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

AGENCIA NACIONAL DE CONTRATACIÓN COLOMBIA COMPRA EFICIENTE

Marzo de 2019

Contenido

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

i) Introducción

El presente documento establece las acciones que Colombia Compra Eficiente ejecuta para tratar y gestionar los Riesgos de Privacidad y Seguridad de la Información. Cabe mencionar que el presente plan corresponde al cumplimiento de lo establecido en la ley 152 de 1994 y el artículo 74 de la ley 1474 de 2011. Además, se encuentra articulado con el plan de acción institucional anual de conformidad con el decreto 612 de 2018.

.

ii) Objetivo

El objetivo del presente documento es identificar actividades que ayuden al tratamiento efectivo de los riesgos de privacidad y seguridad de la información, las cuales se encuentran enmarcadas en el establecimiento del contexto, el tratamiento de los activos de información, identificación de amenazas y vulnerabilidades, consecuencias, evaluación de controles existentes, entre otros, lo anterior con el fin de preservar la Confidencialidad, Integridad y Disponibilidad de los Activos de Información de Colombia Compra Eficiente. El resultado de esta gestión se encontrará plasmado en la matriz de riesgos de la entidad.

iii) Definiciones

Activo de Información: toda aquella información que reside en medio electrónico o físico, que tiene un significado y valor para Colombia Compra Eficiente y, por ende, necesita ser protegida.
Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
Confidencialidad: principio de la Seguridad de la Información que busca asegurar que la información de Colombia Compra Eficiente sea accedida únicamente por personal autorizado (tanto interno como externo a Colombia Compra Eficiente), para suplir una necesidad legítima para la realización de sus funciones, con el fin de prevenir el uso o divulgación de la misma en forma no autorizada.
Contenedor de la Información: cualquier plataforma tecnológica o lugar físico que almacena, procesa, transmite un Activo de Información por cualquier lapso de tiempo o propósito.
Disponibilidad: principio de la Seguridad de la Información que busca asegurar que la información esté disponible cuando sea requerido por los procesos, servicios, ciudadanos y en general partícipes de los procesos de contratación alojados en las plataformas bajo responsabilidad de Colombia Compra Eficiente.
Integridad: principio de Seguridad de la Información que busca asegurar que la información esté protegida contra modificaciones no autorizadas para garantizar su consistencia, exactitud y completitud. Se debe garantizar la trazabilidad de la información.
Proceso: grupo de actividades relacionadas de manera lógica que, cuando se llevan a cabo, utilizan los recursos de Colombia Compra Eficiente para lograr resultados definitivos o transformar elementos de entrada, a través de una serie de actividades, en un producto o servicio.
Propietario del Activo (o de la Información): funcionario encargado de identificar y establecer el alcance y valor o criticidad de un Activo de Información, los requerimientos de seguridad del mismo y la comunicación de éstos a los custodios del Activo de Información.

Dueño del Proceso: funcionario de Colombia Compra Eficiente responsable del adecuado cumplimento de las actividades que conforman un proceso, y que están encaminadas a satisfacer una demanda tanto interna como externa a Colombia Compra Eficiente.
Riesgo Residual: Riesgo restante después de aplicar el tratamiento al Riesgo.
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. **Riesgos de seguridad digital:** Posibilidad Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas
Seguridad de la Información: Preservación de la Confidencialidad, Integridad y Disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas.
Vulnerabilidad: debilidad asociada al Contenedor de un Activo de Información y que puede ser explotada para materializar un Riesgo, causando incidentes no deseados que pueden dar lugar a la pérdida de Confidencialidad, Integridad o Disponibilidad de los Activos de Información.

iv) Gestión de Riesgos de Seguridad y Privacidad de la Información

La gestión de Riesgos de Seguridad y Privacidad de la Información del presente plan, obedece la estructura y etapas definidas en la "Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas" del Ministerio de Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de la Función Pública.
Además de tener en cuenta la política de administración de riesgos de Colombia Compra eficiente.

1.1 Identificación de los Contenedores o Activos de Información

En esta etapa se deben identificar los contendores y Activos de Información que se podrían ver afectados por la materialización de los Riesgos, tomando en cuenta la matriz de identificación de Activos, producto de la ejecución de lo establecido en la metodología de Activos de Información de Colombia Compra Eficiente.

