



Departamento del Quindío



SECRETARÍA TIC



PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD, PRIVACIDAD DE LA
INFORMACION Y SEGURIDAD DIGITAL



GOBERNACION DEL QUINDIO

2019



TABLA DE CONTENIDO

INTRODUCCION.....3

OBJETIVOS.....4

ALCANCE5

GLOSARIO6

NIVELES DE TOLERANCIAS AL RIESGO.....8

IDENTIFICACION Y ANALISIS DE RIESGOS.....9

 Riesgos por incidencia externa9

 Riesgos por incidencia interna9

 Mitigación del riesgo11

MATRIZ DE RIESGOS.....15

IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DIGITAL.....16

ESTABLECIMIENTO DEL CONTEXTO.....17

CONTEXTO EXTERNO18

CONTEXTO INTERNO.....19

CONTEXTO DEL PROCESO.....20

IDENTIFICACION DE ACTIVOS DE SEGURIDAD DE LA INFORMACION.....21

MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL.....27

FASE DE IMPLEMENTACION28

FASE DE SEGUIMIENTO Y CONTROL28

REPORTE Y SOCIALIZACION DE RIESGOS DE SEGURIDAD.....28

AUDITORÍAS INTERNAS Y EXTERNAS29

FASE DE MEJORAMIENTO CONTINUO DE LA GESTION DE REISGOS DE SEGURIDAD DIGITAL.....29



Departamento del Quindío



SECRETARÍA TIC



INTRODUCCION

Desde los inicios de los sistemas de información se sabe que las contingencias forman parte de los mismos, ya que como es sabido las amenazas a la información pueden venir de diferentes fuentes, tanto de origen natural (terremotos, tormentas eléctricas, etc), como de origen humano (huelgas, competencia entre compañeros, problemas laborales, etc) de origen técnico (fallas de hardware, software, suministro de energía, etc.) Y es casi siempre una situación no prevista la que regularmente provoca una crisis y las consecuencias de la misma, según su impacto y extensión, pueden ser catastróficas para los intereses de cualquier organización. Conscientes de ello, se pretende definir en este documento, las políticas más asertivas aplicables a la gobernación del Quindío, en materia de recuperación de la normalidad para aquellas eventualidades no previstas en las que algún recurso informático se vea amenazado o afectado.

La gestión de riesgos establece procesos, procedimientos y actividades encaminados a lograr un equilibrio entre la prestación de servicios y los riesgos asociados a los activos de información que dan apoyo y soporte en el desarrollo de la misionalidad de la gobernación del Quindío. En tal sentido, se debe considerar e implementar medidas que implican tiempo, esfuerzos y recursos necesarios para dar un adecuado tratamiento a los riesgos, generando una estrategia de seguridad efectiva que controle y administre la materialización de eventos o incidentes, mitigando los impactos adversos o considerables al interior de la entidad.

Teniendo en cuenta lo anterior la gobernación del Quindío. Considera que la información es el patrimonio principal de toda la Institución, por lo que planifica y toma medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.



SECRETARÍA TIC



OBJETIVOS

OBJETIVO GENERAL

Plantear y establecer un marco de gestión de riesgos a través del cual se mitiguen las vulnerabilidades y amenazas asociadas a los activos de información de la gobernación del Quindío, con el fin de lograr reducir su probabilidad e impacto en la entidad.

Objetivos específicos

- ❖ Proteger y conservar los activos informáticos de la gobernación del Quindío contra riesgos, desastres naturales o actos malintencionados.
- ❖ Garantizar la operatividad de la red interna de la gobernación del Quindío, cuando se presente alguna eventualidad.
- ❖ Evaluar los riesgos de los procedimientos de contingencia requeridos cuando se presenta una interrupción de las operaciones, de forma que sólo se inviertan los recursos necesarios.
- ❖ Identificar las amenazas e impactos de seguridad digital asociadas a los procesos de la entidad.
- ❖ Gestionar los riesgos identificados con una matriz que ayude a reducir su probabilidad e impacto si se este se llegará a materializar
- ❖ Minimizar la posible pérdida de información en el evento inesperado, previendo procedimientos de recuperación efectivos y eficientes.



SECRETARÍA TIC



ALCANCE

La necesidad de desarrollar un plan de tratamiento de riesgos, está relacionada con el impacto potencial que provoca la interrupción parcial o total de los sistemas de información, sobre el normal desarrollo de las actividades de la GOBERNACION DEL QUINDIO; específicamente, para afrontar la contingencia relacionada con el eventual cese de actividades e inoperatividad de equipos.

Lo que supone que los procedimientos planteados en este documento, contemplan solamente las acciones a realizar con relación al Hardware, software, equipos electrónicos y redes involucrados en los procesos críticos definidos en el Plan.

Adicionalmente, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos principales de los equipos de cómputo y la red interna

Las actividades y procedimientos, están relacionados con las funciones que competen a cada uno de los usuarios y dependen de la diligencia y colaboración de las dependencias y de los recursos disponibles (capacitación, recursos técnicos, presupuesto, etc.).

Como parte del plan de gestión de riesgos de seguridad digital se analiza el contexto estratégico de los riesgos de seguridad digital a los que está expuesta la entidad dando cubrimiento a los procesos estratégicos, misionales, de soporte, de verificación y mejora; y concluye con una matriz de riesgos en la que analizará la probabilidad, el impacto, las acciones continentes y los riesgos residuales identificados del proceso de identificación.



GLOSARIO

Riesgo de gestión: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como 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 (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

Riesgo residual: nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

Gestión del riesgo: 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 (Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)., 2016).

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad (Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)., 2016).

Impacto: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

Evento de seguridad de la información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad (TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS, 2006).

Inventario de activos: [Según ISO 27000.ES]: Sigla en inglés: Assets inventory. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.



Departamento del Quindío



SECRETARÍA TIC



Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

Tolerancia al riesgo: Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable (Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2016).

