para la protección de los derechos patrimoniales sobre los sistemas de información.  Elaboración de auditorías a la Política de Seguridad de la Información.
Información	3	5	3	11	Falta de equipos de seguridad actualizados (hardware-software), para proteger la red de datos de la gobernación	Hackeo indiscriminado de la información Institucional (Ataques que afecten la red interna de la entidad como (Ransomware, DDOS, ARP Spoofing, Phising, Escaneo de puertos, Man in the Middle, entre otros.)Afectando así la integridad, confidencialidad y disponibilidad de los activos de información)	RTI4	Pérdida y/o secuestro de información por falta de controles de seguridad.	Riesgos de imagen	Casi seguro	Catastrófico	25	Muy Alto	Adquisición de equipos de seguridad (hardware-software) para proteger la red de datos de la Gobernación
Software	3	5	3	11	Falta de lineamientos para el desarrollo de Sistemas de Información con criterios de calidad	Desconfianza de clientes y proveedores, respecto a la calidad de la información que genera los sistemas de información	RTI5	Incertidumbre respecto de la calidad de la información que generan los Sistemas informáticos, debido a fallas en su	Riesgo operativo	Probable	Catastrófico	20	Muy Alto	Implementar mecanismos claves en el ciclo de vida de desarrollo de los sistemas de información. (Dominio sistemas de

TIPO ACTIVO	VALORACION ACTIVO				CAUSAS/VULNERABILIDADES	CONSECUENCIA	ID DEL RIESGO	RIESGOS	Clasificación del Riesgo	RIESGO INHERENTE		VALORACION DEL RIESGO	EVALUACION	CONTROLES
	CONFIDENCIAL	INTEGRIDAD	DISPONIBILIDAD	VALOR ACTIVO						PROBABILIDAD	IMPACTO			
						Posibles sanciones de índole legal y fiscal y administrativo		funcionamiento.						información) y programación periódica de mantenimiento y auditorías a los mismos.
Recurso humano	3	1	3	7	Falta de un profesional dedicado a la administración del Modelo de Seguridad de la Información - MSI	Exposición de los activos de información ante pérdida de datos, daños en equipos; así como sanciones y/o multas y pérdida de imagen de la entidad	RT16	Desatención del Modelo de Seguridad y Privacidad de la Información	Riesgo estratégico	Probable	Moderado	12	Alto	Construcción, implementación y seguimiento de la política de seguridad de la información

## APLICACIÓN DE CONTROLES

La siguiente tabla muestra las acciones realizadas para atender los controles aplicados a cada uno de los riesgos que componen la Matriz de Riesgos de la Seguridad de la Información de la Gobernación de Arauca:

ID DEL RIESGO	RIESGO	CONTROL	ACCIONES REALIZADAS	PERIODICIDAD	PERIODO EVALUADO
RT11	Acceso al cuarto de comunicaciones por personal no autorizado	Establecer y documentar una política de control de acceso a información y al DATACENTER de la Gobernación.	Se instaló un sistema biométrico para acceso al cuarto de comunicaciones (DATACENTER), así como el diseño de un procedimiento para su acceso.	ANUAL	01/01/2024-31/12/2024
RT12	Interrupción de los servicios informáticos por incidentes como cambios de voltajes, ataques cibernéticos, eventos catastróficos, errores humanos, accidentes.	Elaboración e implementación, verificación, revisión y evaluación del Plan de continuidad del negocio – ISO 22301, que mediante procedimientos que capacite a la	Se diseñó un Plan de Continuidad del negocio, el cual fue aprobado por calidad; sin embargo, este no se pudo implementar debido a falta de	SEMESTRAL	01/07/2024-31/12/2024

ID DEL RIESGO	RIESGO	CONTROL	ACCIONES REALIZADAS	PERIODICIDAD	PERIODO EVALUADO
		Gobernación para responder a un evento de tal manera que las funciones críticas de la Gobernación continúen con los niveles planeados de interrupción o cambios esenciales	recursos presupuestales.		
RTI3	Posibles sanciones por desatención a las normas, lineamientos, políticas del orden Nacional y/o Departamental.	Definir política para la protección de los derechos patrimoniales sobre los sistemas de información.  Elaboración de auditorías a la Política de Seguridad de la Información.	Desde el área de Sistemas se ha venido haciendo las gestiones encaminadas al registro del software desarrollado, ante la Dirección Nacional de Derechos de Autor (DNDA) del Ministerio del Interior.	ANUAL	01/01/2024-31/12/2024
RTI4	Pérdida y/o secuestro de información por falta de controles de seguridad.	Adquisición de equipos de seguridad (hardware-software) para proteger la red de datos de la Gobernación	Se adquirieron equipos especializados para proteger la red de datos de la gobernación, incluyendo la adquisición de licencias de antivirus y acceso biométrico al DATACENTER.	ANUAL	01/01/2024-31/12/2024
RTI5	Incertidumbre respecto de la calidad de la información que generan los Sistemas informáticos, debido a fallas en su funcionamiento.	Implementar mecanismos claves en el ciclo de vida de desarrollo de los sistemas de información. (Dominio sistemas de información) y programación periódica de mantenimiento y auditorías a los mismos.	Se adaptó la GUIA PARA EL DOMINIO DE SISTEMAS DE INFORMACIÓN, diseñada por MINTIC., como mecanismo para construir un proceso que enfoque la aplicación de las mejores prácticas, para la implementación del dominio de Sistemas de Información, del marco de referencia de arquitectura empresarial para la gestión de TI e la gobernación de Arauca, gestionada por la oficina de TICs.	ANUAL	01/01/2024-31/12/2024