La matriz de activos de información contiene las siguientes variables:

- Proceso en el que se encuentra la custodia y tratamiento del activo de información.
- Clasificación documental (Serie - Subserie)
- Descripción del Activo de Información
- Propietario del Activo
- Medio
- Físico/Electrónico
- Lugar de almacenamiento físico / Lugar de almacenamiento Electrónico

Además de lo establecido en ley de transparencia y acceso a la información pública, como lo es la aclaración de datos personales, idioma y formato entre otros; cabe mencionar que una adecuada identificación de los activos de información y su criticidad es el punto de partida para aplicar la metodología de riesgos adoptada y aprobada por la entidad.

El equipo de seguridad de la Información, proyecta realizar actualizaciones y seguimiento sobre la matriz de seguridad de la Información de manera semestral, con el fin de contar con un inventario de activos de información vigente

1.2 Identificación de las Amenazas

En esta etapa se realiza la identificación de las Amenazas que pueden tener los Contenedores o Activos de Información identificados anteriormente. Las Amenazas tienen el potencial de divulgar, dañar, modificar o eliminar los Activos de Información. Para la identificación de las Amenazas se puede usar la tabla de Amenazas Anexo B.

1.3 Identificación de controles existentes

Luego de Identificar las Amenazas, se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios. Adicionalmente, se debe revisar la efectividad de los controles.

Para la revisión de los controles existentes se debe tener en cuenta:

- Revisar la documentación existente y asociada con los controles.
- Realizar verificaciones con las personas responsables de la Seguridad de la Información y los usuarios que se encuentran involucrados en la gestión de los activos de información y sus controles.
- Efectuar revisiones en sitio, analizando y comparando los controles implementados contra la lista de controles que deberían estar, para establecer la brecha respectiva.
- Cuáles controles están implementados correctamente y si son o no eficaces.
- Revisar los resultados de las auditorías internas.

Además de tener en cuenta lo indicado en la política de riesgos de Colombia Compra Eficiente y en la última versión de la guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

1.4 Identificación de las vulnerabilidades

En esta etapa es necesario identificar las debilidades que puedan ser explotadas por las Amenazas ya identificadas y que puedan comprometer la Confidencialidad, Integridad y Disponibilidad de los Activos de Información.

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de Amenazas, la lista de inventario de Activos y los controles existentes.

Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal.
- Ambiente físico.
- Configuración de los sistemas de información.
- Hardware, software y equipos de comunicaciones.

- Dependencia de partes externas.

En el anexo B se puede evidenciar algunos ejemplos de vulnerabilidades y Amenazas que sirven como guía a la hora de identificar las vulnerabilidades

1.5 Definir actividades de control / acciones de tratamiento

Se deben definir acciones que permitan reducir, evitar o transferir el Riesgo, según sea el caso. Adicionalmente, en esta etapa se debe especificar:

- El alcance de la acción
- Periodicidad con que se ejecutan
- Asignar el responsable de la ejecución de las acciones.
- Propósito del control
- Establecer como se realiza la acción
- Indicar qué acciones se toman cuanto existen observaciones o desviaciones resultantes de ejecutar el control
- La documentación que soporta la ejecución del control

Así mismo, para el tratamiento de los riesgos de Seguridad de la Información, es necesario tener en cuenta lo establecido en el manual de Seguridad de la Información de Colombia Compra Eficiente, y los controles indicados en dicho documento.

Las actividades de control se identifican teniendo en cuenta que pueden ser preventivas o detectivas, aclarando que las preventivas se diseñan para evitar la materialización de un evento no deseado, previniendo la ocurrencia de riesgos que afecten la integridad, disponibilidad y confidencialidad de la Información; mientras que los controles detectivos, se centran en eventos que ya se materializaron con el fin de corregir la situación. Así mismo, es importante que los controles apunten a tratar las causas/vulnerabilidades que generan los riesgos, estos controles pueden tratar varias causas/vulnerabilidades o solo una, lo importante es que cada causa/Vulnerabilidad sea tratada y de forma efectiva.

