Tesis de Grado previo a obtener el Título:

MASTER EN AUDITORIA Y EVALUACION DE SISTEMAS DE INFORMACION

Evaluación de Riesgos de los Sistemas de Información de Audioauto S.A. utilizando MAGERIT V3.0 apoyados para el análisis de las dimensiones de Seguridad en los objetivos de control de COBIT V4.1

Maestrantes:

Bethy Janneth Cruz Quinzo

Juan Carlos Chamorro Noboa

PLANTEAMIENTO DEL PROBLEMA

Las amenazas y vulnerabilidades derivadas de la complejidad tecnológica de Audioauto S.A., su necesidad por mantener un alto nivel de integridad, disponibilidad y confidencialidad de la información, generan la existencia un alto nivel de riesgo en los Sistemas de Información que puede impedir el cumplimiento de su misión y generar consecuencias financieras y legales.

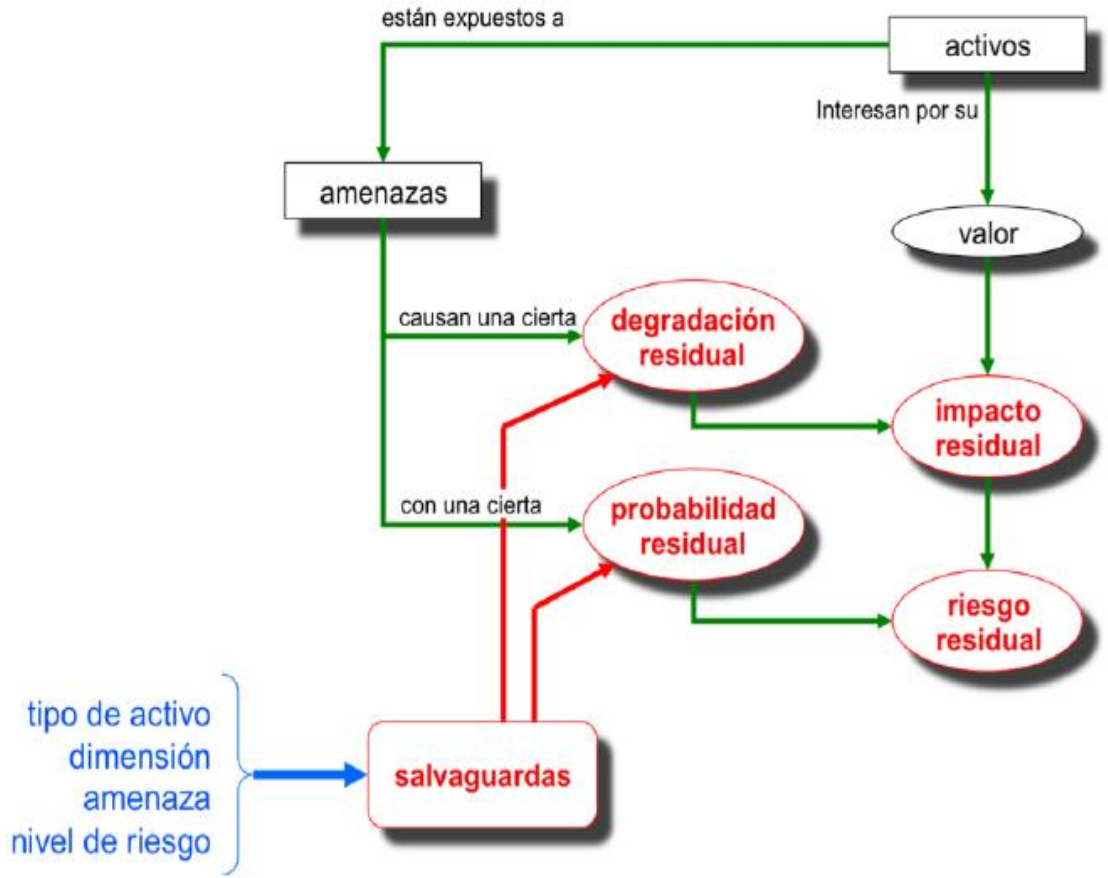
Formulación del Problema a Resolver

Los riesgos relacionados con los Sistemas de Información no han sido evaluados metodológicamente y, por consiguiente no se han determinado los lineamientos sobre los cuales la organización realice una adecuada Gestión de Riesgos, por este motivo se realizará la Evaluación de Riesgos generando la los informes respectivos.

EVALUACIÓN DE LOS RIESGOS

El proceso que sigue MAGERIT para la evaluación de riesgos consiste en determinar los activos más relevantes, su interrelación y valor, posteriormente se identifican las amenazas a las que están expuestos y las salvaguardas que se podrían implementar y su efectividad frente al riesgo. Con esto se estima el impacto sobre el activo derivado de la materialización de la amenaza y el riesgo, definido como el impacto ponderado con la tasa de ocurrencia.

flujo por el que pasa el Impacto Residual y el Riesgo Residual.



Para establecer la Probabilidad de que una amenaza se materialice su Ocurrencia utilizaremos la frecuencia esperada de ocurrencia (ARO – Annual Rate of Occurrence) tomando la siguiente escala nominal:

	Probabilidad	Ocurrencia	Equivalencia
MA	muy alta	casi seguro	Fácil
A	Alta	muy alto	Medio
M	Media	posible	Difícil
B	Baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Escala Nominal para Establecer la Probabilidad que una amenaza se materialice

Para establecer el Impacto tomamos en cuenta la siguiente escala:

	Impacto	Valor	Observación
EX	Extremo	10	Activos que requieren atención inmediata
MA	Muy Alto	9	
AL	Alto	6 - 8	
ME	Medio	3 - 5	
BA	Bajo	1 – 2	
DE	Despreciable	0	Impacto despreciable
Escala para Establecer el Impacto			

El cálculo del Impacto está determinado por el V (valor del activo) x D (% de degradación) para lo cual establecemos la siguiente tabla:

IMPACTO		Degradación del Activo				
		20%	40%	60%	80%	100%
Valor del Activo	EX	AL	MA	EX	EX	EX
	MA	ME	AL	MA	MA	MA
	AL	BA	ME	AL	AL	AL
	ME	DE	BA	ME	ME	ME
	BA	DE	DE	BA	BA	BA
	DE	DE	DE	DE	DE	DE
Escala para calcular el Impacto						

Para establecer el Riesgo tomamos en cuenta la siguiente escala:

	Riego	Valor	Observación
MA	Crítico	9 - 10	Riesgo Extremadamente Alto
A	Importante	7 - 8	
M	Apreciable	5 - 6	
B	Bajo	3 - 4	
MB	Despreciable	0 - 2	Riesgo despreciable
Escala para Establecer el Riesgo			

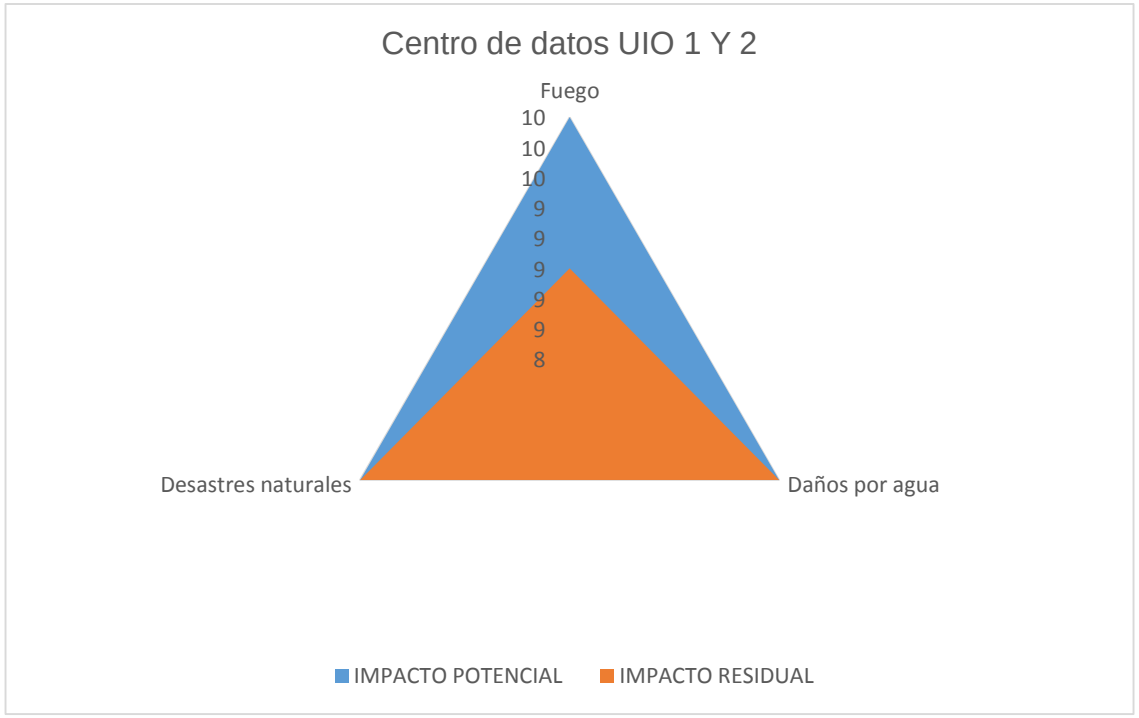
El cálculo del Riesgo está determinado por el I (Impacto) × F (frecuencia) para lo cual establecemos la siguiente tabla:

RIESGO		Probabilidad de que se materialice una amenaza				
		MB	B	M	A	MA
Impacto	EX	MA	MA	MA	MA	MA
	MA	A	MA	MA	MA	MA
	AL	M	A	A	MA	MA
	ME	B	M	M	A	A
	BA	MB	B	B	M	M
	DE	MB	MB	MB	B	B
Escala para calcular el Riesgo						

RESULTADOS DE LA EVALUACION DE RIESGOS

INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR DESASTRES DE ORIGEN NATURAL

En el grafico se puede ver la diferencia entre el impacto potencial y residual debido a la eficacia de las salvaguardas implementadas en el activo. El impacto tiene mayor diferencia en la amenaza Fuego, debido a que la eficacia de la salvaguarda es alta. En la amenaza Daños por agua, la eficacia de la salvaguarda es MB, por lo que el Impacto Residual sigue siendo alto.



INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR DESASTRES DE ORIGEN NATURAL

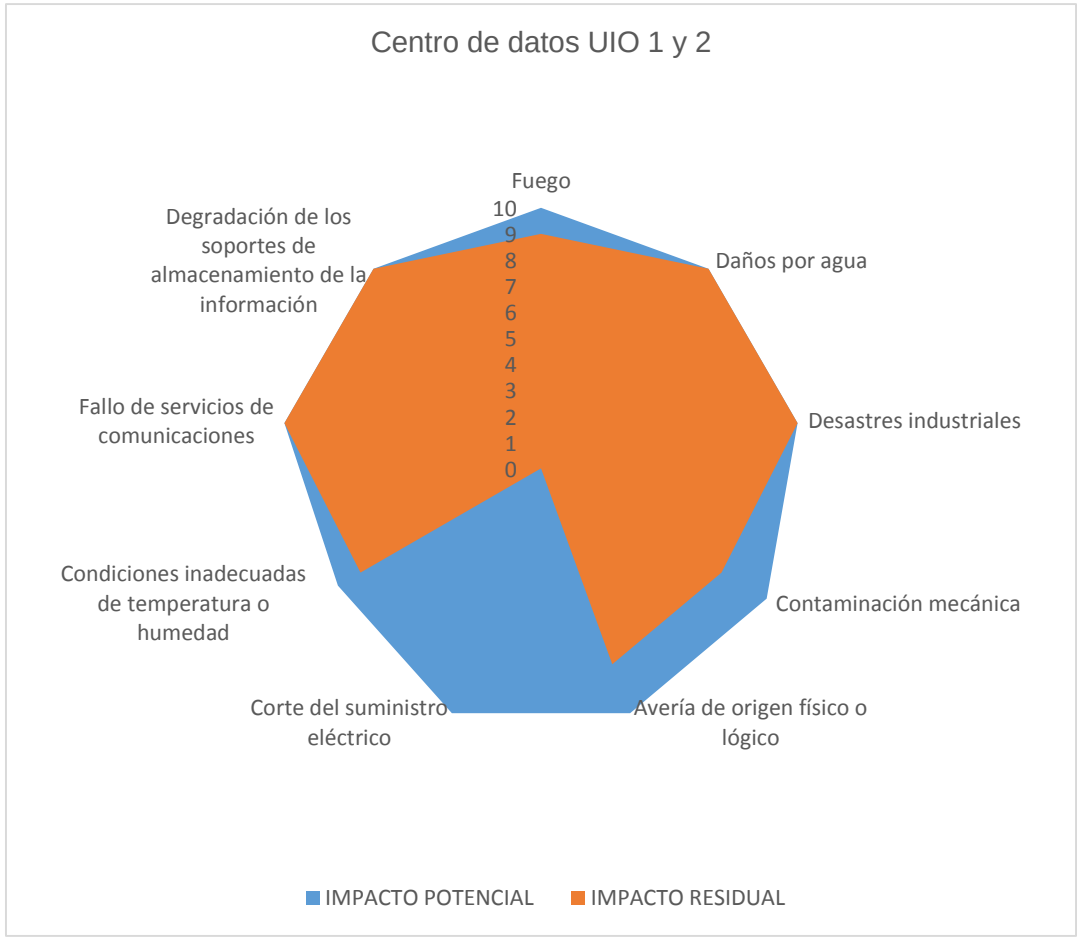
En el grafico se puede ver la diferencia entre el riesgo potencial y riesgo residual debido a la eficacia de las salvaguardas implementadas en el activo. Hay una diferencia mayor en la amenaza Fuego, ya que la eficacia de la salvaguarda es alta. En la amenaza Daños por agua, la eficacia de la salvaguarda es muy baja, por lo que el Riesgo Residual sigue siendo alto

INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR DESASTRES DE ORIGEN INDUSTRIAL

En el Grafico se muestra la diferencia entre Impacto Potencial y residual en función de la eficacia de la salvaguarda.

En las Amenazas:
Fallo de servicios de comunicaciones
Degradación de los soportes de almacenamiento de la información
Daños por agua
Que no tienen implementada una salvaguarda, el punto del Impacto Potencial y el Impacto Residual es el mismo

Las amenazas:
Condiciones inadecuadas de temperatura o humedad
Contaminación mecánica
Avería de origen físico o lógico
Fuego
Que tienen implementadas salvaguardas aunque no eficaces al 100%, el Impacto Residual es menor con respecto al Impacto Potencial.
En el caso de la amenaza:
Corte de Suministro Eléctrico, tiene una salvaguarda 100% Eficaz por tal razón el Impacto es Despreciable



Estimación de Impacto por Desastres de Origen Industrial

INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR DESASTRES DE ORIGEN INDUSTRIAL

En el Grafico se muestra la diferencia entre Riesgo Potencial y residual en función de la eficacia de la salvaguarda.

En las Amenazas:

Fallo de servicios de comunicaciones

Degradación de los soportes de almacenamiento de la información

Daños por agua

Que no tienen implementada una salvaguarda, el punto del Impacto Potencial y el Impacto Residual es el mismo, por tanto el Riesgo Potencial y Residual esta también el mismo

Las amenazas:

Condiciones inadecuadas de temperatura o humedad

Contaminación mecánica

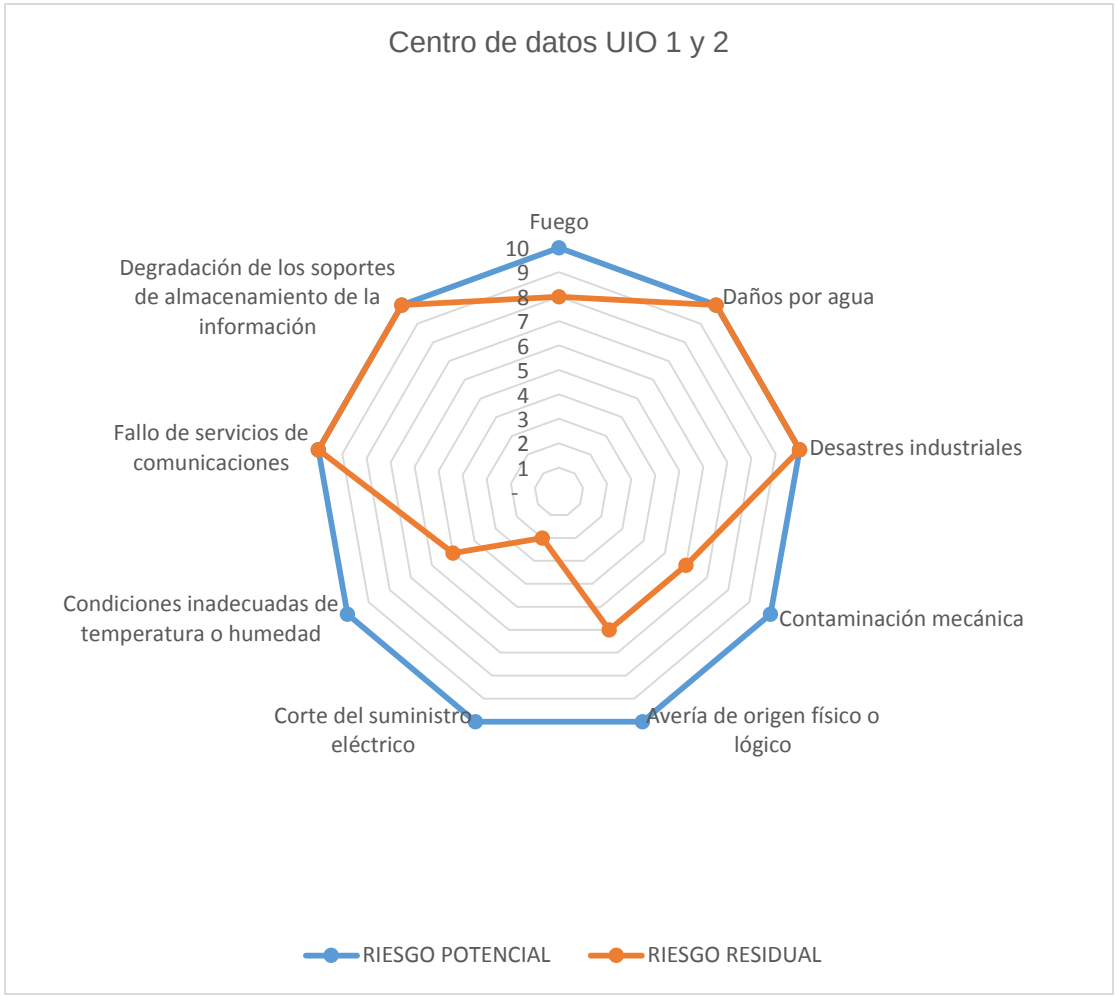
Avería de origen físico o lógico

Fuego

Que tienen implementadas salvaguardas aunque no eficaces al 100%, el Impacto Residual es menor con respecto al Impacto Potencial, por tanto el Riesgo Residual también es menor con respecto al Riesgo Potencial.

En el caso de la amenaza

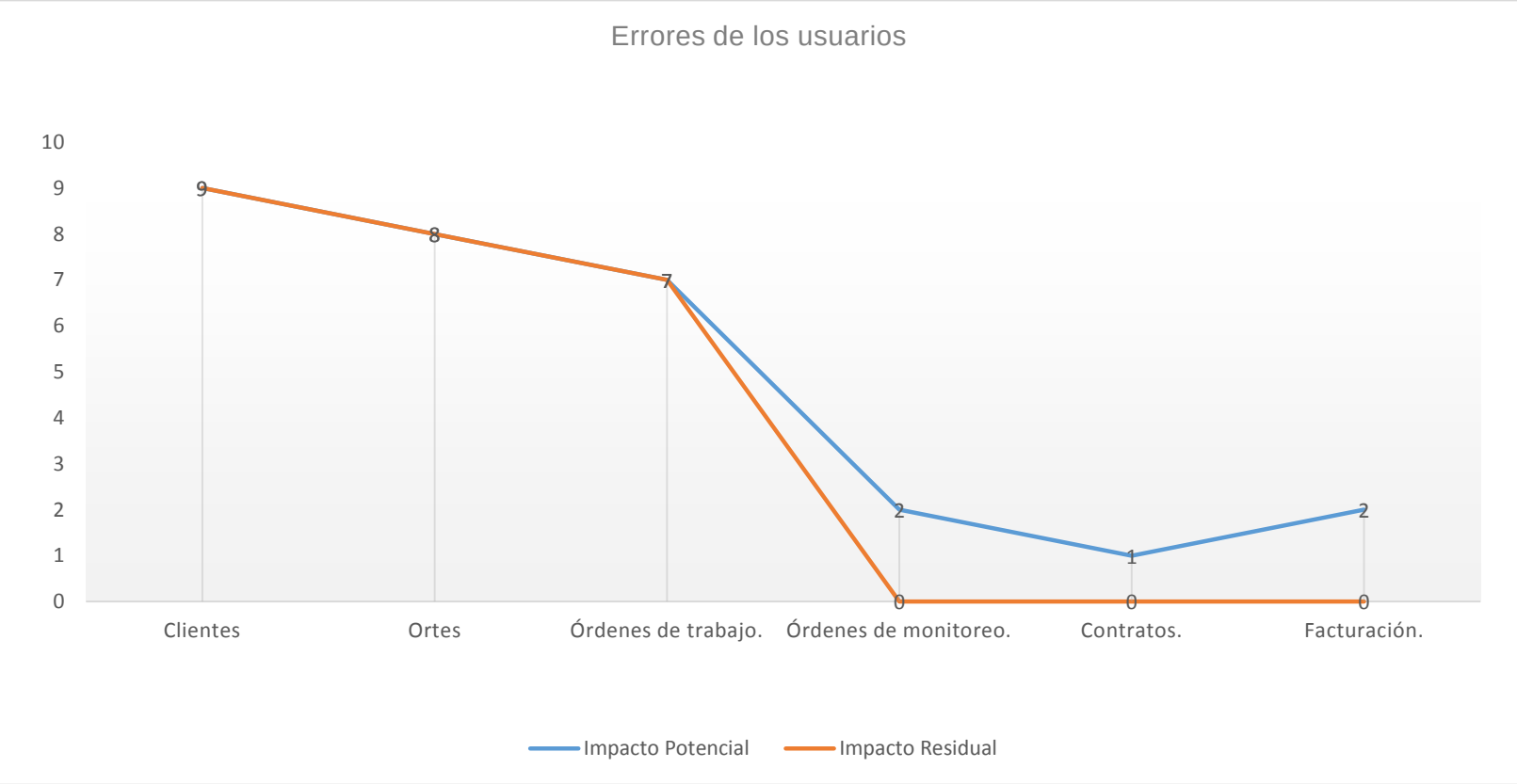
Corte de Suministro Eléctrico, tiene una salvaguarda 100% Eficaz por tal razón el Impacto Residual es Despreciable al igual que el Riesgo Residual, como se puede ver en el gráfico:



Estimación del Riesgo por Desastres de Origen Industrial

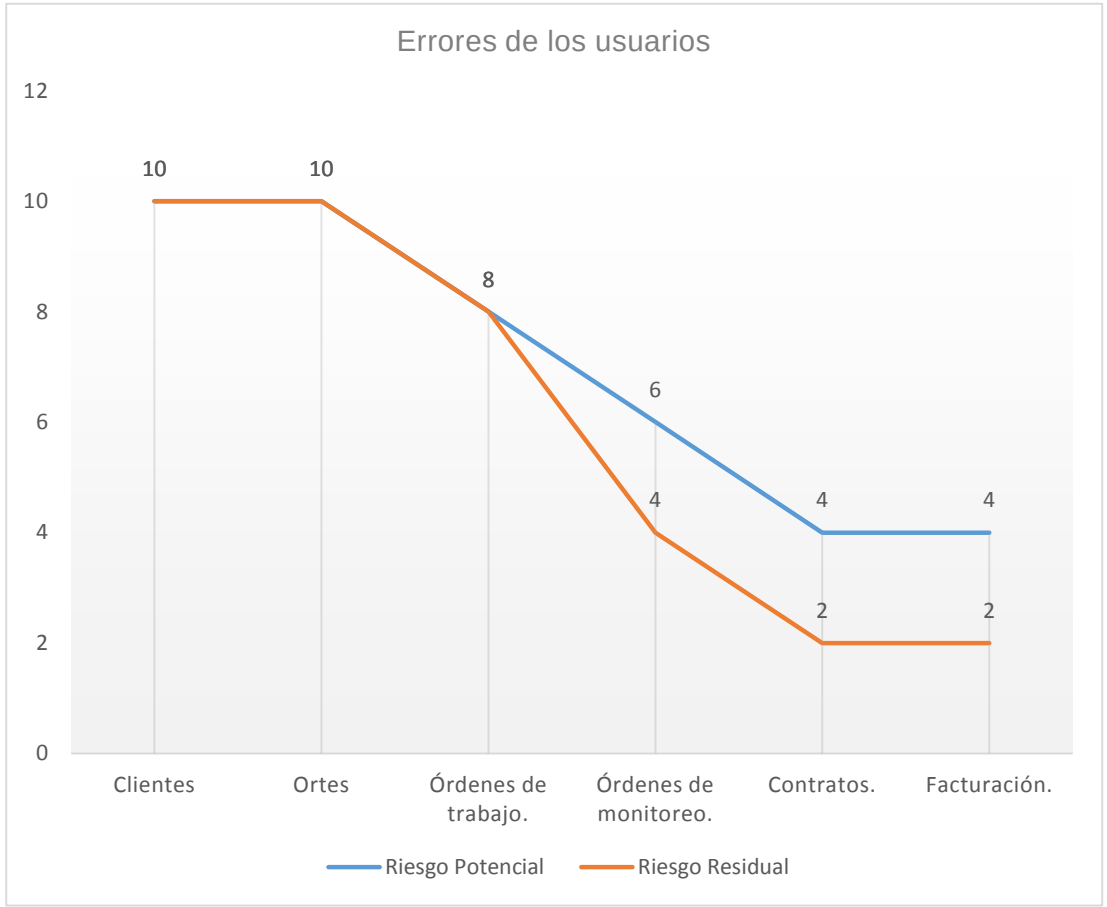
INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR ERRORES DE LOS USUARIOS