ID DEL RIESGO	RIESGO	CONTROL	ACCIONES REALIZADAS	PERIODICIDAD	PERIODO EVALUADO
RTI6	Desatención del Modelo de Seguridad y Privacidad de la Información	Construcción, implementación y seguimiento de la política de seguridad de la información	<p>Se construyó la Política General de Seguridad de la Información que contiene los principios y las reglas básicas que permita la gestión de la seguridad de la información; proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de seguridad de la información de la GOBERNACION DE ARAUCA, atendiendo los procesos, los objetivos y la normatividad vigente en la entidad. Igualmente, esta Política se ha venido implementando mediante la socialización de la misma a los funcionarios de la Gobernación.</p> <p>A pesare de que existe la política de seguridad de la información, no existe un profesional especializado que se dedique a evaluar los controles y valorar los riesgos que se puedan presentar y que afecten la confidencialidad, integridad y disponibilidad de la información de la gobernación de Arauca.</p>	ANUAL	01/01/2024-31/12/2024

## MATRIZ DE RIESGOS RESULTANTE DE APLICAR LOS CONTROLES

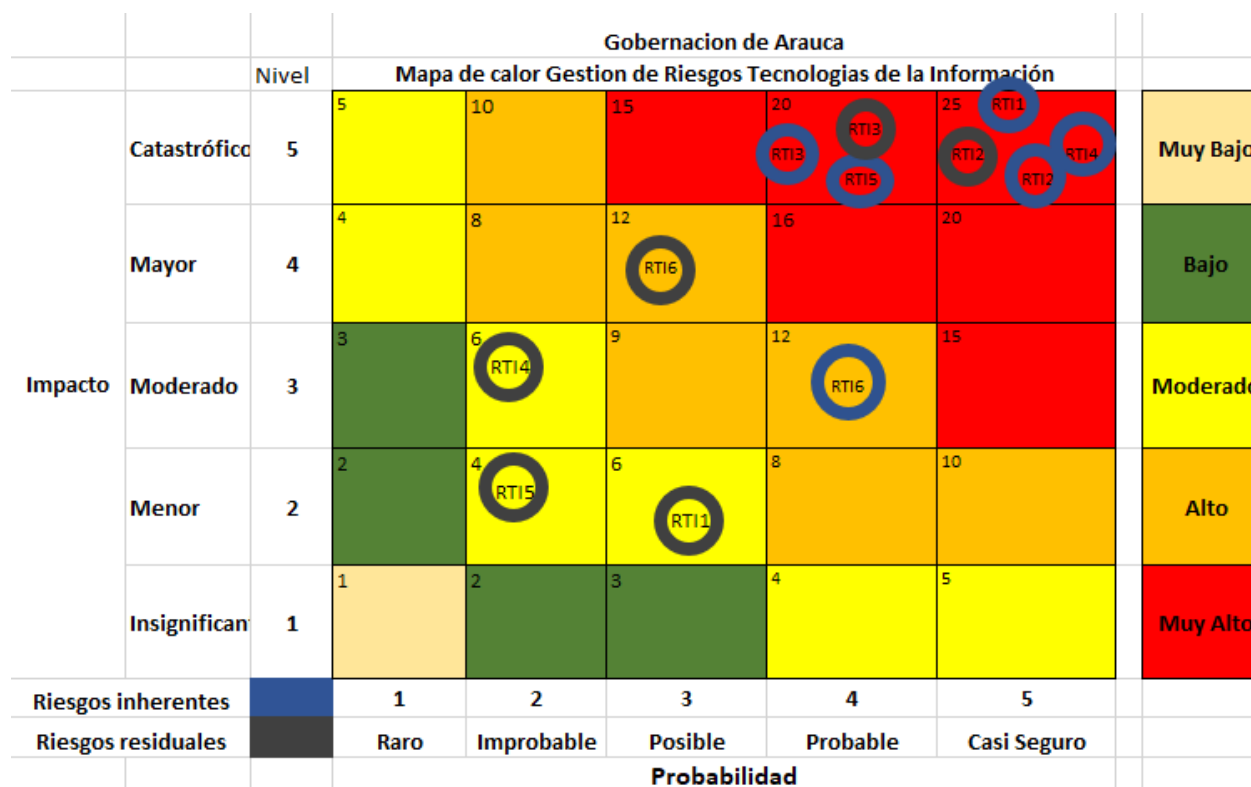
Una vez aplicado los respectivos controles a los riesgos existentes y aplicada la respectiva evaluación, se obtiene una nueva valoración de los Activos y nueva valoración del **riesgo residual**, de la siguiente manera:

TIPO ACTIVO	ID DEL RIESGO	RIESGOS	Clasificación del Riesgo	CONTROLES	NUEVA VALORACION DEL ACTIVO				RIESGO RESIDUAL		VALORACION DEL RIESGO RESIDUAL	EVALUACION
					CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR ACTIVO	PROBABILIDAD	IMPACTO		
Hardware	RTI1	Acceso al cuarto de comunicaciones por personal no autorizado	Riesgo tecnológico	Establecer y documentar una política de control de acceso a información y al DATACENTER de la Gobernación.	1	1	2	4	Posible	Menor	6	Moderado
Servicio	RTI2	Interrupción de los servicios informáticos por incidentes como cambios de voltajes, ataques cibernéticos, eventos catastróficos, errores humanos, accidentes.	Riesgo tecnológico	Elaboración e implementación, verificación, revisión y evaluación del Plan de continuidad del negocio – ISO 22301, que mediante procedimientos que capacite a la Gobernación para responder a un evento de tal manera que las funciones críticas de la Gobernación continúen con los niveles planeados de interrupción o cambios esenciales.	3	5	3	11	Casi seguro	Catastrófico	25	Muy Alto
Hardware	RTI3	Posibles sanciones por desatención a las normas, lineamientos, políticas del orden Nacional y/o Departamental.	Riesgo normativo	Definir política para la protección de los derechos patrimoniales sobre los sistemas de información.  Elaboración de auditorías a la Política de Seguridad de la Información.	2	5	3	10	Probable	Catastrófico	20	Muy Alto
Información	RTI4	Pérdida y/o secuestro de información por falta de controles de seguridad.	Riesgos de imagen	Adquisición de equipos de seguridad (hardware-software) para proteger la red de datos de la Gobernación	3	1	2	6	Improbable	Moderado	6	Moderado
Software	RTI5	Incertidumbre respecto de la calidad de la información que generan los Sistemas informáticos, debido a fallas en su funcionamiento.	Riesgo operativo	Implementar mecanismos claves en el ciclo de vida de desarrollo de los sistemas de información. (Dominio sistemas de información) y programación periódica de mantenimiento y auditorías a los mismos.	1	1	2	4	Improbable	Menor	4	Moderado

TIPO ACTIVO	ID DEL RIESGO	RIESGOS	Clasificación del Riesgo	CONTROLES	NUEVA VALORACION DEL ACTIVO				RIESGO RESIDUAL		VALORACION DEL RIESGO RESIDUAL	EVALUACION
					CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR ACTIVO	PROBABILIDAD	IMPACTO		
Recurso humano	RTI6	Desatención del Modelo de Seguridad y Privacidad de la Información	Riesgo estratégico	Construcción, implementación y seguimiento de la política de seguridad de la información	2	5	2	9	Posible	Mayor	12	Alto

## MAPA DE CALOR RESULTANTE

Una vez evaluado el impacto de los controles aplicados a los riesgos, se obtiene el siguiente mapa de calor:



## CONCLUSIONES

Como conclusión podemos evidenciar que hubo un avance significativo en los riesgos RTI1, RTI4 y RTI5 al pasar de **MUY ALTO** a **MODERADO**, mientras que los riesgos RTI2,

RTI3 se mantuvieron en la misma zona de riesgo **MUY ALTO** y el riesgo RTI6 se mantuvo en la zona de riesgo **ALTO**.

## RECOMENDACIONES

- Se debe continuar aplicando los controles con la periodicidad establecida para cada riesgo.
- Se debe revisar la aparición de nuevos posibles riesgos que puedan afectar la seguridad de la información de la gobernación de Arauca, a efectos de valorarlos e incluirlos en la matriz de riesgos.
- Se debe continuar haciendo gestiones ante la alta gerencia encaminadas a la apropiación de recursos para continuar con la implementación de la política de seguridad de la información de la gobernación de Arauca.
- Se debe contar con un profesional especializado en seguridad de la Información dedicado a evaluar los controles y valorar los riesgos que se puedan presentar y que afecten la confidencialidad, integridad y disponibilidad de la información de la gobernación de Arauca.

### ORIGINAL FIRMADO

**XCIOMARA TORRES VARGAS**

Profesional Universitario SGDI

Elaboró: Javier Vega Otálora, Técnico Operativo SGDI