NIVELES DE TOLERANCIAS AL RIESGO

Entendiendo que el nivel de tolerancia al riesgo es la exposición al riesgo que una entidad, en este caso la gobernación del Quindío, está dispuesta a asumir en el desarrollo de su actividad con el fin de alcanzar sus objetivos estratégicos y cumplir con su misión institucional, la secretaría TIC a definido los siguientes niveles de tolerancia al riesgo:

	CARACTERÍSTICA	MITIGACIÓN
Insignificante	Estos tipos de riesgos, son riesgos rutinarios, propios del desempeño de las funciones	De acuerdo a los niveles de soporte establecidos en el diagrama de servicios, estos pertenecen a soporte nivel 1 y la mayoría se solucionan en este nivel de servicio
Bajo	No tiene impacto potencial sobre la funcionalidad del servicio ni compromete la seguridad de la entidad.	El riesgo que tiene gravedad baja, por lo general no justifica inversión de recursos y controles a los ya establecidos en la matriz de riesgos.
Medio	Impacta sobre la funcionalidad de los servicios que ofrece la entidad, cuyas consecuencias pueden ser absorbidas y subsanadas en el desarrollo normal de las actividades de la secretaría TIC	Aunque deben ejecutarse actividades para la mitigación del riesgo, estas debido a su nivel pueden ser ejecutadas a mediano plazo
Alto	Impacta sobre la funcionalidad del servicio de la entidad, la mayoría de las veces estas consecuencias NO pueden ser absorbidas y subsanadas en el desarrollo normal de las actividades de la secretaría TIC	Requiere que se ejecuten actividades para disminuir la exposición al riesgo, como adquisición de equipos, coberturas de seguros o polizas, personal especializado, etc. Todo lo anterior se debe hacer a corto plazo
Catastrófico	Afecta gravemente el desempeño de las actividades propias de la gobernación del Quindío. Generando riesgos que si no se priorizan, por lo general pueden desencadenar hasta en pérdida de información valiosa de la entidad	Bajo ninguna circunstancia se deberá tener este riesgo y si se llegase a tener, este deberá tener una alta prioridad por el comité de gobierno en línea y se deberá comunicar a la alta dirección de la gobernación del Quindío.



IDENTIFICACION Y ANALISIS DE RIESGOS

Definición: La matriz de riesgos es una confrontación analítica de los posibles riesgos a los que se encuentra sometida el área tecnológica, este análisis nos permitirá evaluar la probabilidad de ocurrencia de los distintos riesgos para diseñar los controles preventivos y correctivos, los que se considera más críticos y causan más impacto para la gobernación del Quindío.

En esta etapa se desarrolla la probabilidad de ocurrencia, posibilidades de mitigación, el Impacto y probabilidades de los riesgos, finalmente las alternativas de corrección de la anomalía.

Análisis de Riesgos: Los diferentes riesgos a los que puede encontrarse sometida el área tecnológica se pueden agrupar de la siguiente forma:

Riesgos por incidencia externa

- ❖ **Desastre natural:** Hace referencia a los riesgos a los que está expuesta cualquier entidad pública, en caso de incendio, terremoto, tormenta eléctrica, etc.
- ❖ **Interrupción del fluido eléctrico:** Esto es la capacidad que tiene la gobernación del Quindío para reaccionar ante el corte parcial del fluido eléctrico, por daños inesperados por parte de la empresa prestadora del servicio.
- ❖ **Modificaciones a la constitución política:** Ya sea por asamblea constituyente, referendo, consulta popular, plebiscito o mediante leyes orgánicas, reestructuración o supresión de entidades.

Riesgos por incidencia interna

- ❖ **Perdida de la información:** Hace referencia a la seguridad de la información que maneja la gobernación del Quindío, ya que debido a los procesos que la entidad maneja, esta debe conservarse de manera confidencial, y así evitar que sea entregada accidentalmente, o bien, que sea objeto de robo.
- ❖ **Falla de equipos electrónicos:** Como cualquier equipo electrónico los computadores son susceptibles a fallos en cualquier momento, pudiendo llegar a provocar pérdida de la información y retrasos en procesos administrativos.



- ❖ **Falla en servidores:** Los servidores que se encuentran en el Data center de la gobernación del Quindío, pueden llegar a presentar fallas de configuración, provocando que se paren los aplicativos esenciales con los que trabajan los funcionarios, como PCT, SEVENET, INTRANET Y DOMINIO.
- ❖ **Virus informáticos:** Los virus informáticos tienen por objeto alterar el funcionamiento normal de los equipos de cómputo, además tienen la facilidad de propagarse con facilidad con el uso de memorias USB, correo electrónico, etc.
- ❖ **Seguridad o Robo:** hace referencia al hurto de la información, de los mismos equipos de cómputo o equipos de red con los que cuenta la gobernación de Quindío.
- ❖ **Calentamiento de la Sala de Cómputo (Data center):** Este riesgo está asociado a la probabilidad de que se incremente la temperatura del data center por encima de los mínimos permitidos por la dirección Tic, cabe aclarar que en el data center se encuentran los servidores de la gobernación del Quindío y switches principales de la red interna, los cuales generan que se incremente la temperatura dentro del cuarto.
- ❖ **Copias de seguridad sistemas de información:** Riesgo asociado a la falta de copias de seguridad de las bases de datos de los sistemas de información con los que cuenta la entidad, dichas copias se deben realizar diariamente y por la dirección TIC.
- ❖ **Falta de Actualización de la infraestructura tecnológica:** se refiere a la falta de adquisición y/o actualización de equipos que se van quedando obsoletos por su tiempo de uso.
- ❖ **Incumplimiento de los contratistas:** Este riesgo puede ocurrir a causa del posible atraso en la contratación, ejecución o trasgresión del de los contratos de actualización, modificación, mantenimiento, que se asumen durante la vigencia, contratos como licenciamiento de antivirus, mantenimiento correctivo de equipos, red de acceso a internet, sistemas de información como PCT, Sevenet, Ventanilla única virtual Quindío, Siscar, etc.
- ❖ **Retrasos en Procesos Administrativos:** La implementación de los procesos tecnológicos relacionados con la ejecución de los contratos, implica el desarrollo de trámites administrativos, los cuales se puede llegar a retrasar por exigencias en el cumplimiento de requisitos.