En el grafico se puede notar que el Impacto Residual baja a 0 en los activos Ordenes de Monitoreo, Contratos y Facturación, debido a la eficacia de las Salvaguardas.



INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR ERRORES DE LOS USUARIOS

En el grafico se puede notar que el Riesgo Residual baja en los activos Ordenes de Monitoreo, Contratos y Facturación, debido a la eficacia de las Salvaguardas.



INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR ERRORES Y FALLOS NO INTENCIONADOS

Para las amenazas Errores del administrador, Errores de monitorización (log) y Errores de configuración, que afectan a los activos: Sistema de administración y seguridades, Clientes, Contratos y Transacciones contables, no existe una salvaguarda implementada, por lo que en grafico que puede ver que el Punto del Impacto Potencial y el Impacto Residual es el mismo.


ERRORES Y FALLOS NO INTENCIONADOS
Sistema de administración y seguridades.
Clientes
Contratos
Transacciones contables.
Sistema Administrativo Financiero.
Sistema Administración Tributaria.
Sistema de activos fijos.
Sistema de gestión humana
Sistema de evaluaciones
Sistema de administración de clientes
Accouting Interfase
Sistema de administración de seguridades
Posfix
CIFS
Sistema de control de mensajes.
Sistema de análisis de mensajes
10
9
8
7
6
5
4
3
2
1
0
IMPACTO POTENCIAL
IMPACTO RESIDUAL

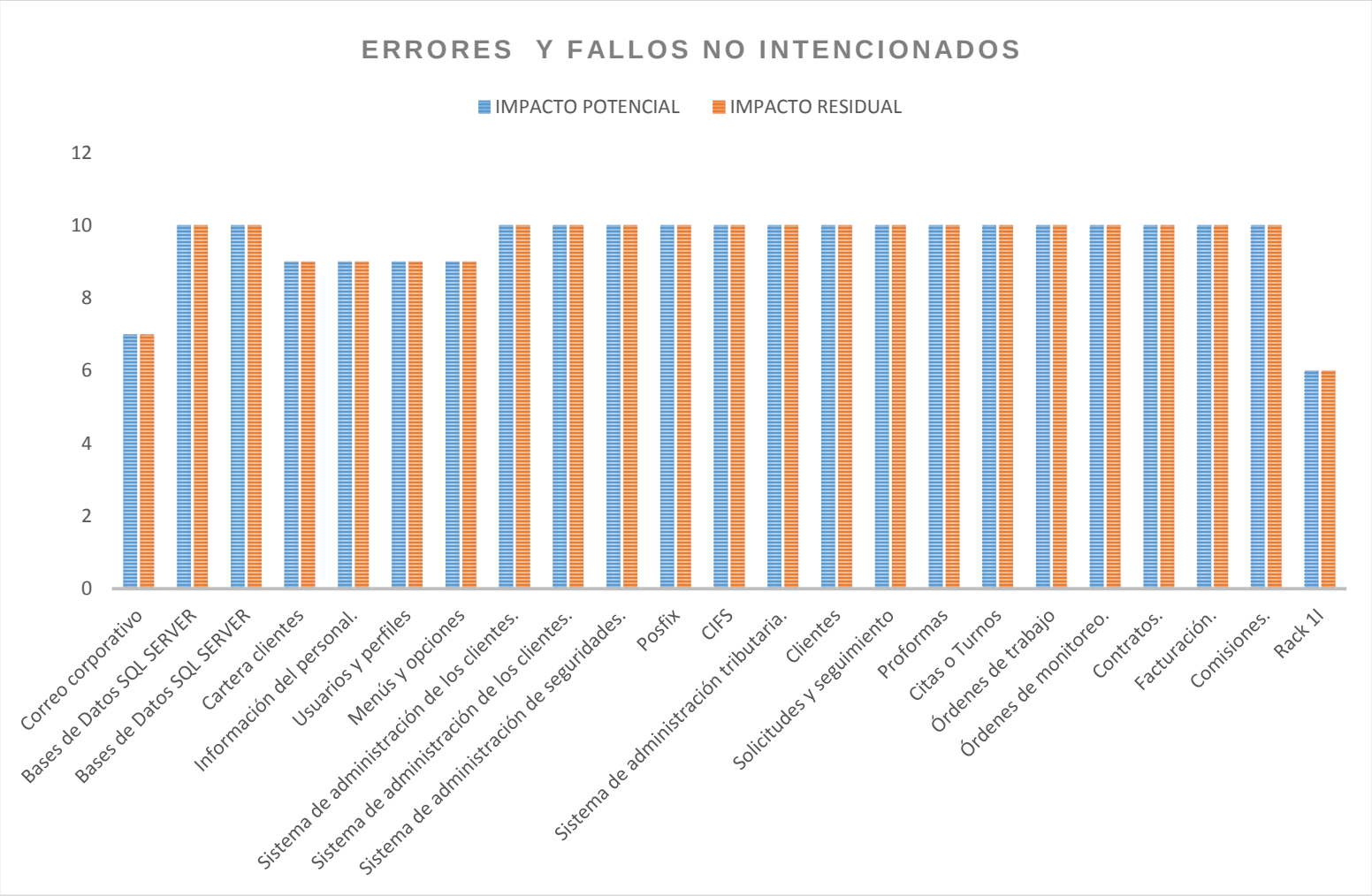
INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR ERRORES Y FALLOS NO INTENCIONADOS

Para las amenazas Errores del administrador, Errores de monitorización (log) y Errores de configuración, que afectan a los activos: Sistema de administración y seguridades, Clientes, Contratos y Transacciones contables, no existe una salvaguarda implementada, por lo que en grafico que puede ver que el Punto del Riesgo Potencial y el Riesgo Residual es el mismo

