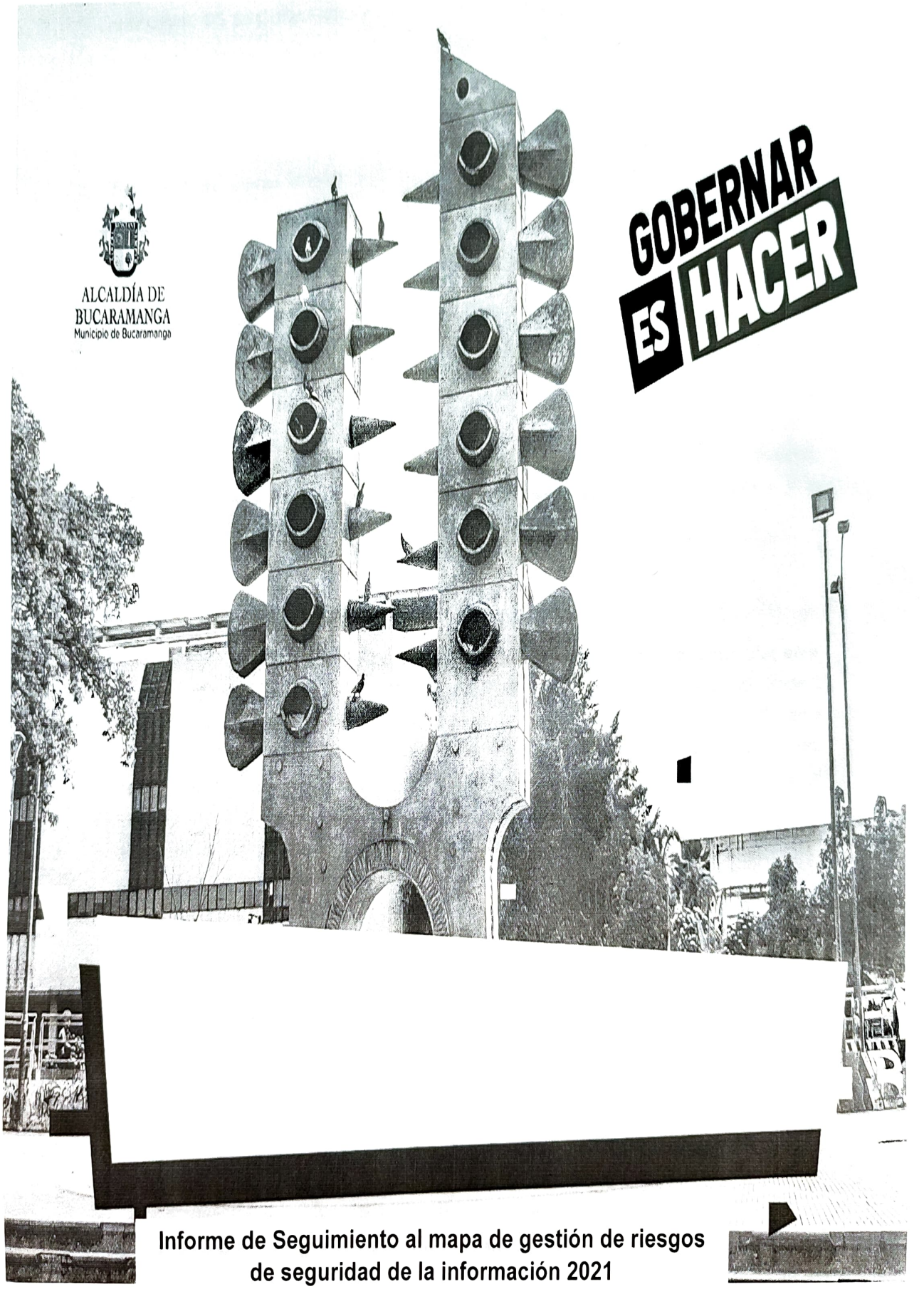


Informe de Seguimiento al mapa de gestión de riesgos de seguridad de la información 2021

Oficina de Control Interno de Gestión a

Marzo 30 de 2022

INFORME DE SEGUIMIENTO AL MAPA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

VIGENCIA 2021

Bucaramanga, marzo 30 de 2022.

