

IDENTIFICACIÓN DE RIESGOS Y DAÑOS EN LA GESTIÓN DE DOCUMENTOS
INFORMÁTICOS EN CORANTIOQUIA

ALEYDES ALEXANDRA VÉLEZ SÁNCHEZ

UNIVERSIDAD DE ANTIOQUIA

ESCUELA INTERAMERICANA DE BIBLIOTECOLOGÍA

ARCHIVÍSTICA

MEDELLÍN - 2019

IDENTIFICACIÓN DE RIESGOS Y DAÑOS EN LA GESTIÓN DE DOCUMENTOS
INFORMÁTICOS EN CORANTIOQUIA

ALEYDES ALEXANDRA VÉLEZ SÁNCHEZ

Trabajo presentado como requisito para optar al título de
Archivista

Director: Mauricio Fino Garzón

Profesional en Ciencia de la Información – Bibliotecólogo

UNIVERSIDAD DE ANTIOQUIA

ESCUELA INTERAMERICANA DE BIBLIOTECOLOGÍA

ARCHIVÍSTICA

MEDELLÍN - 2019

Contenido

1. Introducción	5
1.1. Contexto	6
1.2. Planteamiento del problema.....	8
1.3. Objetivos	10
1.3.1. General	10
1.3.2. Específicos	10
1.4. Justificación.....	10
1.5. Pregunta de investigación	12
2. Marco Teórico.....	13
3. Metodología	18
4. Resultados Y Discusión	23
4. 1. Componente Cualitativo	24
4. 1. 1. Ciberataques	25
4. 1. 2. Procesos de migración de datos	27
4. 1. 3. Programa de Gestión Documental	27
4. 1. 4. Política de seguridad informática.....	28
4. 2. Componente cuantitativo	29
4.3. Análisis al proyecto de política de seguridad de la información.	38
5. Conclusiones y Recomendaciones	41

6. Bibliografía 44

7. Anexos 49

1. Introducción

En este trabajo se expone el proceso de indagación sobre los riesgos y daños en la gestión de documentos informáticos ocurridos en la Corporación Autónoma Regional del Centro de Antioquia (CAR CORANTIOQUIA) en los últimos años, mediante un enfoque investigativo mixto, toda vez que en éste, se combinó el método de estudio de caso, como herramienta de aproximación cualitativa, con la encuesta no probabilística, a su vez como herramienta de aproximación cuantitativa.

La presentación de este proceso de indagación se ha seccionado siguiendo un orden lógico de cuatro apartados principales. En el primer apartado (Introducción), se contextualiza y enmarca el objetivo de indagación, con el propósito de facilitar el acercamiento de los lectores, a la visión de quien investigada y propiciar una mejor contextualización. De esta manera, el contenido presenta los rasgos generales de los procesos de gestión de información digital CORANTIOQUIA.

En la sección Planteamiento del Problema, se hace un breve recuento sobre la problemática a nivel mundial y nacional en cuanto a seguridad informática; en este aparte, se registran algunos datos estadísticos y ejemplos al respecto.

Tanto en la sección Objetivo como en la Justificación, se expresa de forma explícita la motivación que dirige el estudio y a su vez muestra, cómo la revisión crítica de las eventualidades sufridas en los procesos de gestión documental, se constituye en una acción contingente para el fortalecimiento de CORANTIOQUIA; así como, la adaptabilidad de la entidad ante las amenazas informáticas y la obsolescencia de los recursos digitales. De ahí que, cerrando la parte introductoria, se delimita formalmente la pregunta de investigación.

En el Marco Teórico, se exponen las herramientas conceptuales necesarias para la interpretación del proceso de indagación, procurando hacer una delimitación y clasificación de los

conceptos claves, en particular en lo relacionado con la gestión de documentos informáticos, seguridad informática, la migración de datos, las bases de datos y la obsolescencia de recursos digitales.

En el tercer apartado (Metodología), se puntualizan las técnicas de recolección de información desplegadas, consistentes en la revisión de archivos, la indagación a los empleados del área de informática de CORANTIOQUIA y la aplicación de una encuesta semiestructurada, cuya muestra está dirigida hacia a los empleados que utilizan cotidianamente los recursos informáticos de la entidad, en el ejercicio de sus funciones.

