

**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL**

**Bogotá, D.C.,**

**(FEBRERO DE 2019)**

CONTENIDO

[1. INTRODUCCIÓN 3](#_Toc982941)

[2. GLOSARIO DE TERMINOS 3](#_Toc982942)

[3. OBJETIVO GENERAL 4](#_Toc982943)

[4. OBJETIVOS ESPECIFICOS 4](#_Toc982944)

[5. ALCANCE 4](#_Toc982945)

[6. DECLARACIÓN 5](#_Toc982946)

[6.1. Acuerdo de confidencialidad: 5](#_Toc982947)

[7. ROLES Y RESPONSABILIDADES 5](#_Toc982948)

[8. PLAN DE SEGURIDAD PARA LA GESTION DE RIESGOS. 6](#_Toc982949)

1. ****INTRODUCCIÓN****

La gestión integral de riesgos es un principio prioritario en la actuación de los colaboradores de la entidad.

La gestión de riesgos es la combinación de administrar el recurso humano, los procesos, los proyectos, las instalaciones y la implementación de mecanismos de prevención y mitigación de los riesgos identificados. Así mismo, la construcción de una cultura proactiva de conciencia y autocontrol frente al manejo del riesgo. Finalmente, la gestión integral de riesgos tiene como propósito reducir la probabilidad de ocurrencia y afectación en la continuidad de la operación de los procesos que utilicen los sistemas de información y la infraestructura tecnológica de la entidad.

El riesgo es un aspecto inseparable de los procesos y debe ser adecuadamente administrado y gestionado, siendo por ello necesario analizar y considerar la existencia de condiciones, situaciones o eventos que pueden desencadenarse y resultar en consecuencias negativas para la empresa, sus empleados, el medio ambiente, la comunidad o sus accionistas

1. ****GLOSARIO DE TERMINOS****

* **Apetito de Riesgo (Tolerancia al Riesgo):** Es el nivel de riesgo que la entidad está dispuesta a tolerar para que no afecte el desarrollo de los objetivos estratégicos.
* **Control:** Medida que se toma para modificar la exposición al riesgo, bien sea para disminuir la probabilidad de ocurrencia del evento o para disminuir su impacto.
* **Disponibilidad:** Capacidad de un componente o servicio para realizar su función requerida durante un periodo de tiempo.
* **Gestión Integral de Riesgos:** Es el proceso de identificación, valoración y control de los riesgos que amenazan el logro de los objetivos de la entidad.
* **Identificación de riesgos:** Es el proceso de encontrar, reconocer y definir los escenarios de riesgo, sus causas y sus potenciales consecuencias.
* **Proceso:** Grupo de actividades relacionadas de manera lógica que, cuando se llevan a cabo, utilizan los recursos de la entidad para lograr resultados definitivos o transformar elementos de entrada, a través de una serie de actividades, en un producto o servicio.
* **Responsable del Riesgo:** Persona o entidad que tiene la responsabilidad y autoridad para gestionar el riesgo a través de la implementación de los planes de mitigación.
* **Riesgo:** El [riesgo](http://eldia.es/canarias/2014-12-01/3-Abordan-riesgo-nutricional-mayores.htm)es el la exposición a una situación donde hay una posibilidad de sufrir un daño o de estar en peligro. **Es esa vulnerabilidad y amenaza a que ocurra un evento y sus efectos sean negativos y que los activos puedan verse afectados por él.**
* **Riesgo inherente:** Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior. Este riesgo surge de la exposición que se tenga a la actividad en particular y de la probabilidad que un impacto negativo afecte la rentabilidad, el capital de la compañía, y sus procesos.
* **Riesgo residual:** Es aquel riesgo que subsiste, después de haber implementado controles. Es importante advertir que el nivel de riesgo al que está sometido una entidad nunca puede erradicarse. Por ello, se debe buscar un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar o mitigar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable). El riesgo residual puede verse como aquello que separa a la entidad de la seguridad absoluta.
* **Seguridad de la Información:** Conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.
* **Tratamiento del riesgo (Plan de Mitigación):** Selección y aplicación de medidas, con el fin de poder modificar la magnitud del riesgo, para evitar de este modo los daños intrínsecos de materializarse.
* **GSIT:** Gestión de Servicios de Infraestructura Tecnológica.
* **Impacto:** Es el resultado de la materialización de un evento.
* **Probabilidad:** Se refiere a la posibilidad de ocurrencia de un riesgo potencial.
* **Usuario:** Persona que utiliza los servicios diarios.