- ❖ **Procesos de capacitación constante del personal TI:** Riesgo asociado a la falta de actualización y capacitación de los conocimientos en sistemas de información de la gobernación del Quindío.
- ❖ **Accesos no autorizados a los sistemas de información:** Hace referencia a accesos a las bases de datos no autorizados de los diferentes aplicativos misionales de la entidad y de computadores que manejen información confidencial de la misma.
- ❖ **Equivocaciones humanas:** Riesgo permanente que se genera por el desconocimiento, descuido, o mal uso de un sistema de información o aplicativo de la entidad.
- ❖ **Activos de la información desactualizados:** La no actualización de los activos de la información por parte de la dirección TIC, genera un riesgo inherente a la pérdida de la información y/o desconocimiento de lo que se encuentra instalado en cada equipo de la entidad.
- ❖ **Equipos de red (switch) conectados a puntos de red a la vista de funcionarios y de fácil acceso:** Riesgo asociado a equipos de red identificados en diferentes pisos de la entidad, los cuales tienen acceso cualquier funcionario o persona ajena a la entidad, pudiéndose conectar a internet.

Mitigación del riesgo

Consiste en el establecimiento, desarrollo de estrategias y procedimientos previos a la posible materialización del riesgo u ocurrencia de la emergencia, tendientes a la mitigación de los mismos, haciéndolos menos graves, reduciendo al máximo las consecuencias o posibles pérdidas.

Los cuales se resumen a continuación:

Desastres naturales

Aunque realmente un desastre natural no se puede evitar, la gobernación del Quindío puede llegar a prevenir algunas de las consecuencias que este tipo de siniestro pueda llegar a tener sobre la infraestructura tecnológica.

El edificio de la gobernación, cuenta con una estructura sismo resistente, que ayuda a que en caso de terremoto este pueda seguir en pie o en consecuencia, con muchos menos daños que otros edificios.



SECRETARÍA TIC



Por otra parte la red interna de la gobernación del Quindío, está respaldada con UPS, para evitar que los Switchs se dañen en casa de tormentas eléctricas, con este mismo respaldo cuentan los servidores de la gobernación que se encuentran en el data center.

Interrupción del fluido eléctrico

Como se dijo anteriormente la red interna de la Gobernación del Quindío se encuentra respaldada con UPS, para que esta siga su funcionamiento normalmente durante más de 20 minutos de interrupción. Además de que los servidores se encuentran respaldados.

Modificaciones a la constitución política

Leyes, decretos, resoluciones, ordenanzas, etc. Que expida el gobierno nacional a cargo del ministerio de Tecnologías de la información y comunicaciones MinTic, sobre el trato, seguridad y manejo de la información que tienen los entes gubernamentales.

Pérdida de Información

La Gobernación del Quindío, cuenta con una política de respaldo de la información de los servidores de la gobernación, este respaldo se realiza todos los días en discos duros externos que se encuentran en el data center.

Falla de equipos electrónicos

Para tratar de mitigar este riesgo, la gobernación del Quindío a través de la dirección TIC y con el apoyo de la empresa contratista a cargo de los mantenimientos preventivos y correctivos, viene realizando y ejecutando un plan de mantenimiento preventivo, el cual incluye un cronograma de actividades y que es ejecutado durante todo el año.

Falla en servidores

Los servidores se actualizan constantemente con las últimas actualizaciones de seguridad, además estos cuentan con monitores de confiabilidad y rendimiento que envían alertas al administrador ante cualquier eventualidad

Virus informáticos

Contra los virus informáticos, la gobernación del Quindío, cuenta con antivirus en todos los equipos de cómputo de la misma, que protegen los equipos en tiempo real. Además de lo anterior, cabe destacar que a través del año, se está ejecutando el mantenimiento preventivo el cual incluye mantenimiento de software y sistema operativo (desinfección).

Seguridad o Robo

Para reducir el riesgo de robo la gobernación del Quindío se encuentra en proceso de adquisición de cámaras de seguridad para el edificio, además de esto la gobernación cuenta con vigilantes las 24 horas del día, para reforzar la seguridad del mismo.



Calentamiento de la Sala de Cómputo (Data center)

Este riesgo tiene una baja probabilidad de ocurrencia, debido a que la gobernación del Quindío ha implementado procedimientos para su mitigación, tales como: La implementación en el centro de cómputo principal (piso 1) de un Sistema de Temperatura autorregulada, provisto de un sistema de aire acondicionado, con sensores ambientales para el control y monitoreo de temperatura.

Copias de seguridad sistemas de información

La Gobernación del Quindío, cuenta con una política de respaldo de la información de los servidores de la gobernación, este respaldo se realiza todos los días en discos duros externos que se encuentran en el data center.

Falta de actualización de la infraestructura tecnológica

La Gobernación del Quindío cuenta con un plan de compras, en el cual se tiene proyectado siempre la adquisición de equipos y/o dispositivos que ayuden a actualizar la infraestructura tecnológica de la misma.

Incumplimiento de los contratistas

Dentro de los procesos de contratación que tiene la gobernación del Quindío, con los proveedores de sistemas de información, se cuenta con pólizas de cumplimiento y responsabilidad que ayudan a mitigar el riesgo inherente al incumplimiento.

Retrasos en Procesos Administrativos

La gobernación del Quindío tiene como prioridad el resguardo de la seguridad de la información, por tal motivo se intenta contar como primer lugar con todos los proveedores y personal capacitado para la dirección TIC

Procesos de capacitación constante del personal TI

La dirección TIC, capacita en el manejo de los sistemas de información a todo el personal que ingresa a la dependencia, se realiza un proceso de aprendizaje en el cual el ingeniero, técnico o tecnólogo aprende a dominar las herramientas tecnológicas que se tienen en la gobernación.

Por otra parte, a través de la estrategia de gobierno en línea, la dirección TIC capacita constantemente a su personal en implementación de la misma.

Accesos no autorizados a los sistemas de información: Como parte de las políticas de seguridad de la información aprobadas por la secretaría administrativa, la entidad cuenta con una política de bloqueo de cesión de los equipos cada 5 minutos de inactividad. Lo anterior con el fin de evitar accesos no autorizados a los sistemas cuando el funcionario responsable del equipo no se encuentre en el sitio de trabajo.

Por otra parte, y con el fin de evitar acceso no autorizado a los sistemas de información por parte de personas tanto internas como externas a la gobernación del Quindío; La entidad cuenta con un firewall instalado y con un sistema de antivirus



Departamento del Quindío



SECRETARÍA TIC



licenciado que brindan seguridad a la hora de bloquear intentos de ataques o accesos a sistemas de información de la entidad.