EQUIPO DE SEGUIMIENTO

CLAUDIA ORELLANA HERNANDEZ. Jefe Oficina Control interno de Gestión.
WILSON CASTAÑO GALVIZ. Contratista Profesional OCIG.

OBJETIVO

Realizar seguimiento al mapa de gestión de riesgos de seguridad de la Información, correspondiente a la Oficina Asesora de las Tecnologías de la Información y la Comunicación (OATIC) con corte a 31 de diciembre de 2021.

DESARROLLO DEL SEGUIMIENTO

Con la expedición del Decreto 1499 de 2017 (cuyas disposiciones fueron compiladas en el Decreto Único Reglamentario del Sector Función Pública 1083 de 2015, Título 22, Parte 2 del Libro 2), el Departamento Administrativo de la Función Pública, se definió el Sistema Integrado de Planeación y Gestión y actualizó el modelo para su implementación, denominado "Modelo Integrado de Planeación y Gestión" (MIPG), el cual corresponde al "marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio"

Este modelo de planeación y gestión plantea diecisiete políticas de gestión y desempeño institucional conlleva a un parámetro específico dentro del cual establece el Eje de Gestión para el Resultado con Valores que conlleva al planteamiento de "Gobierno Digital", el cual obliga a la implementación de los lineamientos de seguridad de la información dentro de las entidades del estado, en el cual este último posea al menos el 90% de su propiedad.

Dentro de Gobierno Digital se ha establecido el Modelo de Seguridad y Privacidad de la Información, con el cual se especifican los lineamientos para proteger la información de las entidades del estado y dentro de estos lineamientos se tiene la estructuración de un mapa de gestión de riesgos de seguridad de la información, el cual es el objetivo de este seguimiento dentro de la Alcaldía de Bucaramanga.

La misma OATIC ha definido los criterios de evaluación del riesgo de seguridad digital, indicando que la evaluación de los riesgos de seguridad de la información se debe enfocar en:

• El valor estratégico del proceso de información en la Alcaldía de Bucaramanga.

• La criticidad de los activos de información involucrados.

• Los requisitos legales y reglamentarios, así como las obligaciones contractuales.

• La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la Alcaldía de Bucaramanga.

• Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la Alcaldía de Bucaramanga.

Los criterios de impacto se deben especificar en términos del grado, daño o de los costos para la Alcaldía de Bucaramanga, causados por un evento de seguridad de la información, considerando aspectos tales como:

• Nivel de clasificación de los activos de información impactados.

• Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad).

• Operaciones deterioradas (afectación a partes internas o terceras partes).

• Pérdida del negocio y del valor financiero.

• Alteración de planes o fechas límites.

• Daños en la reputación.

• Incumplimiento de los requisitos legales, reglamentarios o contractuales.

Antes de identificar y evaluar de los riesgos de seguridad digital, es necesario identificar los activos de información de la Alcaldía de Bucaramanga, posterior a ellos se requiere identificar los riesgos por cada activo (o grupos de activos) de información, para esto se recomienda usar el modelo para mapas de riesgos definidos por el Mintic.