1. ****OBJETIVO GENERAL****

Suministrar los lineamientos sobre las acciones que se deben adelantar al interior la entidad, encaminadas a establecer un plan de tratamiento de riesgos con el fin de disminuir la probabilidad de ocurrencia y el impacto de todas aquellas situaciones que puedan interferir con la continuidad de la operación de la infraestructura tecnológica y los sistemas de información que afecten el funcionamiento de los procesos de la entidad.

1. ****OBJETIVOS ESPECIFICOS****

* **Minimizar la materialización de los riesgos asociados infraestructura tecnológica y sistemas de información.**
* **Identificar las principales amenazas y vulnerabilidades a los que están expuestos los activos de información.**
* **Garantizar la disponibilidad, confidencialidad e integridad de los activos de información de la entidad minimizando el riesgo que se pueda generar por la fuga o perdida de alguna credencial de acceso.**

1. ****ALCANCE****

El alcance de los lineamientos que se definen en este documento da cubrimiento a:

1. Identificación de amenazas asociadas a los activos de información.
2. Identificación de vulnerabilidades asociadas a los activos de información.
3. Identificación del riesgo inherente.
4. Tratamiento del riesgo.
5. Aplicación de controles.

Todos los Servidores Públicos de la Unidad: Empleados públicos de planta (de carrera administrativa y los provisionales), funcionarios de libre nombramiento y remoción, trabajadores oficiales, contratistas y demás personal que tengan asignados activos de información, deberán realizar la identificación de los riesgos inherentes de mencionados activos, así como aplicar los controles necesarios para minimizar el riesgo inherente.

1. ****DECLARACIÓN****

En este documento se encuentran los lineamientos que aseguran una actuación adecuada para alcanzar un alto nivel en cuanto a seguridad de la información en la UAERMV. La información es un activo importante para la entidad, tiene un alto valor para la misma, por esto mismo la unidad ha definido las directrices de seguridad para los Activos de Información, por medio de las cuales se deben orientar todas las acciones a seguir.

Estas directrices hacen parte del marco de POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE INFORMACIÓN Y COMUNICACIONES y están basadas en la NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información publicado por la [*International Organization for Standardization*](http://es.wikipedia.org/wiki/International_Organization_for_Standardization) y la [Comisión Electrotécnica Internacional](http://es.wikipedia.org/wiki/Comisi%C3%B3n_Electrot%C3%A9cnica_Internacional). La versión más reciente es la ISO/IEC 27002:2013).

Por lo anterior, se busca minimizar los riesgos asociados a los activos de información, asegurar la continuidad de la UAERMV y ayudar en el cumplimiento de los objetivos misionales.

## Acuerdo de confidencialidad:

Todos los Usuarios que administran, leen, modifican o crean información en la UAERMV deben firmar un acuerdo de confidencialidad o de no divulgación como parte de sus términos y condiciones iníciales de empleo. Esta directriz también incluye a personal ocasional y los Usuarios externos no contemplados en un contrato formalizado.

1. ROLES Y RESPONSABILIDADES

**7.1 Encargado de seguridad de la información:** Persona delegada cuyas funciones principales son asesorar en materia de seguridad de la información a la UAEMRV y supervisar el cumplimiento de la presente Política.

1. PLAN DE SEGURIDAD PARA LA GESTION DE RIESGOS.

Los riesgos de seguridad digital se basan en la afectación de 3 criterios en un activo o un grupo de activos dentro del proceso: “Integridad, confidencialidad o disponibilidad”.