ERRORES Y FALLOS NO INTENCIONADOS

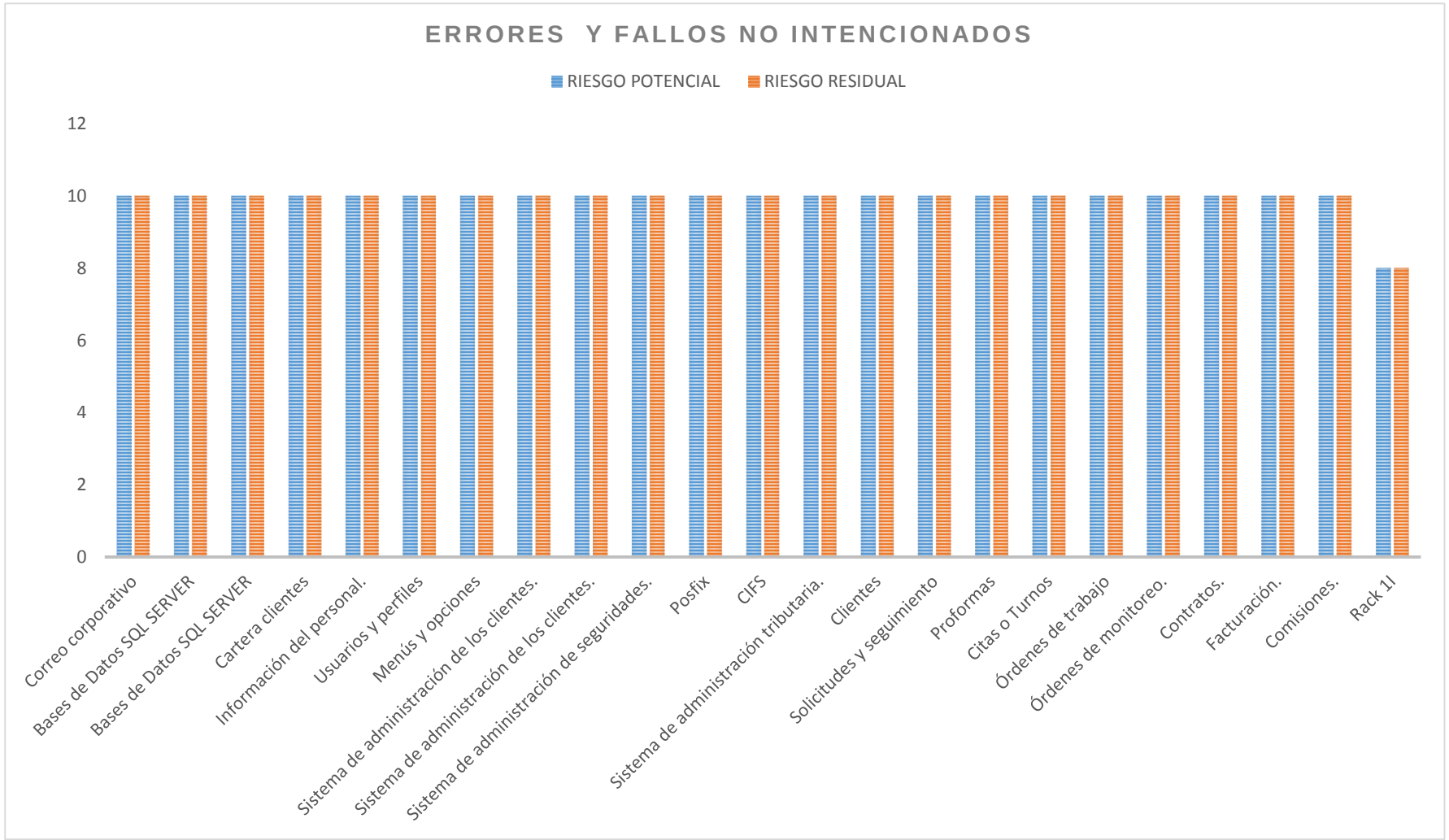
INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR ERRORES Y FALLOS NO INTENCIONADOS

El IMPACTO Potencial y Residual es el mismo.



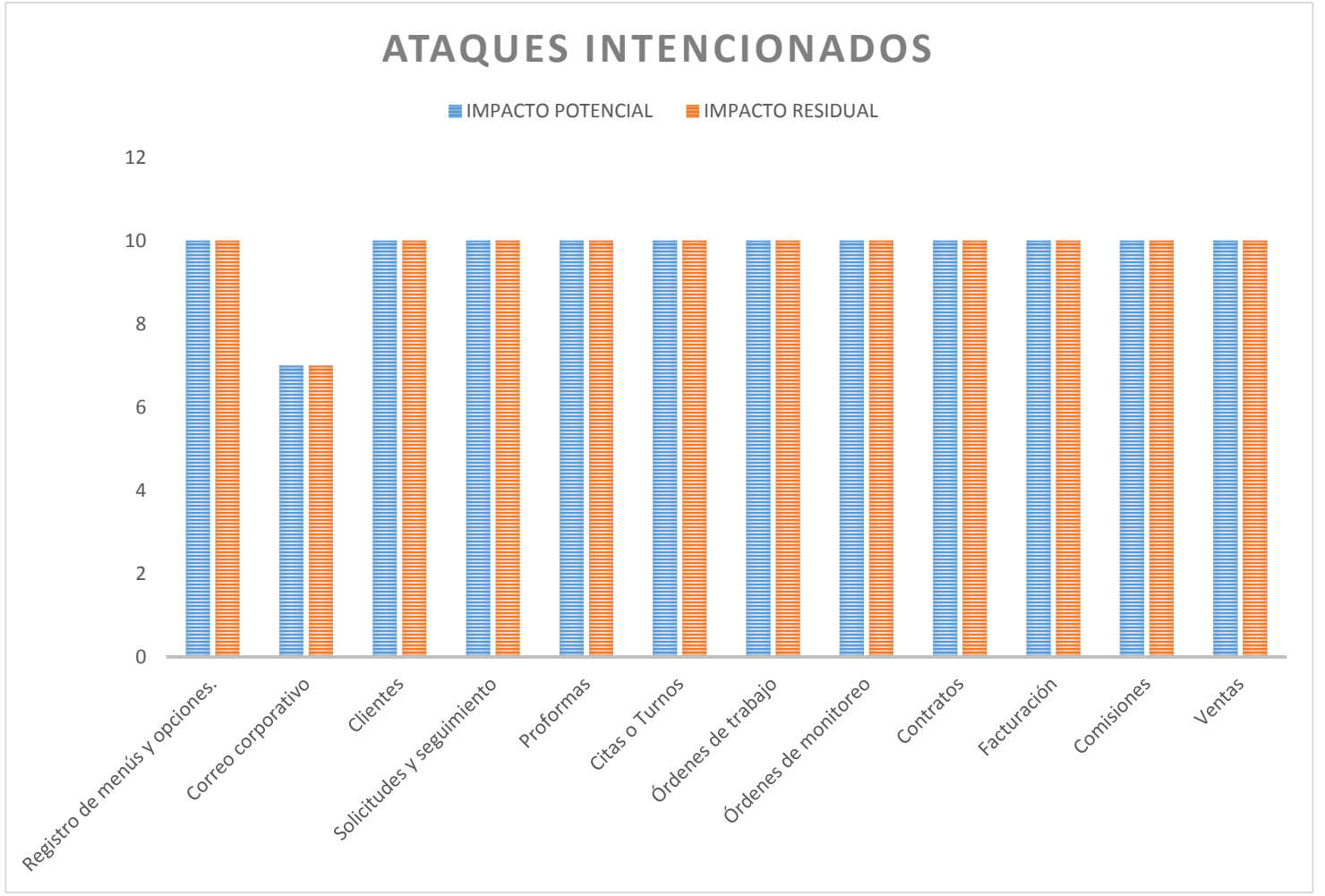
INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR ERRORES Y FALLOS NO INTENCIONADOS

El RIESGO Potencial y Residual es el mismo, debido a que estos activos no tienen salvaguardas implementadas



INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR ATAQUES INTENCIONADOS

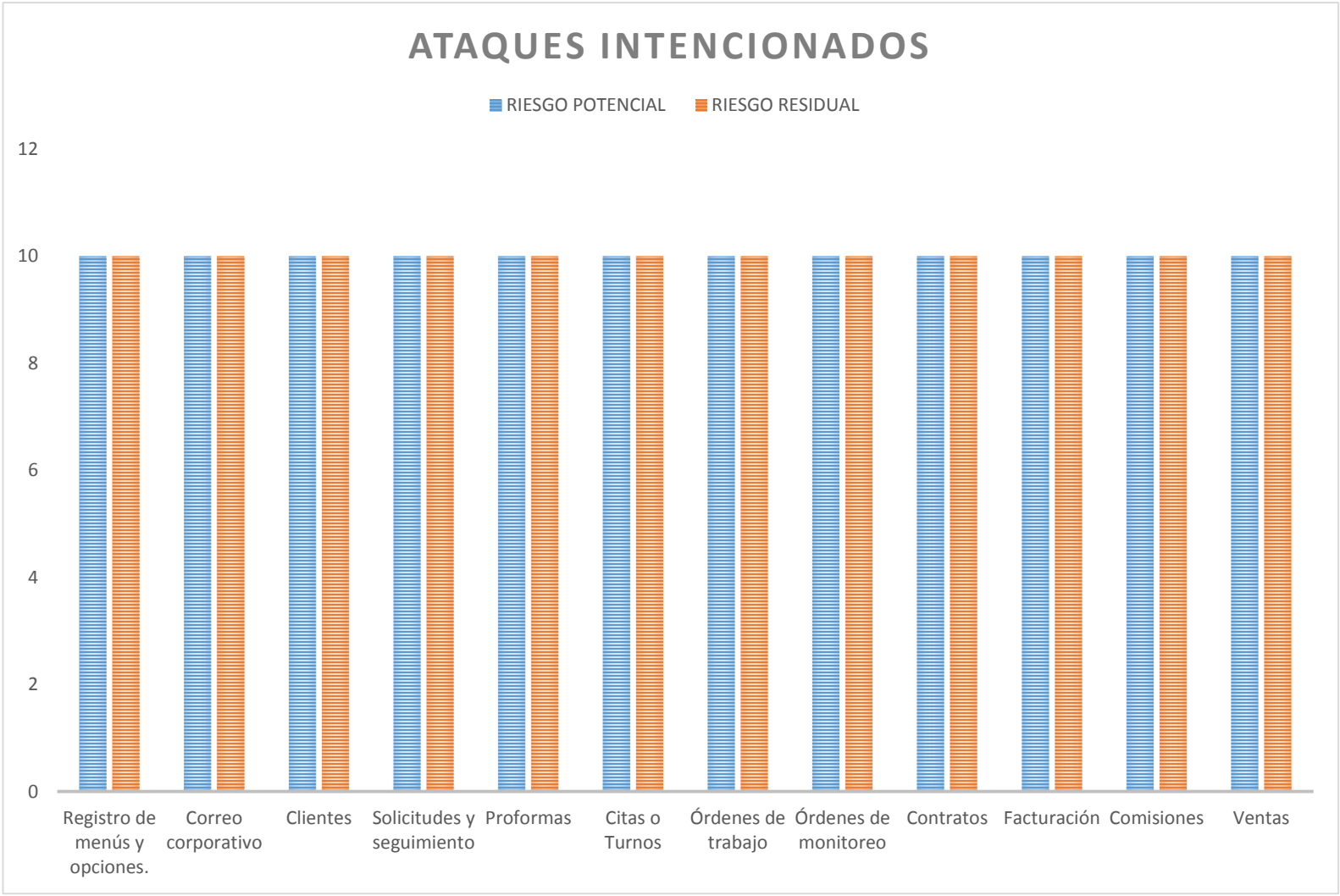
Ante las amenazas:
Suplantación de la identidad del usuario, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas
Abuso de privilegios de acceso, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas
Tienen salvaguardas implementadas para hacerles frente, pero su eficacia es Muy baja por lo que el Impacto residual es igual al impacto Potencial sobre los activos.
Ante las amenazas:
Manipulación de la configuración que afecta al activo: Registro de menús y opciones.
Alteración de secuencia, que afecta al activo: Correo corporativo
Y Acceso no autorizado, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas
No tienen salvaguardas para hacerles frente, debido a esto el Impacto Potencial y Residual son iguales.
El grafico se muestra que el Impacto Potencial y el Impacto Residual son iguales ante las amenazas indicadas anteriormente.


ATAQUES INTENCIONADOS
IMPACTO POTENCIAL
IMPACTO RESIDUAL
12
10
8
6
4
2
0
Registro de menús y opciones.
Correo corporativo
Clientes
Solicitudes y seguimiento
Proformas
Citas o Turnos
Órdenes de trabajo
Órdenes de monitoreo
Contratos
Facturación
Comisiones
Ventas

INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR ATAQUES INTENCIONADOS

Ante las amenazas:
Suplantación de la identidad del usuario, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas
Abuso de privilegios de acceso, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas
Tienen salvaguardas implementadas para hacerles frente, pero su eficacia es Muy baja por lo que el RIESGO residual es igual al RIESGO Potencial sobre los activos.
Ante las amenazas:
Manipulación de la configuración que afecta al activo: Registro de menús y opciones.
Alteración de secuencia, que afecta al activo: Correo corporativo
Y Acceso no autorizado, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas
No tienen salvaguardas para hacerles frente, debido a esto el RIESGO Potencial y Residual son iguales.

El gráfico se muestra que el Riesgo Potencial y el Riesgo Residual son iguales ante las amenazas indicadas anteriormente, en ambos tipos es un Riesgo Critico.


ATAQUES INTENCIONADOS
RIESGO POTENCIAL
RIESGO RESIDUAL
12
10
8
6
4
2
0
Registro de menús y opciones.
Correo corporativo
Clientes
Solicitudes y seguimiento
Proformas
Citas o Turnos
Órdenes de trabajo
Órdenes de monitoreo
Contratos
Facturación
Comisiones
Ventas

INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR USO NO PREVISTO

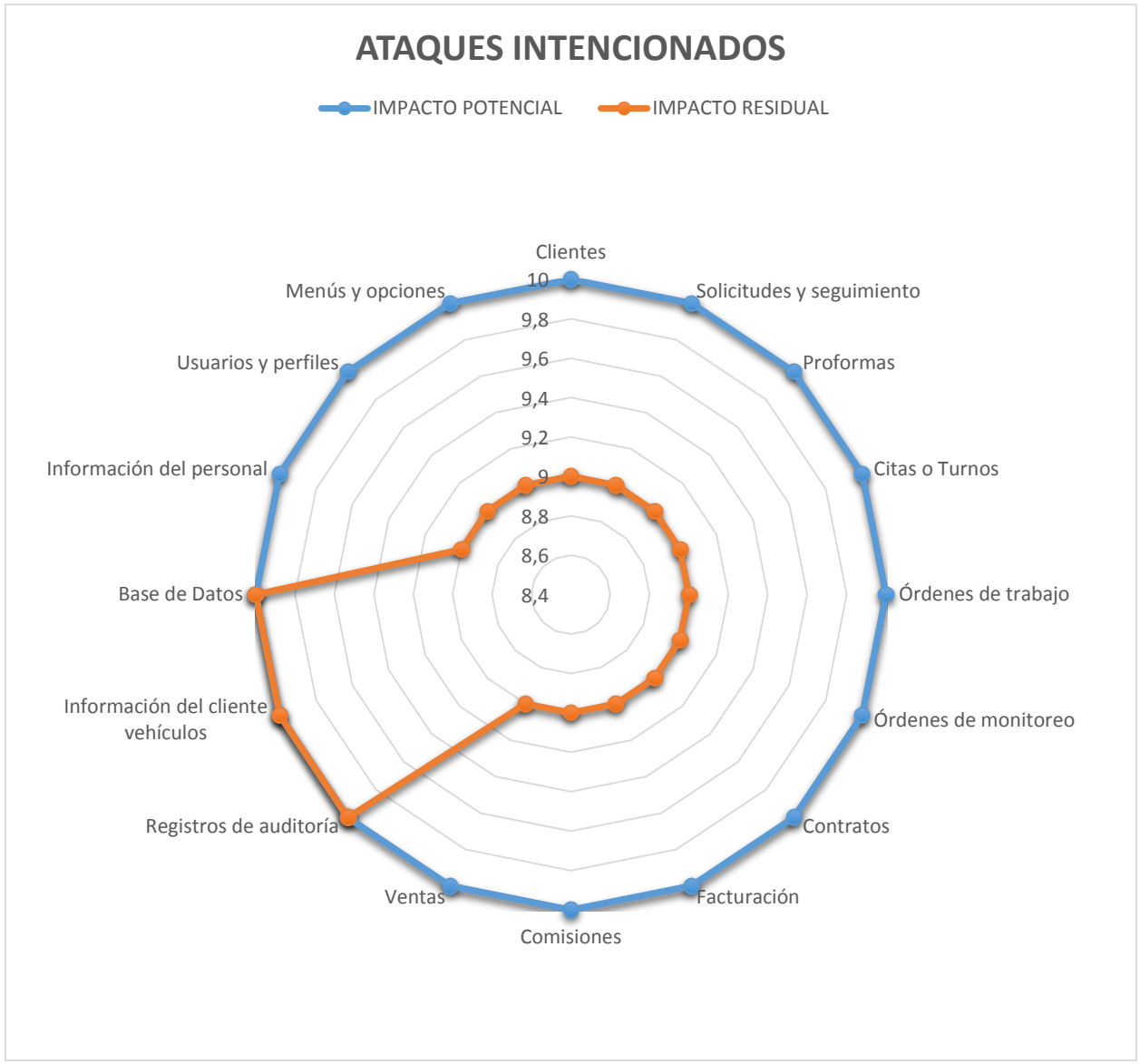
Ante la amenaza Uso no previsto, existe implementada una salvaguarda altamente eficaz para hacerle frente, por lo que el IMPACTO RESIDUAL se considera Despreciable sobre los activos con Respecto al IMPACTO POTENCIAL, esto se muestra claramente en el gráfico.

INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR USO NO PREVISTO

Ante la amenaza Uso no previsto, existe implementada una salvaguarda altamente eficaz para hacerle frente, por lo que el RIESGO RESIDUAL que tienen los activos en que se materialice la amenaza se considera Despreciable con Respecto al RIESGO POTENCIAL, esto se muestra claramente en el gráfico.

INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR ATAQUES INTENCIONADOS

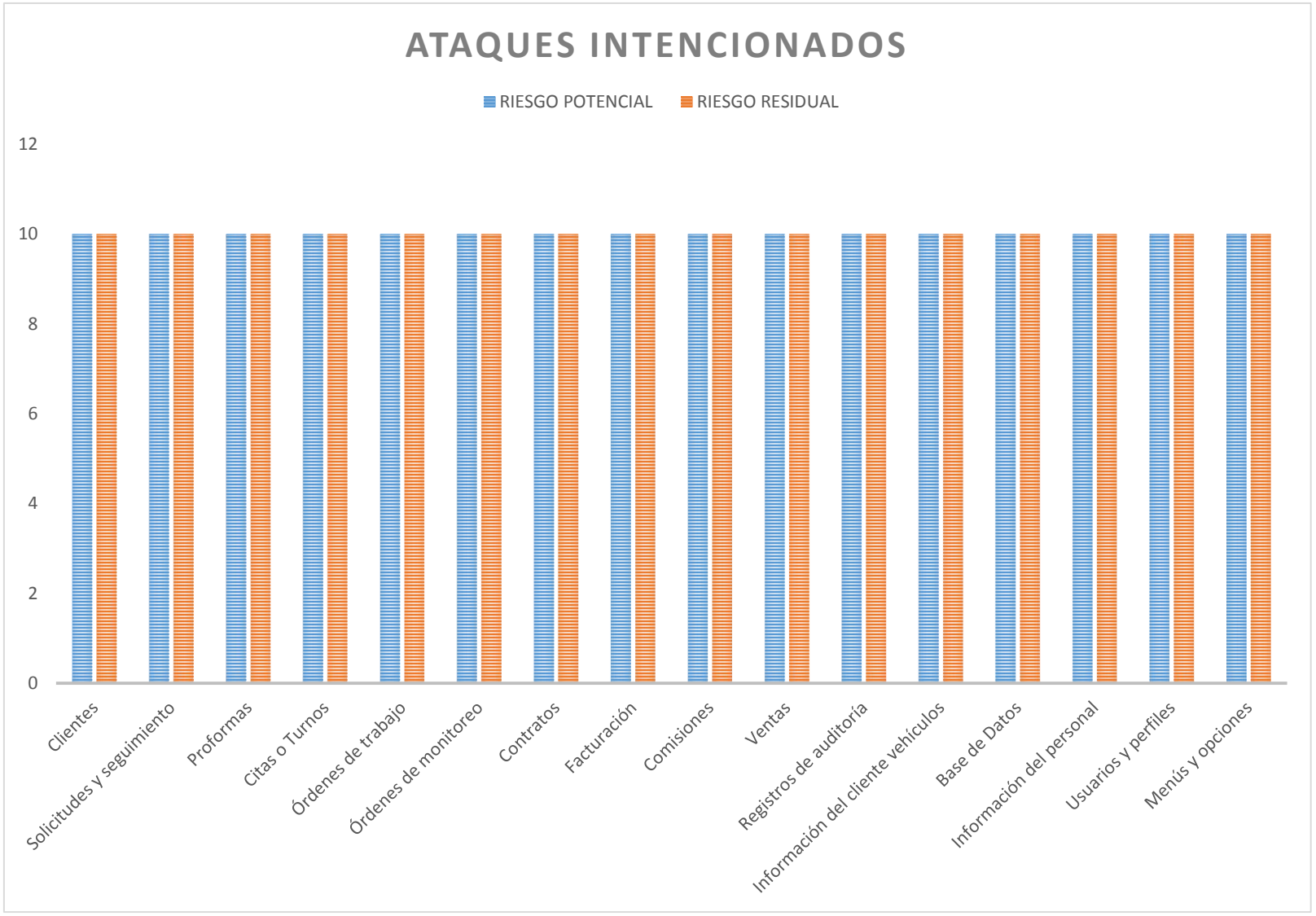
Ante la amenaza:
Repudio, que afecta los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, y Ventas.
Tiene una salvaguarda 60% eficaz, por lo que el IMPACTO RESIDUAL es menor con respecto al IMPACTO POTENCIAL.
Ante la amenaza:
Destrucción de información que afecta a las Bases de Datos, y **Modificación deliberada** que afecta a significativamente a Registros de auditoría, e Información del cliente vehículos, No tienen salvaguardas que se pueden hacer frente por lo Impacto Residual y el Impacto Potencial es el mismo sobre estos activos.


ATAQUES INTENCIONADOS
IMPACTO POTENCIAL
IMPACTO RESIDUAL
Clientes
Solicitudes y seguimiento
Proformas
Citas o Turnos
Órdenes de trabajo
Órdenes de monitoreo
Contratos
Facturación
Comisiones
Ventas
Registros de auditoría
Información del cliente vehículos
Base de Datos
Información del personal
Usuarios y perfiles
Menús y opciones
10
9,8
9,6
9,4
9,2
9
8,8
8,6
8,4

INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR ATAQUES INTENCIONADOS

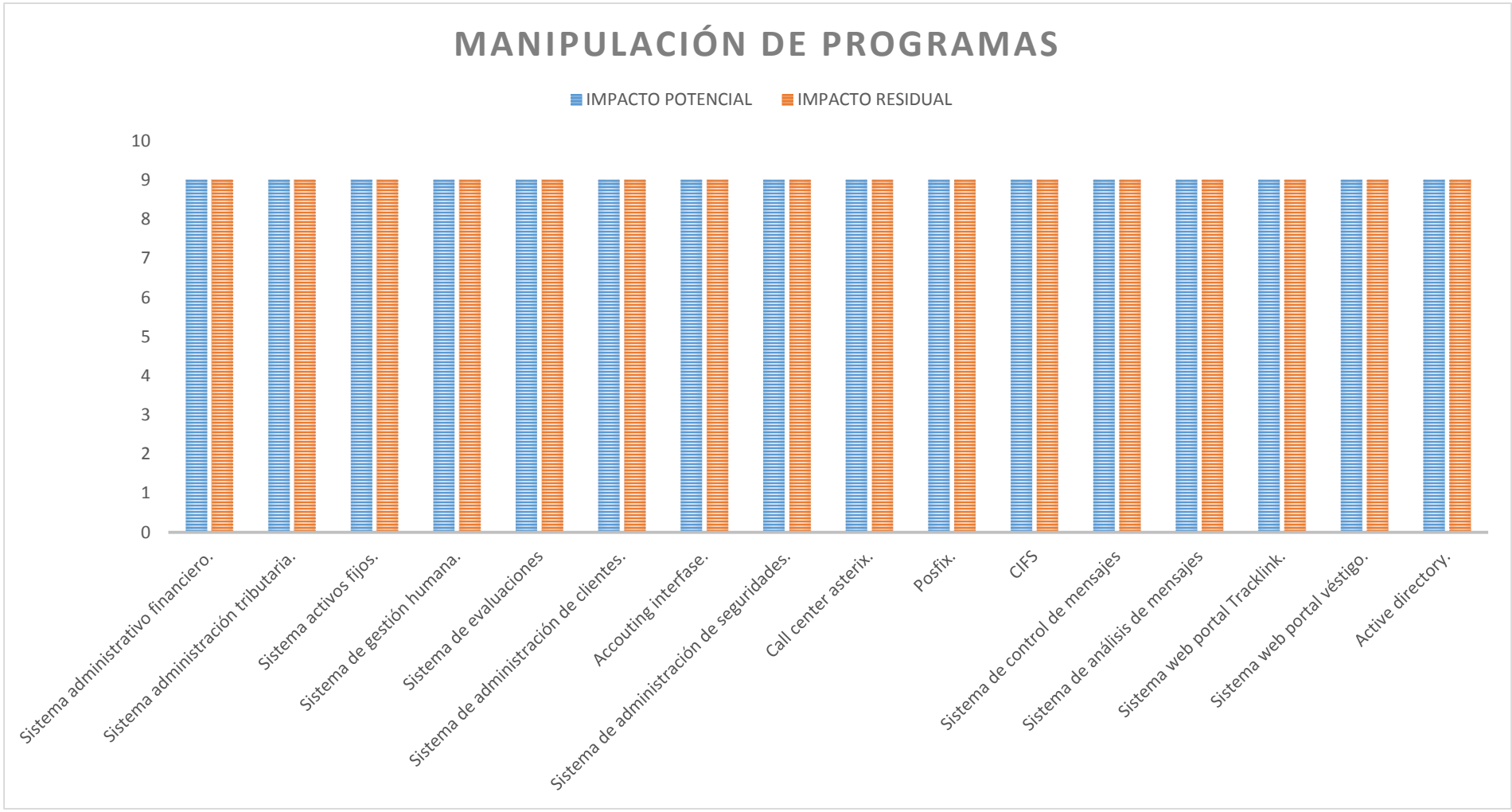
Ante la amenaza:
Repudio, que afecta los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, y Ventas.
Tiene una salvaguarda 60% eficaz, por lo que el impacto residual es menor con respecto al Impacto Potencial, pero no lo significativamente para poner disminuir el Riesgo, por lo que el Riesgo Potencial y Residual son iguales, estos activos tienen un Riesgo Critico.