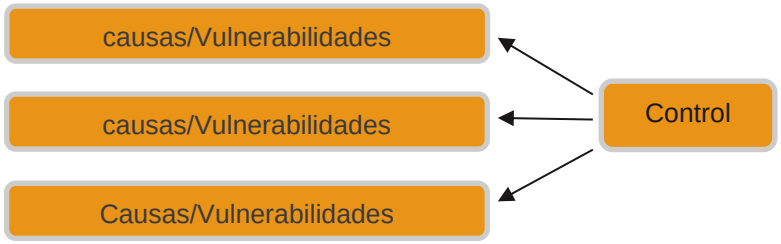


Ilustración 1 Relación de actividades de control con causas/Vulnerabilidades

Las acciones planteadas deben disminuir la probabilidad y el impacto de la materialización de los riesgos identificados.

2. Seguimiento

Los Riesgos y sus factores (es decir, el valor de los Activos, los impactos, las Amenazas, las vulnerabilidades y la probabilidad de ocurrencia) se deberían monitorear y revisar con el fin de identificar todo cambio en el contexto de la organización en una etapa temprana, y para mantener una visión general de la perspectiva completa del Riesgo.

Para ello, se deben documentar las revisiones realizadas por el área de seguridad, la fecha para la implementación de los tratamientos, la frecuencia y auto seguimientos que los responsables del tratamiento del riesgo deben realizar sobre la implementación de los controles.

El Oficial de Seguridad de la Información, liderará los auto seguimientos con los responsables y realizará reuniones con el fin de verificar la efectividad y la correcta aplicación de los controles. La periodicidad para cada reunión depende de las fechas establecidas en la ejecución de los controles.

3. Comunicación

Todas las novedades que impactan a los Riesgos de Seguridad de la Información se deberán comunicar al Oficial de Seguridad de la Información y se dejará documentación asociada que puede ser por correo electrónico o por medio de GLPI.

4. Actividades proyectadas en el plan de tratamiento de Riesgos

Las actividades planteadas a continuación fortalecen la gestión de los riesgos de privacidad y seguridad de la Información en Colombia Compra Eficiente, y complementan lo indicado en la Matriz de riesgos gestión, corrupción y seguridad de la Información, como también la Política y metodología de riesgos de seguridad de la Información y la metodología de activos de información; en las cuales se plantean los riegos ya identificados, con sus respectivos controles para el tratamiento respectivo, realizando el establecimiento y entendimiento del contexto, estimación, evaluación y tratamiento.

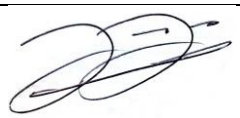
Para la vigencia 2019 se planean adelantar las siguientes actividades por parte de la Subdirección de Información y Desarrollo Tecnológico y el equipo de seguridad de la Información:

ID	Actividad	Descripción	Fecha de Actividad	Responsable
A1	Articular la metodología de riesgos de seguridad de la Información, con los riesgos de gestión y corrupción, según lo indicado en la última versión de la guía del DAFP.	Se realiza análisis de la metodología existente de riesgos de seguridad de la Información, en búsqueda de la articulación con los riesgos de gestión y corrupción, teniendo en cuenta los lineamientos	Febrero de 2019	Equipo de Seguridad de la Información / Subdirección de Información y Desarrollo Tecnológico.

		dados por el Gobierno Nacional.		
A2	Actualización y aprobación de metodología de activos de Información.	Se realiza actualización sobre la metodología de activos de información, articulándola con la guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, para luego ser aprobada.	Febrero de 2019	Equipo de Seguridad de la Información / Subdirección de Información y Desarrollo Tecnológico.
A2	Diseño matriz para tratamiento de riesgos de Seguridad de la Información	Tomando como referencia la última versión de la guía de DAFP, se adapta matriz para que incluya los riesgos de seguridad de la información. Gestión y corrupción.	Marzo de 2019	Equipo de Seguridad de la Información / Subdirección de Información y Desarrollo Tecnológico.
A3	Apoyo a la construcción de la política de administración de riesgos de la entidad.	Se realiza apoyo, incluyendo lo relacionado con riesgos de seguridad de la Información, y haciendo observaciones en la política general.	Marzo de 2019	Equipo de Seguridad de la información