La entidad, se compromete a gestionar los riesgos, identificando y administrando los eventos potenciales que pueden afectar la plataforma estratégica, los objetivos institucionales y los macroprocesos y procesos de la entidad. Para la adecuada gestión integral del riesgo en la UAERMV, se presenta los siguientes lineamientos:

1. Se adoptará las metodologías para gestionar los riesgos de la entidad a través del análisis del contexto, entendido como el entorno externo e interno, y la valoración de los mismos, es decir, su identificación, análisis y evaluación, y su posterior tratamiento, todo esto manteniendo comunicación y consulta constante y permanente monitoreo y revisión, para evitar así su materialización.
2. Asegurar los recursos necesarios para ayudar a los responsables a gestionar y tratar los riesgos.
3. Los riesgos que se gestionan en la UAERMV son los siguientes:
4. **Riesgos Estratégicos:** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
5. **Riesgos gerenciales:** Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
6. **Riesgos operativos:** Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
7. **Riesgos financieros:** Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
8. **Riesgos tecnológicos:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
9. **Riesgos de cumplimiento:** Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones
10. contractuales.
11. **Riesgo de imagen o reputacional:** posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.
12. **Riesgos de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado**.**
13. **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.
14. Se deben identificar los activos de información por cada proceso.
15. Se deben identificar los dueños de los activos.
16. Se deben clasificar los activos.
17. Se debe determinar la criticidad de los activos.
18. Se deben identificar las vulnerabilidades de los activos.
19. Se deben identificar las amenazas de los activos.
20. Se deben identificar los riesgos de los activos.
21. Se debe realizar una descripción de los riesgos.
22. Se debe revisar la probabilidad y el impacto de ocurrencia de los riesgos.
23. Se debe calcular el riesgo inherente.
24. Se deben aplicar los controles a los riesgos identificados.
25. Los controles deben tener una frecuencia de aplicación.
26. La tolerancia es el nivel del riesgo que la entidad puede o está dispuesta a soportar, que corresponden a los riesgos que se encuentren en zona residual Baja y los que se encuentran en otra zona se trataran de acuerdo a los lineamientos establecidos en el procedimiento de Gestión de Riesgos de la entidad.
27. La entidad revisará y actualizará la política de Gestión de Riesgos de acuerdo con los cambios del entorno, las nuevas metodologías y los resultados de los indicadores de gestión asociados a la materialización de riesgos definidos.
28. Los riesgos identificados en la entidad deberán ser monitoreados permanentemente, para asegurar que los controles sean eficaces y eficientes, y obtener información para mejorar la evaluación y gestión de los riesgos e identificar la materialización oportuna de los riesgos.
29. Los niveles de responsabilidad sobre periodicidad de seguimiento y evaluación de los riesgos se llevarán a cabo de acuerdo procedimiento de Gestión de Riesgos.
30. Comunicar interna y externamente, los resultados de la gestión del riesgo desarrollada institucionalmente, reportando en el Mapa Institucional de Riesgos, los riesgos priorizados de acuerdo con los lineamientos establecidos en el procedimiento de Gestión de Riesgos.
31. Las opciones del tratamiento a los riesgos que se evalúan en la entidad son:
    1. **Evitar el riesgo:** Se logra cuando al interior de los procesos se genera cambios sustanciales por rediseño, eliminación o cancelación de una actividad o conjunto de actividades que causan el riesgo, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.
    2. **Reducir el riesgo:** Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.
    3. **Compartir el riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones o dependencias, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.
    4. **Asumir el riesgo**: Después de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el líder del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo. No aplica para los riesgos de corrupción, estos siempre deben conducir a un plan de acción o de tratamiento para mitigarlo.

**REVISIÓN Y APROBACIÓN:**

|  |  |  |
| --- | --- | --- |
| **Elaborado y/o Actualizado por**  **EQUIPO OPERATIVO SIG del Proceso:** | **Validado por**  **RESPONSABLE DIRECTIVO SIG**  **del Proceso:** | **Aprobado por:** |
| **OMAR FERNANDO GARZON /**  **GLORIA MENDEZ**  **Contratista / Proceso EGTI** | Firma: | Firma: |
| **Acompañamiento EQUIPO TÉCNICO SIG:** |
| **ANDREA DEL PILAR ZAMBRANO**  **Contratista/ Proceso DESI** |
| **MARCELA ROCIO MARQUEZ ARENAS**  **(Secretaria General)** | **MARTHA PATRICIA AGUILAR COPETE**  **Representante de la Alta Dirección** |

**CONTROL DE CAMBIOS:**

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSIÓN** | **DESCRIPCIÓN** | **FECHA** | **APROBADO**  **Representante de la Alta Dirección SIG** |
| 1 | Elaborado por el Ing. Omar Fdo. Garzón Giraldo (especialista en seguridad de la información), versión inicial del documento conforme a los requerimientos de MINTIC. | Febrero 2019 | Jefe Oficina Asesora de Planeación |