Finalmente en los Resultados y Conclusión del proyecto, se presentan los aspectos relevantes de la información recolectada, se reseñan los daños y riesgos identificados durante la gestión documental digital de CORANTIOQUIA en los últimos años y se revisa si las políticas de seguridad informática y gestión documental de la entidad, atienden los riesgos y daños observados.

1.1. Contexto

La Corporación Autónoma Regional del Centro de Antioquia (CAR CORANTIOQUIA) tiene como misión “Contribuir al logro del desarrollo sostenible, mediante el conocimiento y mejoramiento de la oferta ambiental y la administración del uso de los recursos para responder a su demanda, a través de la construcción de una cultura ambiental del territorio” (CORANTIOQUIA, 2017). A esta misión está ligada de forma inherente la necesidad de almacenar, procesar y difundir información de forma eficiente y flexible, respetando siempre los principios y procesos archivísticos, para que ésta esté a disposición de sus diferentes oficinas, desplegadas por ocho territoriales, que abarcan los ochenta municipios que están bajo su jurisdicción, además de las oficinas centrales ubicadas en la capital del departamento.

Para hacer frente a la misión corporativa, CORANTIOQUIA ha desarrollado algunas herramientas y estrategias informáticas, como por ejemplo las bases de datos e-Sirena (<http://sirena.corantioquia.gov.co/esirena/>) y SIRENA

(<https://aplicaciones.corantioquia.gov.co/RDWeb/Pages/en-US/login.aspx?ReturnUrl=/RDWeb/Pages/en-US/Default.aspx>), así como también su portal oficial.

En este contexto, e-Sirena es un aplicativo web en el cual los usuarios registrados en la entidad (solicitantes de trámites, funcionarios de alcaldías municipales, empleados de empresas generadoras de energía, clientes de laboratorio, proveedores de los viveros, entre otros), encuentran un canal de comunicación virtual, con la Corporación. Por ello, cualquier persona puede acceder a este aplicativo, en lo que necesita registrar un perfil de usuario y obtener y aplicar una contraseña.

De otro lado, Sirena es una base de datos cerrada (ya que solo los empleados de la entidad tienen acceso mediante un perfil de usuario asignado y su respectiva contraseña), cuya naturaleza privada, tiene lugar a que, a su interior se maneja la totalidad de la información técnica de carácter confidencial.

En el portal oficial *Corantioquia* (<https://www.corantioquia.gov.co>) se enlaza multitud de aplicativos, con el objetivo de facilitar a los usuarios toda la información de interés, tanto de proyectos como de trámites ambientales; así mismo, las políticas, mecanismos de participación e incluso brinda la posibilidad de realizar pagos. En este portal se puede navegar libremente, sin la necesidad de la creación de un perfil de usuario; no obstante, al realizar el registro completo, se amplían las posibilidades de uso de la herramienta.

De esta forma, es previsible que la entidad no esté exenta de riesgos por pérdida de datos; lo anterior, debido a los posibles ataques cibernéticos o en los procesos de migración, es posible que se presenten pérdidas, por la obsolescencia de los soportes físicos o virtuales. De hecho, como precedente a esta investigación, se conoce por comunicación directa con funcionarios de la entidad, que en 2015 y 2016, CORANTIOQUIA sufrió daños por ataques informáticos. Este hecho alerta la necesidad de revisar críticamente lo ocurrido, con el fin de descubrir oportunidades de mejoramiento, desarrollar estrategias de fortalecimiento y proponer acciones de mitigación de riesgos.

1.2. Planteamiento del problema

A la vez que las TIC cuentan con beneficio que se brinda al proceso de gestión documental, el uso de éstas conlleva inevitablemente una variedad de riesgos asociados, los cuales exigen adoptar estrategias tendientes a su minimización. Estos riesgos pueden clasificarse en dos categorías: la primera, relacionada con la seguridad informática y la legitimidad de la información; la última, relacionada con la eventual obsolescencia de los soportes físicos y virtuales.

Entre los riesgos más notorios de la primera categoría, se encuentran registrados los ciberataques, el fraude y la violación de derechos de autor. Así, por ejemplo, la compañía Cybersecurity Ventures ha señalado que “El fraude virtual, solo durante el 2016, causó pérdidas por 1.500 millones de dólares; ello, teniendo en cuenta la pérdida de productividad, la investigación y la recuperación de los datos” (Portafolios, 2017).