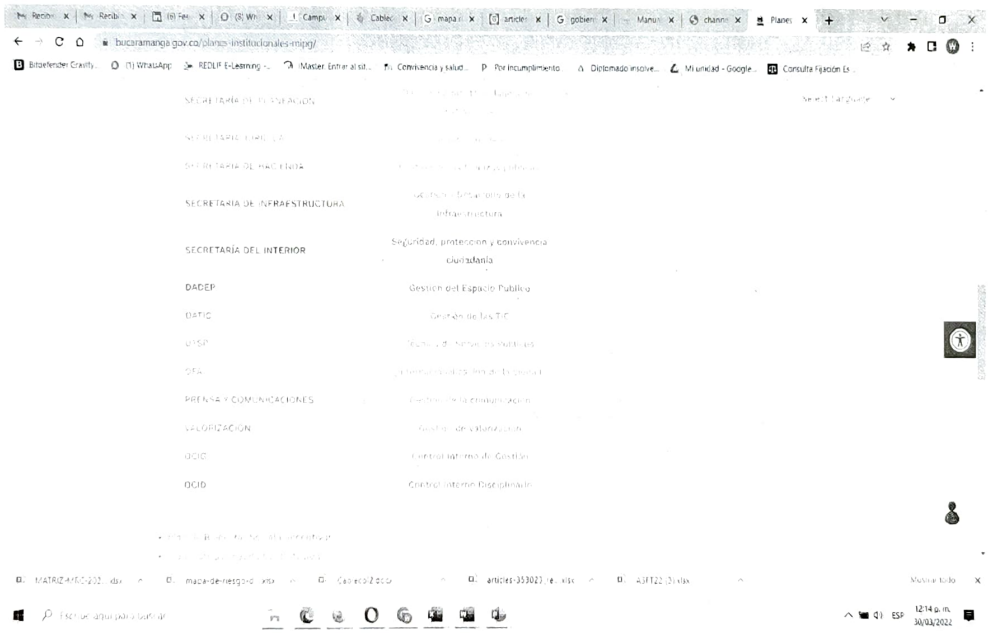
Después de tener una relación con todos los activos, se deben identificar las amenazas que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños, para esto se recomienda usar una metodología para el análisis de riesgos de seguridad digital, la norma "ISO 27005" o la metodología de análisis y gestión de riesgos "Magerit".

Una vez se haya clasificado el listado de activos, sus amenazas y las medidas que ya se han tomado, es necesario revisar las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de la Alcaldía de Bucaramanga.

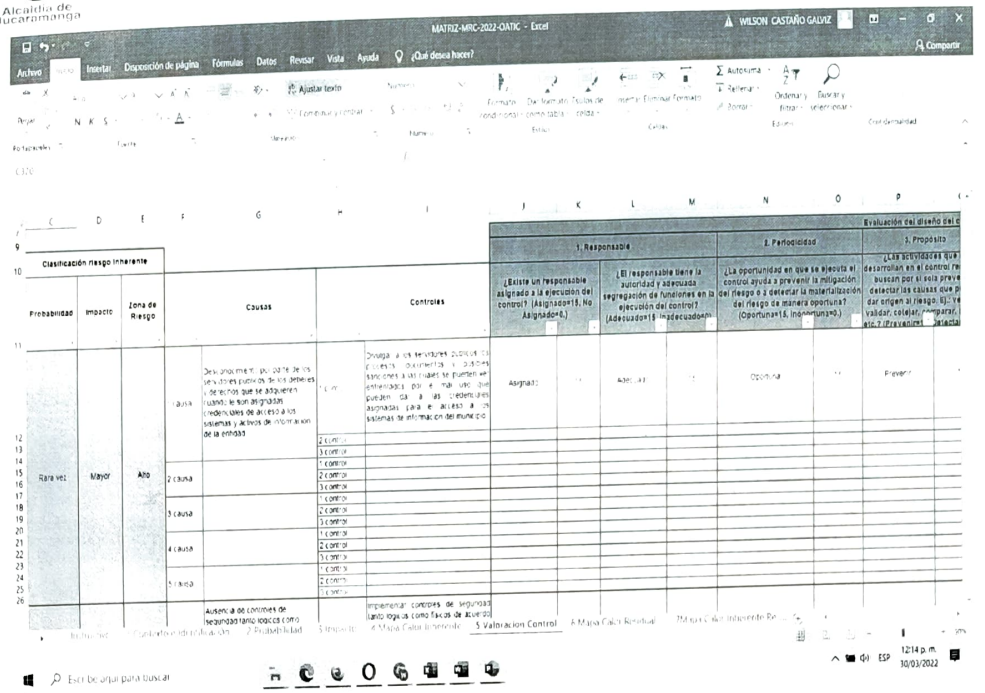
El día 28 de marzo de 2022, se lleva a cabo reunión con personal adscrito a la OATIC, se realizó el seguimiento a la estructuración y puesta en funcionamiento del mapa de gestión de riesgos de seguridad de la información, se presentaron los informes que corresponden a la estructuración de los riesgos de seguridad de la información que han sido reportados en el año 2021 en los siguientes informes:

- ✓ Política de gestión de riesgos de la entidad en el capítulo 9.4 donde se establecieron los lineamientos para los riesgos de seguridad de la información, de acuerdo a las recomendaciones del DAFP.
- ✓ En el mapa de gestión de riesgos del año 2021 están identificados los riesgos, con su contexto, probabilidad de impacto y planes de acción, los cuales fueron monitoreados y revisados.
- ✓ En el mapa de riesgos de corrupción del año 2021, también están identificados los riesgos, los cuales fueron monitoreados y revisados

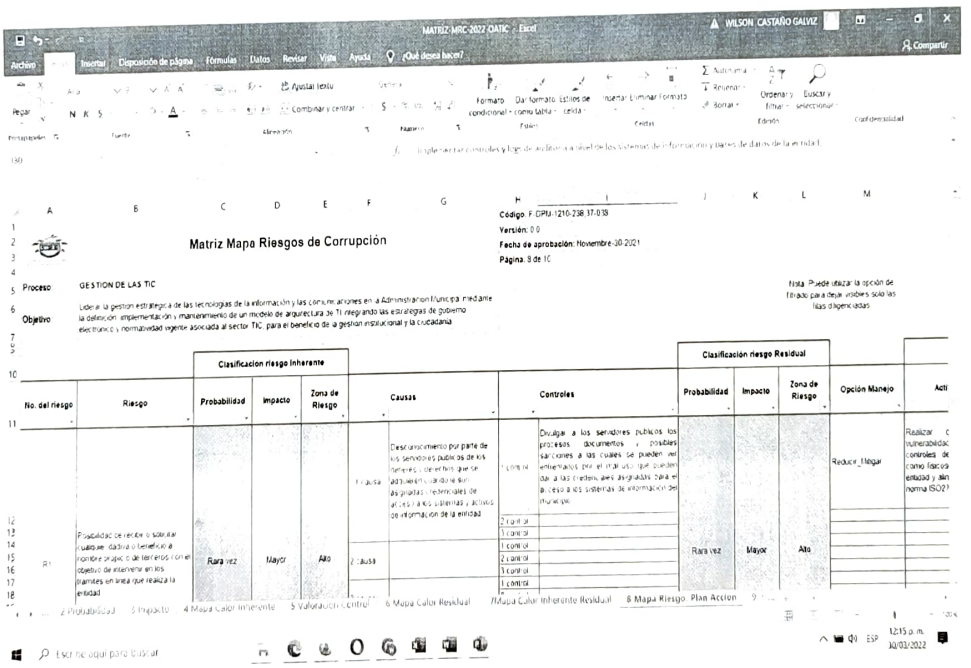
Una vez revisada la información, se procede a verificar su publicación en la página web de la Alcaldía de Bucaramanga, encontrando los siguientes documentos publicados por la OATIC:



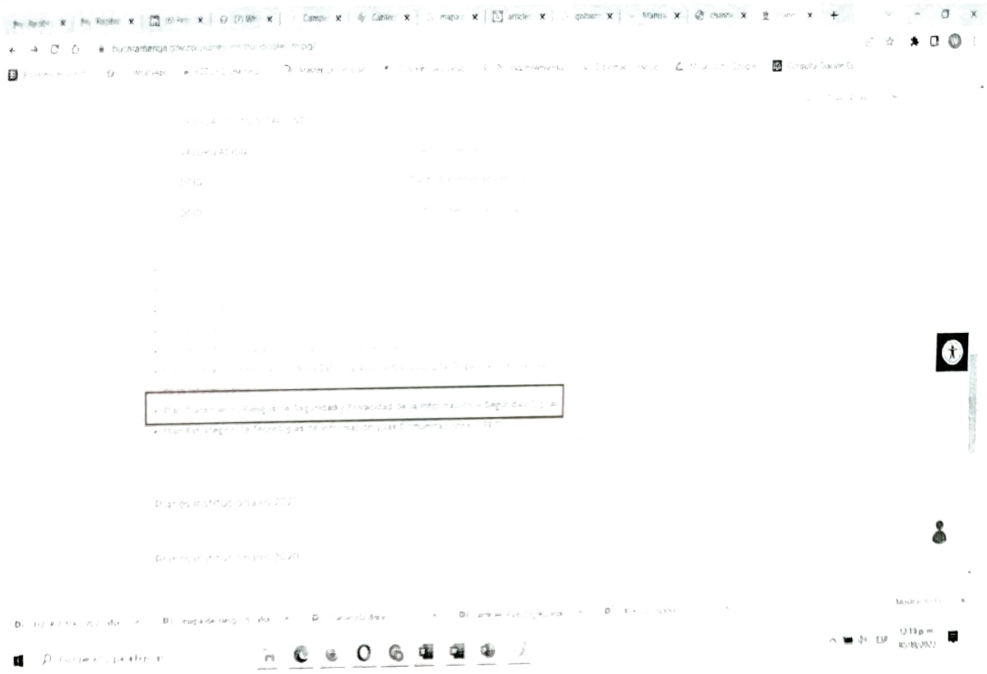
En este link, se puede descargar un archivo en formato .xls, que contiene los diferentes riesgos de seguridad de la información definidos para la Alcaldía de Bucaramanga.



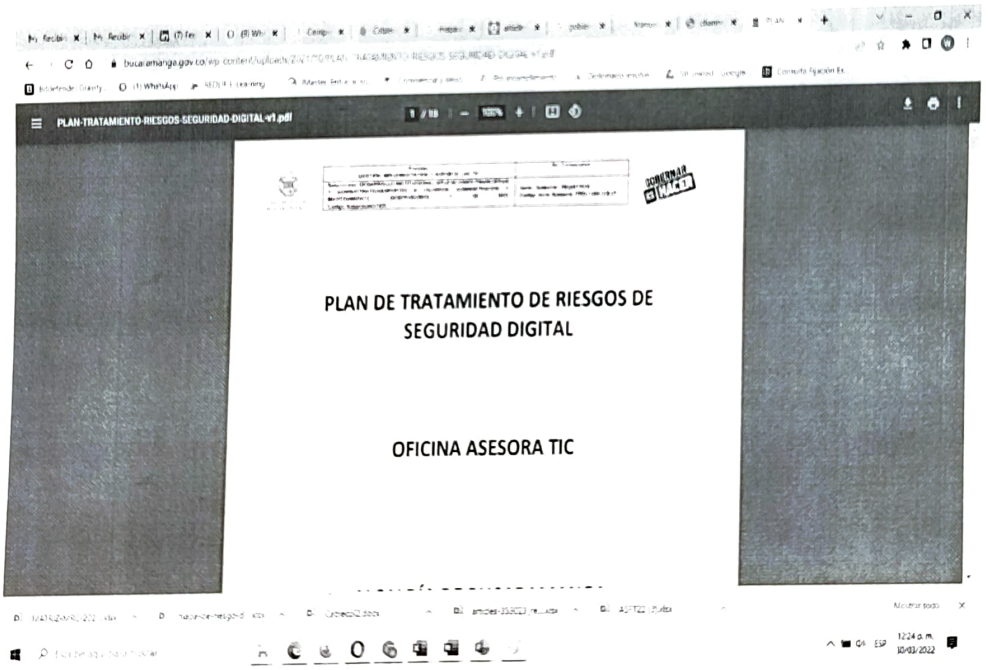
En este documento, también están definidos los riesgos de corrupción que tienen influencia en la seguridad de la información, tal como se puede observar en la siguiente imagen:



También se encuentra publicado el Plan de Tratamiento Riesgos de Seguridad y Privacidad de la Información – Seguridad Digital, la cual se puede acceder desde la página web de la Alcaldía de Bucaramanga, tal como se observa en la siguiente imagen:



Se cuenta con un documento que sigue el formato: Serie / Subserie: REGISTROS, Código Serie-Subserie /TRD) 1400-238.07, el cual se puede observar en la siguiente imagen:



Cabe destacar que pese a que una vez corroborada esta información y además de lo correspondiente a documentos de registros de activos de información e índice de información clasificada y revisada para la vigencia 2021, los cuales conforman el inventario de activos de información, se hace necesario que se utilice el documento tipo "Inventario y clasificación de activos de información", pero se determina que, aunque la información está distribuida en los 3 documentos anteriores, el mapa de riesgos de seguridad de la información, no se encuentra consolidada en este documento tipo.

RECOMENDACIONES

Se evidencia que ya existe el listado de activos, riesgos de seguridad y tratamiento de riesgos de seguridad de la información, es necesario que se consolide la información correspondiente a: inventario de activos, riesgos de seguridad de la información y tratamiento de riesgos de seguridad de la información en el documento tipo "Inventario y clasificación de activos de información" quedando como compromiso a que se entregará a más tardar el día 30 de abril de 2022 por parte de la OATIC.

Según el documento Plan Tratamiento Riesgos de Seguridad y Privacidad de la Información – Seguridad Digital que se encuentra publicado en la página web de la Alcaldía de Bucaramanga, para realizar el análisis de riesgo de los procesos, se utiliza el "Formato Consolidado Calificación del Riesgo" (OATIC-F-001) en el cual personas del equipo deberán calificar el impacto y la probabilidad de cada uno de los riesgos identificados de acuerdo con los niveles para la estimación de los riesgos que deberán ser tomados del documento - Manual para la Administración de Riesgos y Oportunidades y medidas de anticorrupción de la Alcaldía de Bucaramanga, pero para el mapa de riesgos de seguridad de la información, se recomienda usar el formato definido por el Mintic, el documento tipo para los activos de información y el mapa de riesgos de seguridad de la información.

Se recomienda que la persona encargada de seguridad de la información, al interior de la OATIC, coordine la estructuración de los activos de información y el mapa de gestión de riesgos de la información, toda vez que se requiere que lo gestione una persona con altos conocimientos en seguridad de la información, utilizando como metodología para tratamiento de riesgos de la información, la norma "ISO 27005" o la metodología de análisis y gestión de riesgos "Magerit".

Las recomendaciones anteriormente mencionadas se realizan desde el rol de liderazgo estratégico con enfoque hacia la prevención y evaluación de la gestión del riesgo de seguridad de la información y no tiene otro fin que el de sugerir a la OATIC de la Administración Municipal, a que implemente buenas prácticas y acciones de mejora que pueden ayudar a evidenciar de manera efectiva el cumplimiento de las metas de acuerdo a lo establecido en los indicadores, contribuyendo de esta manera a un proceso de mejora continua institucional.

CLAUDIA ORELLANA HERNANDEZ
Jefe de Oficina de Control Interno de Gestión
Alcaldía de Bucaramanga

Proyectó: Wilson Castaño Galviz. CPS Profesional OCIG.