Equivocaciones humanas: Si bien es cierto que este riesgo es difícil de mitigar, por la cantidad de funcionarios que laboran en la entidad, cabe decir que la dirección TIC, brinda capacitaciones continuas a los funcionarios de la entidad, sobre el manejo de los aplicativos de la entidad, además de eso, desde el área se generan copias de seguridad diarias de las bases de datos de los aplicativos de la entidad, lo anterior con el fin restaurar la información, ante cualquier pérdida o daño que se haga en una base de datos.

Activos de la información desactualizados: Dentro de los planes y controles que la dirección ejecuta, se tiene establecido el catálogo de servicios tecnológicos y la arquitectura de servicios TI, los cuales deben de tener actualizados los activos de la información para su correspondiente actualización anual.

Igualmente, la dirección TIC cuenta con un sistema de información, el cual hace un levantamiento de la información de los equipos de la entidad, su licenciamiento y sus características de hardware.

Equipos de red (switch) conectados a puntos de red a la vista de funcionarios y de fácil acceso: Como parte del levantamiento de los diagramas de red y activos de la información de IPV6, se identificó diferentes puntos de red, los cuales están conectados switch no autorizados por la dirección TIC, por tal motivo se ha venido trabajando en deshabilitar puertos de red que no están utilizando o que no han sido autorizados por la gobernación del Quindío.

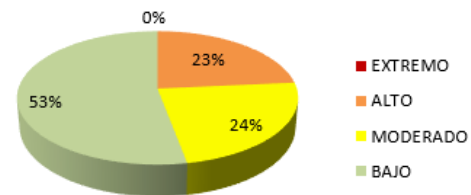
MATRIZ DE RIESGOS

A continuación se relaciona matriz de probabilidad e impacto de los riesgos relacionados con anterioridad

Impacto \ Probabilidad	1	2	3	4	5
	Insignificante	Menor	Moderado	Mayor	Catastrófico
5	0	0	0	0	0
Casi cierto	ALTO	ALTO	EXTREMO	EXTREMO	EXTREMO
4	0	0	0	0	0
Probable	MODERADO	ALTO	ALTO	EXTREMO	EXTREMO
3	0	0	1	0	0
Posible	BAJO	MODERADO	ALTO	EXTREMO	EXTREMO
2	0	4	3	3	0
Poco Probable	BAJO	BAJO	MODERADO	ALTO	EXTREMO
1	1	4	1	0	0
Raro	BAJO	BAJO	MODERADO	ALTO	ALTO
TOTAL	BAJO 9	MODERADO 4	ALTO 4	EXTREMO 0	

DISTRIBUCION DE RIESGOS - Inherente	
ZONA DE RIESGO	TOTAL
EXTREMO	0
ALTO	4
MODERADO	4
BAJO	9
TOTAL	17

Niveles de Riesgo - Residual



Ver archivo de excel matriz de riesgos



SECRETARÍA TIC



IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DIGITAL

Conforme lo indica el ámbito de aplicación del Decreto 1078 de 2015 respecto a la estrategia de Gobierno Digital, las entidades públicas deben realizar la implementación del Modelo de Seguridad y Privacidad de la Información MSPI con el objetivo de conformar un Sistema de Gestión de Seguridad de la Información al interior de la entidad.

El MSPI integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad digital, ya que esta práctica constituye su base fundamental. La guía para la gestión del riesgo de función pública, junto con el MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL (MGRSD), llevarán a cumplir dichas tareas de gestión de riesgo de seguridad digital requeridas en el MSPI (MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, 2018).

En esencia, la interacción entre ambos modelos puede resumirse de la siguiente manera:

- ❖ Las actividades de identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos se alinean con la fase de PLANIFICACIÓN del MSPI.
- ❖ Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de IMPLEMENTACIÓN del MSPI.
- ❖ Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de MEDICIÓN DEL DESEMPEÑO del MSPI.
- ❖ Las actividades de MEJORAMIENTO CONTINUO en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de Medición del Desempeño para identificar aspectos a mejorar en la aplicación de ambos Modelos.

Teniendo en cuenta lo anterior la gobernación del Quindío, adoptará el modelo de identificación de riesgos de seguridad digital propuesto el departamento de la función pública en su guía para la administración del riesgo y el diseño de controles en entidades públicas:

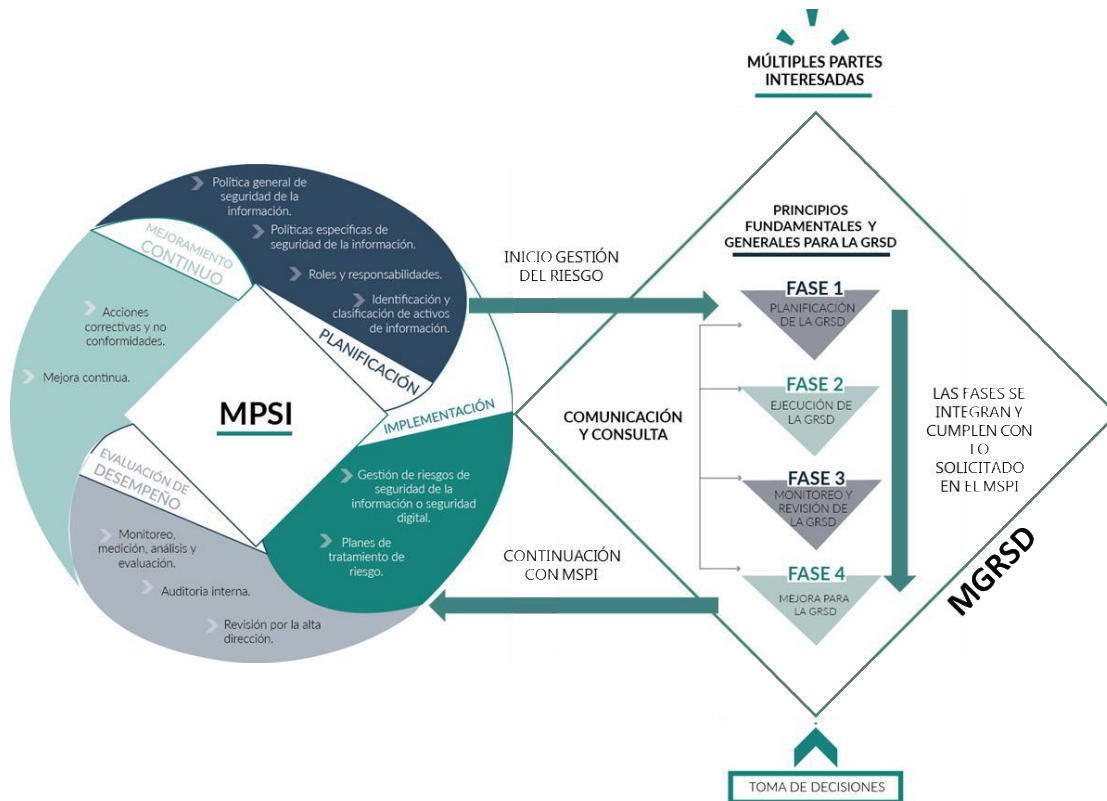


Imagen 1. Interacción entre el MSPI y el MGRSD.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