En el mismo sentido, la empresa de seguridad informática SonicWall afirmó sobre los ciberataques que “Uno de los aspectos que más preocupa es la forma como se han incrementado este tipo de ataques, mientras en el 2015 se registraron 3,8 millones de casos en el mundo, la cifra pasó a 638 millones en el 2016” (Portafolio, 2017).

Por ejemplo, en 2017 miles de computadoras alrededor del mundo fueron infectadas de manera simultánea por el virus WANNACRY, un tipo de malware conocido como ransomware, cuyo objetivo consiste en cifrar la información resguardada en un equipo de cómputo y exigir un pago a cambio de la herramienta para recuperar los archivos comprometidos (Reyes y Salinas, 2017).

Durante este ataque se vieron afectadas empresas, instituciones educativas, hospitales y oficinas de gobierno, entre otras, en alrededor de cien países, convirtiéndose así en la mayor infección por ransomware de la historia (Reyes y Salinas, 2017). A nivel nacional, en 2017 *“La Policía reportó que las arcas públicas perdieron al menos 50.000 millones de pesos, en especial por causa de accesos abusivos a las cuentas de distintas alcaldías por todo el país”* (Semana, 2017).

Para visualizar el panorama nacional en cuanto a seguridad informática, basta con mencionar algunas estadísticas. En 2016 la Fiscalía abrió 8.682 investigaciones por ciberdelitos (El Tiempo, 2018). En 2017 dichos delitos se incrementaron a 11.332, lo que representa un aumento del 31 % y puede traducirse a un promedio de 31 casos diarios (El Tiempo, 2018). Para agosto de 2018 la Fiscalía reportó la ocurrencia de 8.000 casos de hurto por medios informáticos, 2.000 por violación de datos personales y otros 2.000 por acceso abusivo a un sistema informático (Caracol Radio, 2018). Hasta dicha fecha se habían recibido 15.181 denuncias, lo que quiere decir que cada hora al menos tres colombianos fueron víctimas de los hackers (Caracol Radio, 2018). Al cerrar el 2018 las cifras se hicieron más contundentes: fueron denunciados 21.687 casos de Ciberdelitos, lo que implica un incremento del 36% frente al 2017 (Enter.Co, 2019). Según esta cifra, cada día se denuncian 60 nuevos casos por ataques cibernéticos a ciudadanos y empresas (Enter.Co, 2019). Según estas cifras, pese a las medidas de las autoridades, la ciber delincuencia en Colombia parece crecer de forma exponencial.

Adicionalmente, sumándose a los riesgos de seguridad informática, por su naturaleza, los archivos digitales están sujetos a riesgos por el deterioro y desactualización de sus soportes físicos y virtuales, lo cual constituye todo un fenómeno económico típico de la era digital, conocido como obsolescencia. Cuando los sistemas informáticos quedan obsoletos, se hace necesario reemplazar y hacer migración de datos a la nueva tecnología entrante, lo cual, además de los costos, acarrea la posibilidad de pérdida de información.

Como ya se mencionó, en el caso particular de CORANTIOQUIA, se conoció en 2015 y 2016 que la entidad sufrió daños por ataques informáticos, lo cual ha motivado la realización de esta indagación, al considerar que la revisión crítica de las eventualidades que se experimentaron permite descubrir oportunidades de mejoramiento y es, lógicamente, el primer paso para desarrollar estrategias de fortalecimiento y mitigación de riesgos.

1.3. Objetivos

1.3.1. General

Identificar los riesgos generados por el uso de las tecnologías de información y comunicación en la gestión documental durante los últimos años en CORANTIOQUIA.

1.3.2. Específicos

- Analizar los procesos de gestión documental electrónica durante los últimos años en el archivo de CORANTIOQUIA.
- Recopilar información sobre situaciones específicas de pérdida de información, cuando se han realizado acciones de migración en las bases de datos y ataques cibernéticos durante los últimos años en CORANTIOQUIA.
- Revisar la articulación entre las políticas de seguridad informática y los eventos de daño y pérdida de información electrónica durante los últimos años en CORANTIOQUIA.
- Aportar ideas para el fortalecimiento de la gestión documental de CORANTIOQUIA, con base en la identificación de debilidades manifiestas y riesgos evidenciados durante los últimos años.