Ante la amenaza:
Destrucción de información que afecta a las Bases de Datos, y **Modificación deliberada** que afecta a significativamente a Registros de auditoría, e Información del cliente vehículos, No tienen salvaguardas que se pueden hacer frente por lo Impacto Residual y el Impacto Potencial es el mismo sobre estos activos, y también tienen un Riesgo Critico.


ATAQUES INTENCIONADOS
RIESGO POTENCIAL
RIESGO RESIDUAL
12
10
8
6
4
2
0
Clientes
Solicitudes y seguimiento
Proformas
Citas o Turnos
Órdenes de trabajo
Órdenes de monitoreo
Contratos
Facturación
Comisiones
Ventas
Registros de auditoría
Información del cliente vehículos
Base de Datos
Información del personal
Usuarios y perfiles
Menús y opciones

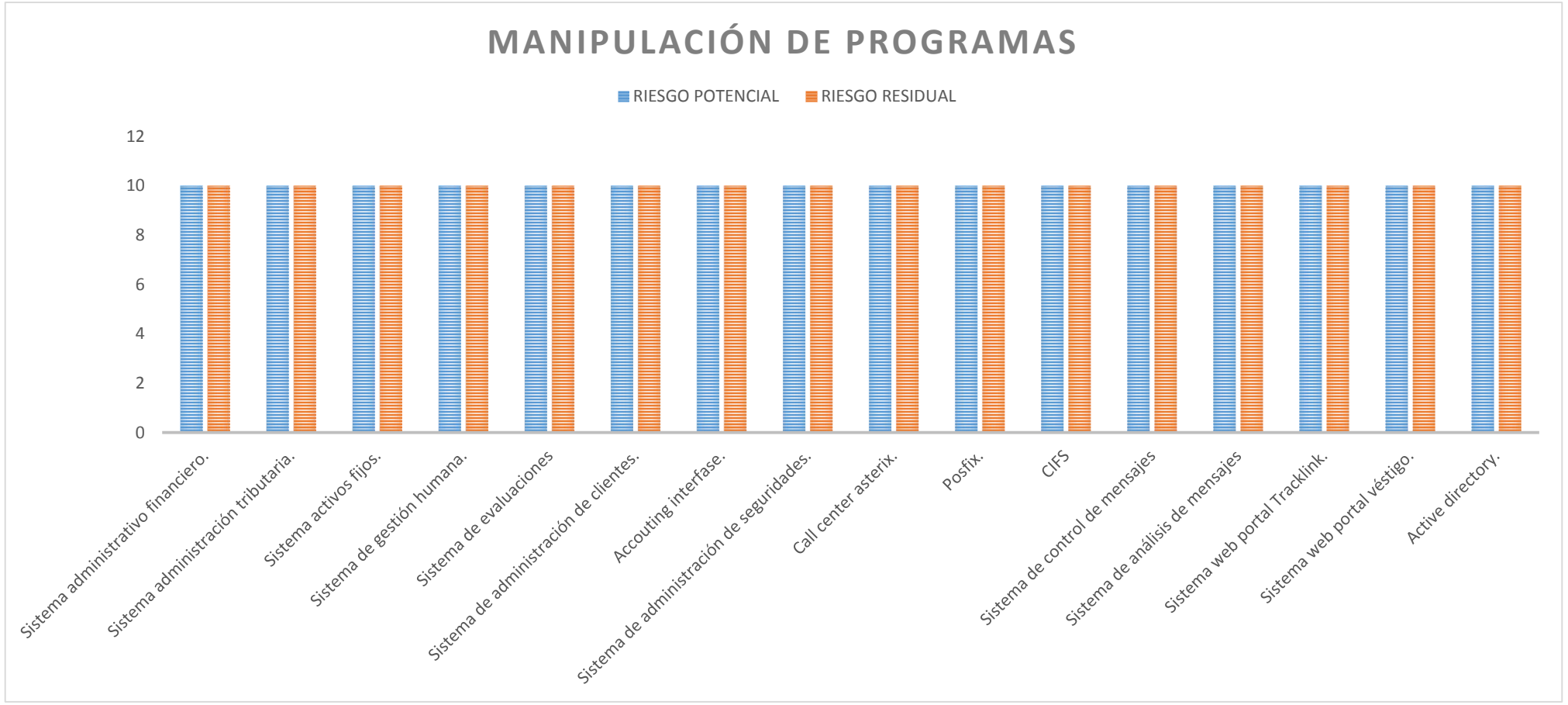
INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR MANIPULACION DE PROGRAMAS

Ante la amenaza:
Manipulación de programas, hay una salvaguarda para hacerle frente pero eficazmente muy baja, por lo que el Impacto sobre los activos tanto RESIDUAL como POTENCIAL, es el mismo.
En el grafico se muestra la continuidad del IMPACTO


MANIPULACIÓN DE PROGRAMAS
IMPACTO POTENCIAL
IMPACTO RESIDUAL
10
9
8
7
6
5
4
3
2
1
0
Sistema administrativo financiero.
Sistema administración tributaria.
Sistema activos fijos.
Sistema de gestión humana.
Sistema de evaluaciones
Sistema de administración de clientes.
Accouting interfase.
Sistema de administración de seguridades.
Call center asterix.
Posfix.
CIFS
Sistema de control de mensajes
Sistema de análisis de mensajes
Sistema web portal Tracklink.
Sistema web portal vestigo.
Active directory.

INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR MANIPULACION DE PROGRAMAS

Ante la amenaza:
Manipulación de programas, hay una salvaguarda para hacerle frente pero eficazmente muy baja, por lo que el RIESGO sobre los activos tanto RESIDUAL como POTENCIAL, es el mismo.
En el grafico se muestra la continuidad del RIESGO


MANIPULACIÓN DE PROGRAMAS
RIESGO POTENCIAL
RIESGO RESIDUAL
12
10
8
6
4
2
0
Sistema administrativo financiero.
Sistema administración tributaria.
Sistema activos fijos.
Sistema de gestión humana.
Sistema de evaluaciones
Sistema de administración de clientes.
Accouting interfase.
Sistema de administración de seguridades.
Call center asterix.
Posfix.
CIFS
Sistema de control de mensajes
Sistema de análisis de mensajes
Sistema web portal Tracklink.
Sistema web portal véstigo.
Active directory.

CONCLUSIONES

- Al finalizar el análisis de riesgos utilizando Magerit como metodología de análisis de Riesgos, se determinaron vulnerabilidades en el Sistema de información de la empresa, que deben ser atendidas oportunamente, ya que la mayoría de activos están con Riesgo Critico y con Impacto Muy Alto.

- Hacer un análisis de riesgos es esencial en los sistemas de información, ya que estos siempre están expuestos a amenazas.

- La Metodología de Análisis de Riesgos de Sistemas de Información – MAGERIT, junto con los Objetivos de Control para la Tecnología de la Información COBIT 5, contribuye a reducir las amenazas y brechas existentes entre los objetivos del negocio y aspectos técnicos de los Sistemas de Información

- El hacer una Análisis de Riesgos permite detectar la situación real de la compañía.

RECOMENDACIONES

- Concientizar a los directivos de la compañía la importancia de ejecutar una Gestión de los Riesgos encontrados, los mismos que si no son atendidos oportunamente se van a tener consecuencias No deseadas.

- Promover en el personal de la empresa, la toma de conciencia sobre el manejo de los riesgos

- Tomar las medidas de Seguridad y aplicar los objetivos de control que mitiguen el riesgo existente