ESTABLECIMIENTO DEL CONTEXTO

Según la guía del departamento administrativo de la función pública, la definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC ISO31000, Numeral 2.9). Se debe establecer el contexto tanto interno como externo de la entidad, además del contexto del proceso y sus activos de seguridad digital (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

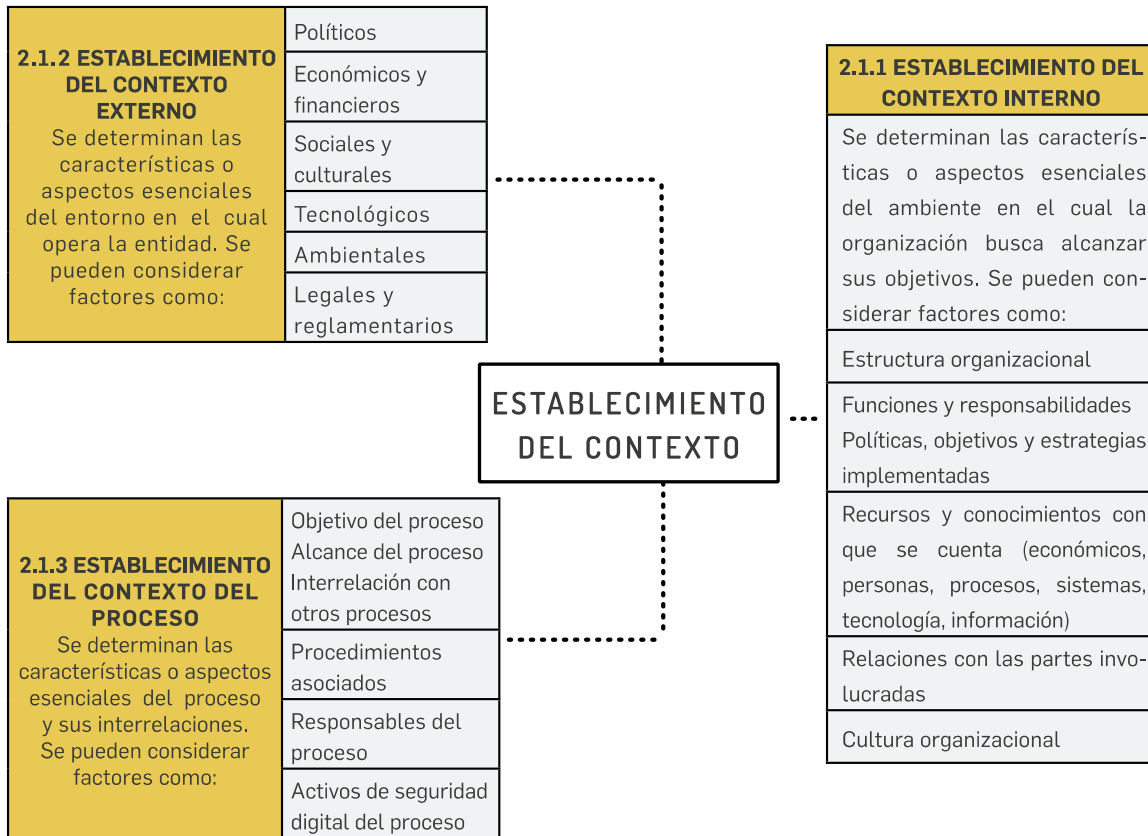


Imagen 2: establecimiento del contexto

Fuente: (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018)

CONTEXTO EXTERNO

A nivel nacional el decreto 1581 del año 2012 *“Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales”* y el cual hace referencia, en particular, al artículo 15 de la Constitución Nacional, según el cual *“todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.*



SECRETARÍA TIC



Por lo que toda información de carácter personal que se encuentra en los distintos medios o dispositivos de almacenamiento de la gobernación del Quindío, debe contemplar medidas de protección de dicha información de modo que no se vea afectada la integridad y buen nombre de las personas.

Por otra parte la ley 1712 del año 2014 "*Ley de Transparencia y del Derecho de Acceso a la Información Pública*" la cual hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que "Todas las personas tiene derecho a acceder a los documentos públicos salvo los casos que establezca la ley". El objeto de la ley es "regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información".

En razón a esto, la gobernación del Quindío está comprometida con la identificación y clasificación de todo tipo de información que es creada, almacenada, administrada y publicada, permitiendo así dar correcto cumplimiento a lo establecido en esta ley.

Por su parte, el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC el 14 de Junio de 2018 estableció el decreto 1008 "*Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*" que por medio del uso de tecnologías de la información y las comunicaciones permita lograr una mejor competitividad, proactividad e innovación en la ciudadanía y el Estado, por lo que la gobernación del Quindío desempeña un papel importante con la implementación de recursos tecnológicos que le permita alcanzar los propósitos que dispone esta ley, gestionando los riesgos y amenazas que traigan consigo la implementación de nuevas tecnologías de la información o avances tecnológicos que puedan beneficiar tanto a la entidad como a los municipios del departamento y sus comunidades.

CONTEXTO INTERNO

La gobernación del Quindío dentro de su estructura organizacional recientemente modificada adhirió a la secretaría TIC, mediante el decreto 187 del 28 de marzo del 2019, como una más de sus secretarías y creando a su vez dos direcciones que ayudarán a cumplir los objetivos institucionales que la entidad trace a corto, mediano y largo plazo.



