LOGO	MATRIZ DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS PARA DATOS PERSONALES	VERSIÓN:	1
		FECHA CREACIÓN:	julio de 2018
		FECHA ACTUALIZACIÓN:	julio de 2018

Finalidad de la matriz:

La presente matriz esta diseñada según los requisitos de la Norma Integrada, y tiene como finalidad evaluar y tratar los riesgos identificados a los que están expuestos los datos personales, a raíz del contexto de la organización.

Secuencia del análisis:

El análisis consta de la siguiente secuencia:
1. Identificación de los riesgos, teniendo en cuenta el análisis del contexto de la empresa.
2. Análisis de los riesgos encontrados, hallando en nivel del riesgo.
3. Valoración de los riesgos, determinando si el riesgo es aceptable según el criterio establecido de aceptabilidad.
4. Gestión de los riesgos identificados, hallando el valor del riesgo residual.
5. Valoración de los riesgos residuales, determinando determinando la frecuencia de seguimiento a realizar para cada riesgo residual.
6. Establecer el seguimiento y gestión de los riesgos.
7. Evaluar el desemèño de la gestión realizada.
NOTA. Para mayor información de la metodología y consulta de definiciones, remitirse a los numerales 3.3.11 Evaluación de los riesgos, 3.3.12 Tratamiento de los riesgos, y 3.3.13 Evaluación del desempeño., en el documento del diseño del S.I.G.

MATRIZ DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS PARA DATOS PERSONALES