A4	Aprobación de la política de tratamiento de Riesgos de la entidad, actualización del plan de tratamiento de riesgos de Seguridad de la Información, actualización de la matriz de riesgos de gestión, corrupción y seguridad de la información.	Se busca la aprobación de los documentos y formatos asociados con la gestión del riesgo de la entidad, con el fin de aplicarlas formalmente en la Entidad y utilizarlas como guía y complemento para el tratamiento de los riesgos de seguridad de la Información.	Abril de 2019	Subdirección de Información y Desarrollo Tecnológico./Planeación
A5	Sensibilización de la metodología de Riesgos de seguridad de la Información y matriz de manejo de riesgos	Se realizan jornada de sensibilización de la metodología de riesgos de Seguridad de la Información en la Subdirección de Información y Desarrollo Tecnológico.	De forma trimestral	Equipo de Seguridad
A6	Seguimiento de riesgos IDT (Seguridad de la Información) y activos de Información.	Se realizan seguimientos periódicos, de acuerdo a la periodicidad de los controles establecidos para cada riesgo. En estos seguimientos se evalúa la efectividad de los controles.	De forma bimensual	Equipo de Seguridad
A7	Planteamiento de acciones de mejora respecto al análisis de los riesgos y el tratamiento identificado en la subdirección de IDT.	De acuerdo a las validaciones realizadas, se proponen mejoras sobre el tratamiento de riesgos de seguridad de la Información en la entidad.	De forma bimensual	Subdirección IDT.(Responsables de cada riesgo y control)

5. Autorizaciones

	Fecha	Nombre	Firma	Cargo o Perfil
Elaboró	27/03/2019	Luis Alejandro Ruiz		Contratista con rol de apoyo y asesor de seguridad de la información
Revisó	28/03/2019	Frederick Nicolai Ferro Mojica / Dana Pineda Marín	 	Contratista con rol de líder de seguridad de la información Subdirector de Información y Desarrollo Tecnológico
Aprobó	05/04/2019	Comité Institucional de Gestión y Desempeño	Acta Comité Institucional de Gestión y Desempeño No. 7 Abril 05 de 2019	

Anexos

Anexo A. Amenazas

Ejemplo Amenazas

Fuente	Amenaza
Daño físico	Fuego
	Agua
	Contaminación
	Accidente Importante
	Destrucción del equipo o medios
	Polvo, corrosión, congelamiento
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Fenómenos meteorológicos
	Inundación
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado
	Perdida de suministro de energía
	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 técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	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
	Error en el uso

Compromiso de las funciones	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la Disponibilidad del personal

Ilustración 1 - Tabla de Amenazas (Fuente Política de Gobierno Digital)

Anexo B. Amenazas y Vulnerabilidades

Ejemplo Amenazas y vulnerabilidades

Tipo	Vulnerabilidad	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 electromagnética	Radiación 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.
Software	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 eficaz	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 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
	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 electromagnética	Radiación 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
Red	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 contraseñas en claro	Espionaje remoto
	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
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
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	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 para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	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

Ilustración 2 Vulnerabilidades conocidas (Fuente Política de Gobierno Digital)

Anexo C Formato Matriz de Riesgos de Seguridad y Privacidad de la Información

Variables que maneja la matriz de riesgos de Seguridad y Privacidad de la Información.

		Identificación						Estimación Inicial				
Nombre Ref.	**Id**	**RIESGO**	**Activos / Contenedores**	**Amenazas**	**Vulnerabilidades**	**Consecuencias**	**Controles / acciones sugeridas**	**Impacto.**	**Prob.**	**Estimación Riesgo**	**Responsable Riesgo**	**Medidas de Respuesta**

Tratamiento										
Responsable del Tratamiento	**Acciones Tratamiento de riesgo**	**Frecuencia de seguimiento**	**Ultima fecha revisión del Tratamiento**	**Siguiente fecha de revisión**	**Fecha objetivo implementación Tratamiento**	**Estado del Tratamiento**	**Impacto. (Después de TR)**	**Prob. (Después de TR)**	**Riesgo Residual**	**Estado**