SECRETARÍA TIC



Dentro de las funciones de la secretaría TIC están Diseñar y formular los planes, programas y proyectos, así como fortalecer el uso, la innovación y la apropiación de las tecnologías de la información y las comunicaciones y la gestión de la información, con el fin de propiciar la implementación de la TI en el Departamento del Quindío.

Teniendo en cuenta lo anterior y como parte de las funciones propias de la secretaría se debe encaminar esfuerzos para ejecutar las acciones orientadas a la gestión de riesgos de seguridad digital, hacia la protección de la disponibilidad, integridad y confidencialidad de los datos e información que se almacena en la gobernación del Quindío, que se procesa, que se almacenada y se trasmite, previniendo la materialización de amenazas que puedan impactar de forma considerable la información concerniente a los ciudadanos y funcionarios propios de la administración departamental.

Por otra parte, y con la adopción del modelo de seguridad y privacidad de la información MSPI y con la definición del plan estratégico de tecnologías de la información PETI, la gobernación del Quindío da un paso adelante en la consecución de la estrategia de gobierno digital con todos sus componentes, logrando así beneficiar a los funcionarios y a la comunidad en general.

CONTEXTO DEL PROCESO

El plan de gestión de riesgos y la matriz de identificación de riesgos, hacen parte del modelo de seguridad y privacidad de la información adoptado por la gobernación del Quindío, en cumplimiento con la estrategia de gobierno digital y apuntan básicamente a la protección de los activos de información de la entidad, garantizando así el funcionamiento interno de los procesos que van de cara a los ciudadanos.



IDENTIFICACION DE ACTIVOS DE SEGURIDAD DE LA INFORMACION

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

Teniendo en cuenta lo anterior se puede determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, unos archivos, servidores web o aplicaciones claves para que la entidad pueda prestar sus servicios). Así la entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Para la fase de identificación de activos de información, se tomará como base de referencia el catálogo de servicios tecnológicos y sus fichas de servicio con los que cuenta la secretaría TI:

Correo electrónico Institucional				
Descripción	<p>Permitir a los usuarios de la Gobernación del Quindío el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilite el desarrollo de sus funciones.</p> <p>Aplica a todos los usuarios que tengan un vínculo con la Gobernación del Quindío, usuarios tales como</p> <p>Funcionarios en todos los niveles (Carrera administrativa, provisionales, libre nombramiento, Contratistas etc)</p> <ul style="list-style-type: none"> - El tamaño del buzón tiene una capacidad de 20GB. - La capacidad de envío y recepción de archivos adjuntos es de 25MB -La cuenta de correo electrónico es creada como nombre.apellido@imprensa.gov.co 			
Tipo	<i>Cliente interno</i>	<i>Cliente externo</i>	<i>infraestructura</i>	<i>soporte</i>
	X			
Categoría	Correo (e-mail)			
Servicio de soporte	SECRETARIA TIC <i>Email: intranet@quindio.gov.co ></i>			



Responsable	<i>Director de sistemas de información e infraestructura tecnológica</i> <i>Email: dirsistemas@quindio.gov.co ></i>			
impacto				
Prioridad	<i>[Critica]</i>	<i>[Alta]</i>	<i>[Media]</i>	<i>[Baja]</i>
			X	
Horas de servicio	< Las24 horas del día, los 7 días de la semana.>			

Intranet				
Descripción	<p>Establecer un sistema de gestión y comunicación interna para todas las áreas y usuarios de la Gobernación del Quindío de una forma ágil y segura.</p> <p>la Intranet de la Gobernación del Quindío está compuesta por los siguientes elementos principales: - Mi cuenta: Opciones personales del usuario (información personal, agenda, archivos). - Para Todos: Información publicada por el administrador de la Intranet (clasificados, cumpleaños, foros de discusión, encuestas) - Bandeja de Correo electrónico: Correo de la intranet del usuario (solo para uso de intranet) - Grupos de Trabajo: Grupos a los que pertenece cada usuario. Por defecto es el grupo de la secretaría donde labora y el grupo Gobernación para comunicarse con el resto de funcionarios de la Intranet. - Programador de reuniones: sistema que permite organizar reuniones tanto para el grupo de trabajo propio, como para toda la gobernación (público).</p>			
Tipo	<i>Cliente interno</i>	<i>Cliente externo</i>	<i>infraestructura</i>	<i>soporte</i>
	X			
Categoría	Internet			
Servicio de soporte	< SEVENET®>			
Propietario	<i>SECRETARIA TIC</i> <i>Email: intranet@quindio.gov.co ></i>			
impacto	<A>			
Prioridad	<i>[Critica]</i>	<i>[Alta]</i>	<i>[Media]</i>	<i>[Baja]</i>
	X			
Horas de servicio	< Las24 horas del día, los 7 días de la semana.>			



Página Web					
Descripción	Permite a los usuarios conocer los procesos y estructura organizacional de la Gobernación del Quindío, a través de tecnología web, la divulgación de su gestión e interacción con la ciudadanía.				
Tipo	Cliente interno	Cliente externo	IT	infraestructura	soporte
		X			
Categoría	Internet				
Servicio de Soporte	< SECRETARIA TIC GOBERNACION : Email: tecnologia@quindio.gov.co >				
Propietario	SECRETARIA TIC Email: intranet@quindio.gov.co >				
impacto	<C>				
Prioridad	[Critica]	[Alta]	[Media]	[Baja]	
			X		
Horas de servicio	< Las24 horas del día, los 7 días de la semana >				

PQRDS					
Descripción	Permite a la Gobernación del Quindío la gestión de las peticiones, quejas, reclamos				
Tipo	Cliente interno	Cliente externo	infraestructura	soporte	
	X	X			
Categoría	Internet				
Servicio de soporte	< SECRETARIA TIC GOBERNACION : Email: tecnologia@quindio.gov.co >				
Propietario	SECRETARIA TIC Email: intranet@quindio.gov.co >				
impacto	<C>				
Prioridad	[Critica]	[Alta]	[Media]	[Baja]	
			X		
Horas de servicio	< Las24 horas del día, los 7 días de la semana >				