EVALUACIÓN DEL RIESGO											TRATAMIENTO DEL RIESGO										RESPONSABLE	EVALUACIÓN DEL DESEMPEÑO (DESCRIBIR PERIODO DEL ANÁLISIS)					
IDENTIFICACIÓN DE RIESGOS				ANÁLISIS DE RIESGOS					VALORACIÓN DEL RIESGO			GESTIÓN DE LOS RIESGOS IDENTIFICADOS							VALORACIÓN DEL RIESGO RESIDUAL					INDICADOR DE GESTIÓN: % RIESGO MEJORADO		(DESCRIBIR PERIODO ACTUAL DEL ANÁLISIS)	SEGUIMIENTO DEL RIESGO PERIODOS ANTERIORES		
No. RIESGO	FUENTE	AMENAZA	RIESGOS	CONTROLES EXISTENTES	DESCRIPCIÓN DE CONTROLES EXISTENTES	PROBABILIDAD	NIVEL DE CONSECUENCIA	NIVEL DE RIESGO	VALORACIÓN CUALITATIVA DEL RIESGO	ACEPTABILIDAD DEL RIESGO	DECISIÓN DEL RIESGO	MEDIDAS DE CONTROL PROPUESTAS	RECURSOS NECESARIOS	FRECUENCIA DE SEGUIMIENTO DE LA IMPLEMENTACIÓN DE LAS MEDIDAS DE CONTROL	SE HAN IMPLEMENTADO LAS MEDIDAS DE CONTROL	NIVEL DE CONSECUENCIA TRAS IMPLANTACIÓN DE LAS MEDIDAS PROPUESTAS	PROBABILIDAD TRAS IMPLANTACIÓN DE LAS MEDIDAS PROPUESTAS	NIVEL DE RIESGO RESIDUAL	CRITERIO DEL RIESGO RESIDUAL	ACEPTABILIDAD DEL RIESGO RESIDUAL	DECISIÓN DEL RIESGO RESIDUAL	FRECUENCIA DE SEGUIMIENTO DEL RIESGO RESIDUAL		$\left(\frac{Nivel\ de\ Riesgo - Nivel\ de\ Riesgo\ Residual}{Nivel\ de\ Riesgo} x\ 100\%\right)$	META %	OBSERVACIONES Y/O SEGUIMIENTO DEL RIESGO	% PROMEDIO DEL INDICADOR DE GESTIÓN	OBSERVACIONES Y/O SEGUIMIENTO DEL RIESGO (DESCRIBIR PERIODO DEL ANÁLISIS)	ANÁLISIS FINAL (TENIENDO EN CUENTA PERIODO ACTUAL Y PERIODOS ANTERIORES DEL ANÁLISIS)
1	Externo	Ataque cibernético	Robo de información	No	-	2	3	6	Crítico	No	Realizar opciones para el tratamiento del riesgo con urgencia	Compra de antivirus icenciado, restringir le acceso a determinadas páginas.	Se requiere de recursos económicos no elevados.	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
2	Externo	Ataque cibernético	Suplantación de identidad	No	-	2	3	6	Crítico	No	Realizar opciones para el tratamiento del riesgo con urgencia	Compra de antivirus icenciado, restringir le acceso a determinadas páginas.	Se requiere de recursos económicos no elevados.	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
3	Externo	Ataque cibernético	Pérdida de información	No	-	2	3	6	Crítico	No	Realizar opciones para el tratamiento del riesgo con urgencia	Compra de antivirus icenciado, restringir le acceso a determinadas páginas.	Se requiere de recursos económicos no elevados.	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
4	Interno	Fallos eléctricos	Pérdida de información	No	-	1	2	2	Significativo	No	Realizar opciones para el tratamiento del riesgo	Realizar backup en disco duro externo, con acceso restringido a personal no autorizado al mismo	Se requiere de recursos económicos no elevados.	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
5	Interno	Falta de conocimiento de normatividad aplicable	Pérdidas económicas por el Incumplimiento de requisitos legales	No	-	3	3	9	Crítico	No	Realizar opciones para el tratamiento del riesgo con urgencia	Capacitación con respecto a la normatividad aplicable y sus requisitos, tanto a los directivos, como a las personas destinadas para desempeñar los roles específicos del sistema. Si es necesario, buscar asesoría jurídica.	Se requiere de recursos humanos principalmente.	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
6	Interno	Falta de conocimiento de normatividad aplicable	Pérdida de clientes por sanciones	No	-	2	3	6	Crítico	No	Realizar opciones para el tratamiento del riesgo con urgencia	Capacitación con respecto a la normatividad aplicable y sus requisitos, tanto a los directivos, como a las personas destinadas para desempeñar los roles específicos del sistema. Si es necesario, buscar asesoría.	Se requiere de recursos humanos principalmente.	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
7	Interno	Acceso a los datos digitales sin restricciones	Uso ilegítimo de la información	No	-	1	3	3	Significativo	No	Realizar opciones para el tratamiento del riesgo	Asignar una carpeta con acceso restringido (clave) a la misma, en la que contenga los documentos con datos del inventario de activos del S.I.G.	Recursos humanos (encargado del tratamiento) Hardware (computador asignado)	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
8	Interno	Acceso a los datos digitales sin restricciones	Alteración de la información	No	-	2	3	6	Crítico	No	Realizar opciones para el tratamiento del riesgo con urgencia	Asignar una carpeta con acceso restringido (clave) a la misma, en la que contenga los documentos con datos del inventario de activos del S.I.G.	Recursos humanos (encargado del tratamiento) Hardware (computador asignado)	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
9	Interno	Acceso a los datos físicos sin restricciones	Pérdida de la información	No	-	1	3	3	Significativo	No	Realizar opciones para el tratamiento del riesgo	Asignar una carpeta con acceso restringido a la misma (solamente la manejara el encargado del tratamiento),en la que contenga los documentos que contenga datos del inventario de activos del S.I.G.	Recursos humanos (encargado del tratamiento) Carpeta o AZ	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
10	Interno	No se tiene autorización por parte de los titulares, para el tratamiento de los datos personales	Demanda por parte del titular y sanciones por parte de la S.I.C.	No	-	2	3	6	Crítico	No	Realizar opciones para el tratamiento del riesgo con urgencia	Solicitar autorización por parte de los titulares de los datos, de acuerdo a lo establecido en la legislación vigente.	Recursos humanos (encargado del tratamiento)	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
11	Externo	Entrega de información en original a entidad o persona externa.	Acceso incontrolado de personal no autorizado a la información	No	-	3	3	9	Crítico	No	Realizar opciones para el tratamiento del riesgo con urgencia	Solicitar y tener toda la información en la empresa, y realizar acuerdo de tratamiento de datos que se le entreguen de manera digital, que garantice cumplimiento de la política.	Recursos humanos (encargado del tratamiento)	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
12	Externo	Entrega de información en original a entidad o persona externa.	Pérdida de información	No	-	3	3	9	Crítico	No	Realizar opciones para el tratamiento del riesgo con urgencia	Solicitar y tener toda la información en la empresa, y realizar acuerdo de tratamiento de datos que se le entreguen de manera digital, que garantice cumplimiento de la política.	Recursos humanos (encargado del tratamiento)	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
13	Externo	Entrega de información en original a entidad o persona externa.	Suplantación de identidad	No	-	2	3	6	Crítico	No	Realizar opciones para el tratamiento del riesgo con urgencia	Solicitar y tener toda la información en la empresa, y realizar acuerdo de tratamiento de datos que se le entreguen de manera digital, que garantice cumplimiento de la política.	Recursos humanos (encargado del tratamiento)	Mensual	No			0				Encargado del tratamiento de datos.	100%	80%				
								0										0					#¡DIV/0!	80%				