PCT				
Descripción	PCT Enterprise es un Sistema de Información Administrativo y Financiero exclusivo para el Sector Público. PCT Enterprise está presente en entidades del Sector Público que operan en 23 Departamentos y la ciudad de Bogotá. Actualmente productivo en el 50% de las Gobernaciones de Colombia, 27 Alcaldías Municipales, 15 Corporaciones Autónomas Regionales (44%) y otras entidades públicas de Nivel Central, Territorial y Empresas del Estado.			
Tipo	<i>Cliente interno</i>	<i>Cliente externo</i>	<i>infraestructura</i>	<i>soporte</i>
	X			
Categoría	Aplicación software			
Servicio de soporte	< SOPORTE EN LINEA contactos SKYPE: soporte1@pctlda.com soporte2@pctlda.com soporte3@pctlda.com soporte4@pctlda.com			
Propietario	<PCT LTDA> <NOMBRE>, < Carrera 28 Bis N. 51-08 Bogotá D.C. Colombia - Transversal 18B N. 20B - 14 Valledupar - Colombia Teléfonos: (1) 480 0069 - (1) 480 0046 - (1) 481 1984 Correo Electrónico: pctlda@pctlda.com - www.pctlda.com - Código Postal 111311			
impacto	<A>			
Prioridad	<i>[Critica]</i>	<i>[Alta]</i>	<i>[Media]</i>	<i>[Baja]</i>
	X			
Horas de servicio	< Lunes a Viernes 7:30 a. m. a 12:00 m. - 2:00 p. m. a 6:00 p. m>			

Dominio				
Descripción	Active directory instalado y configurado en la gobernación del Quindío, desde el cual se aplican la mayoría de políticas de seguridad informáticas de la gobernación del Quindío			
Tipo	<i>Cliente interno</i>	<i>Cliente externo</i>	<i>infraestructura</i>	<i>soporte</i>
	X			
Categoría	Aplicación software			
Servicio de soporte	< Microsoft>			
Propietario	< SECRETARIA TIC GOBERNACION : Email: tecnologia@quindio.gov.co >			
impacto	<A>			



Prioridad	[Crítica]	[Alta]	[Media]	[Baja]
		X		
Horas de servicio	< Las24 horas del día, los 7 días de la semana.>			

Correspondencia Sevenet				
Descripción	Permite la incorporar la gestión de los documentos a los procesos de la Gobernación del Quindío, automatizando procedimientos, con importantes ahorros en tiempo, costos y recursos tales como toners de impresora, papel, fotocopias, entre otros, así como el control sobre los documentos.			
Tipo	Cliente interno	Cliente externo	infraestructura	soporte
	X			
Categoría	Aplicación software			
Servicio de soporte	SECRETARIA TIC A través del aplicativo mesa de ayuda			
Propietario	<SEVENET> , <Email: tecnologia@quindio.gov.co>			
impacto	<C>			
Prioridad	[Crítica]	[Alta]	[Media]	[Baja]
			X	
Horas de servicio	<Lunes a Viernes 7:30 a. m. a 12:00 m. - 2:00 p. m. a 6:00 p. m>			

Internet				
Descripción	<p>Permite a los usuarios conocer los procesos y estructura organizacional de la Gobernación del Quindío, a través de tecnología web, la divulgación de su gestión e interacción con la ciudadanía</p> <p>El funcionario y/o contratista solicita el servicio de internet mediante oficio dirigido al secretario TIC.</p> <p>Para brindar conectividad a los funcionarios y/o contratistas en la red Wifi Administrativo, se debe acercar a la secretaria TIC para la asignación voucher.</p> <p>El servicio de internet esta disponible para los funcionarios y/o contratistas de la Gobernación del Quindío</p>			
Tipo	Cliente interno	Cliente externo	infraestructura	soporte
	X			



Categoría	Internet			
Servicio de soporte	<A&A comunicaciones, (06) 741 008 5 321 6443266 Calle 26 No 16 - 25			
Propietario	SECRETARIA TIC Email: dirsistemas@quindio.gov.co >			
impacto	<A>			
Prioridad	[Critica]	[Alta]	[Media]	[Baja]
	X			
Horas de servicio	<Las24 horas del día, los 7 días de la semana>			

Mesa de ayuda				
Descripción	Permite a los usuarios conocer los procesos y estructura organizacional de la Gobernación del Quindío, a través de tecnología web, la divulgación de su gestión e interacción con la ciudadanía			
Tipo	Cliente interno	Cliente externo	infraestructura	soporte
	X			
Categoría	Internet			
Servicio de soporte	SECRETARIA TIC Email: tecnologia@quindio.gov.co link: http://190.90.218.37/mesadeayuda/			
Propietario	SECRETARIA TIC Email: dissistemas@quindio.gov.co >			
impacto	<Descripción del impacto en el negocio en caso de no estar disponible el servicio>			
Prioridad	[Critica]	[Alta]	[Media]	[Baja]
			X	
Horas de servicio	<Lunes a Viernes 7:30 a. m. a 12:00 m. - 2:00 p. m. a 6:00 p. m>			

Copia de seguridad (NAS departamental)	
Descripción	La gobernación del Quindío a través de la Secretaría TIC ha identificado los procesos operativos o de misión crítica que se manejan a través de los diferentes aplicativos de la Entidad, los cuales son respaldados con copias de seguridad diaria, las frecuencias de estas copias fueron

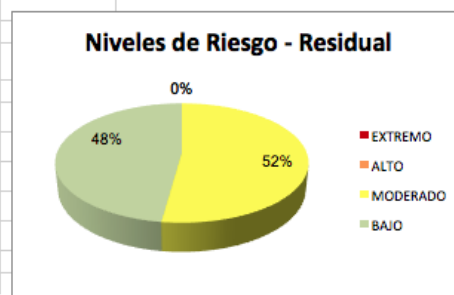
	establecidas por la dirección de sistemas de información e infraestructura tecnológica.			
Tipo	<i>Cliente interno</i>	<i>Cliente externo</i>	<i>infraestructura</i>	<i>soporte</i>
	X			X
Categoría	Backup			
Servicio de soporte	SECRETARIA TIC Email: intranet@quindio.gov.co >			
Propietario	SECRETARIA TIC Email: intranet@quindio.gov.co >			
impacto	<Descripción del impacto en el negocio en caso de no estar disponible el servicio>			
Prioridad	[Crítica]	[Alta]	[Media]	[Baja]
		X		
Horas de servicio	< Lunes a Viernes 7:30 a. m. a 12:00 m. - 2:00 p. m. a 6:00 p. m>			

MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL

A continuación se presenta el mapa de calor del resultado del análisis de riesgos de los activos de información con los que cuenta la gobernación del Quindío.

Impacto \ Probabilidad	1	2	3	4	5
	Insignificante	Menor	Moderado	Mayor	Catastrófico
5 Casi cierto	0 ALTO	0 ALTO	0 EXTREMO	0 EXTREMO	0 EXTREMO
4 Probable	0 MODERADO	0 ALTO	0 ALTO	0 EXTREMO	0 EXTREMO
3 Posible	0 BAJO	3 MODERADO	0 ALTO	0 EXTREMO	0 EXTREMO
2 Poco Probable	1 BAJO	6 BAJO	9 MODERADO	0 ALTO	0 EXTREMO
1 Raro	2 BAJO	2 BAJO	0 MODERADO	0 ALTO	0 ALTO
TOTAL	BAJO 11	MODERADO 12	ALTO 0	EXTREMO 0	

DISTRIBUCIÓN DE RIESGOS - Inherente	
ZONA DE RIESGO	TOTAL
EXTREMO	0
ALTO	0
MODERADO	12
BAJO	11
TOTAL	23





SECRETARÍA TIC



La anterior matriz se pone a disposición y se encuentra anexa a este plan de tratamiento de riesgos de seguridad digital

FASE DE IMPLEMENTACION

Actualmente desde la secretaría TIC de la gobernación del Quindío ya se está haciendo un control sobre los riesgos identificados en las dos matrices de riesgos, reduciendo así la posibilidad de que los riesgos anteriormente mencionados puedan materializarse.

Ahora bien, en esta fase se seguirá la ruta definida para la aplicación de controles, los cuales estarán a cargo de su implementación en los tiempos definidos, los responsables o líderes de proceso con el apoyo de la Secretaría TIC, en lo concerniente a controles tecnológicos e informáticos, también será necesario contar con el apoyo y compromiso del responsable de la seguridad digital (director de sistemas e infraestructura tecnológica) que brinde conocimiento, apoyo y experticia en la aplicación de los controles.

FASE DE SEGUIMIENTO Y CONTROL

De acuerdo al modelo de integrado de planeación y gestión MIPG, la entidad debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad.

Dado que el origen y tipos de riesgos son variables, el monitoreo constante será necesario para detectar cambios respecto a nuevos activos de información, nuevos procesos o procedimientos, nuevos factores o amenazas que afecten los activos de información, nuevas vulnerabilidades, incremento del impacto e incluso la materialización de incidentes de seguridad.

REPORTE Y SOCIALIZACION DE RIESGOS DE SEGURIDAD

A la fecha, la secretaría TIC ha gestionado eventos e incidentes que han afectado la seguridad en la entidad con un impacto bajo, tratando de mitigar y trasladar los riesgos, por lo que no ha sido necesario aún realizar reporte al Centro Cibernético Policial y al Equipo de Respuesta a Incidentes de Seguridad Informática CSIRT.

Por otra parte desde la secretaría TIC se trabajará de manera eficaz con los funciona funcionarios, gestores de proceso y la dirección de sistemas e infraestructura tecnológica para la restauración de los activos de información afectados por el incidente y como acciones de mejora para prevenir futuras recurrencias del incidentes, se trabajará en la identificación de causa raíz e



Departamento del Quindío



SECRETARÍA TIC



implementación de mejoras y controles que ayuden a la protección de los distintos activos de información.

Se realizará la comunicación respectiva, de la mano con el plan de sensibilización y comunicación de las políticas de seguridad de la información, para capacitar a los funcionarios y que ellos sepan reportar de manera correcta un evento o riesgo de seguridad el cual pueda comprometer la integridad de los sistemas de información de la gobernación del Quindío.

AUDITORÍAS INTERNAS Y EXTERNAS

Se espera que desde la Oficina Asesora de Control Interno realice el seguimiento a las acciones de mejora necesarias para lograr una efectiva gestión de riesgos de seguridad digital y permita esto salvaguardar los activos de información de la entidad.

FASE DE MEJORAMIENTO CONTINUO DE LA GESTION DE REISGOS DE SEGURIDAD DIGITAL.

La secretaría TIC, trabajará en la mejora continua de la gestión de riesgos de seguridad digital, como parte del modelo de seguridad y privacidad de la información MSPI, velando por la mitigación de vulnerabilidades, amenazas, riesgos, eventos e incidentes que atenten contra la disponibilidad, integridad y confidencialidad de los datos e información asociada a los distintos activos de información como parte de los procesos de la entidad y se llevaran a cabo las acciones necesarias para atender los hallazgos o no conformidades producto de auditorías internas y externas.



BIBLIOGRAFÍA

Guía para la administración del riesgo y el diseño de controles en entidades públicas. (2018). *Departamento de la función pública*. Obtenido de Función pública:



<http://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+3+Identificacio%C2%B4n+de+Riesgos+de+Corrupcio%C2%B4n+asociados+a+la+Prestaci%C3%B3n+de+Tra%C2%B4mites+y+Servicios+-+Gu%C3%ADa+de+Riesgos+2018.pdf/a491717d-7d0d-8ada-32f6-e0f62afb0625>

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (20 de Mayo de 2016). *NORMA TÉCNICA COLOMBIANA NTC/ISO-IEC 27000. NORMA TÉCNICA COLOMBIANA NTC/ISO-IEC 27000*. Bogota, DC, Colombia: ICONTEC INTERNACIONAL. Obtenido de Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (20 de Mayo de 2018). *LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS. LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS*. Bogota , DC, Colombia.

TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS. (2006). *Icontec*. Obtenido de Bogota turismo: <http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf>


JAIME ALBERTO LLANO CHAPPARO
Secretario TIC
Departamento del Quindío

Elaboro: Andrés Felipe Barrera Pérez – Ingeniero, Contratista 
Aprobó: Jesús Ignacio Moncaleano Caicedo – Director de Gobierno Digital 

CONTROL DE CAMBIOS		
VERSION	FECHA	DESCRIPCION DE LA MODIFICACION
VERSION 1.0	15/05/2018	Creación primera versión del documento
VERSION 2.0	21/05/2019	Implementación de riesgos de seguridad digital