1.4. Justificación

La importancia de las TIC ha sido reconocida por diversas entidades, como, por ejemplo, el Ministerio de las Tecnologías de la Información y de las Comunicaciones y el Archivo General de la Nación.

Como manifestación de este reconocimiento, en el año 2000 la Ley 594, por medio de la cual se dicta la Ley General de Archivos, dio vía libre a las entidades públicas para usar los medios tecnológicos en el proceso de gestión documental, además de orientar y regular su uso, al señalar que en todo caso “deberán observarse los principios y procesos archivísticos”.

Estos reportes llevan a enfatizar la necesidad de que las entidades cuenten con protocolos y políticas de seguridad informática, tendientes a evitar los ciberataques, garantizar la autenticidad, verificar la legalidad y evitar al máximo la pérdida de datos, evadiendo así fallas de funcionamiento y pérdidas económicas asociadas.

Tales dificultades han llamado la atención gubernamental, tanto a nivel mundial como nacional. Así por ejemplo, la Organización de las Naciones Unidas (ONU) en su 13° Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 2015, desarrolló un seminario en el cual se actualizó la definición de delitos informáticos, se tipificaron dichos delitos, se discutió sobre las mediciones de las frecuencias de ocurrencia de ciberdelitos y se brindaron orientaciones para hacerle frente a la ciberdelincuencia (Organización de las Naciones Unidas, 2015).

En el mismo sentido, en Colombia se expidió la ley 1273 de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la Protección de la información y de los datos”. Sin embargo, tales avances en materia de legislación y penalización no parecen incidir en la disminución de los casos de ciberataques, por tanto, las entidades deben prevenirse de los riesgos, adelantando acciones propias tendientes a minimizarlos.

Para proteger la información digital, tanto de los ciberataques, como de los procesos de migración de datos, se hace necesario que las entidades cuenten con una oficina de seguridad informática que trabaje de manera articulada con el área de archivo, la adquisición de equipos y programas informáticos que cumplan los requisitos técnicos y funcionales y buenas prácticas en el manejo documental por parte de los empleados, todo lo cual debe ser consignado en un plan de gestión documental electrónica, que además debe recoger políticas y protocolos de seguridad informática. Adicionalmente es perentorio que ante ataques y daños experimentados, las entidades revisen esmeradamente los hechos para luego enfocarse en la identificación de debilidades y diseñar estrategias de mejoramiento bien fundamentadas. Es previsible que hacer lo contrario, es decir, desatender las malas experiencias en la gestión de archivos informáticos,

conlleve inevitablemente a la maximización de los daños, pérdidas y contrariedades en la gestión documental y puede ir convirtiendo el uso de las TIC en un obstáculo en vez de un aliado al servicio de los objetivos de gestión.

Para el caso particular de CORANTIOQUIA, los antecedentes de ataques informáticos conocidos por comunicación directa con funcionarios de la entidad, han motivado la realización de esta indagación, al considerar que la revisión crítica de las eventualidades que se experimentaron permite descubrir oportunidades de mejoramiento y es, lógicamente, el primer paso para desarrollar estrategias de fortalecimiento y mitigación de riesgos.

1.5. Pregunta de investigación

Teniendo como base las consideraciones antes relacionadas, se hace factible y necesario especificar la pregunta de investigación, sin dejar de lado la necesidad de sintetizar los elementos contextuales que delimitan el objeto de interés de esta indagación.

Como primer elemento puede considerarse el aspecto funcional, el cual puede ser enunciado como el análisis de riesgos y daños informáticos en la gestión documental. De ahí que, el segundo elemento puede referirse a la delimitación espacial (definida para este caso, como la Corporación Autónoma Regional del Centro de Antioquia -CAR CORANTIOQUIA).

Por último, se hace necesario definir el proceso de delimitación temporal, que para este caso (como se expresó en la sección Objetivos), cuenta con un límite inicial, trazado en 2015 y un límite final, que irrumpe a mediados de 2019.

Con la fusión de los tres elementos en comento, se hace posible formular de manera concisamente, la pregunta de investigación objeto de este trabajo: ¿Cuál es el origen de los riesgos y daños sufridos en la gestión de documentos informáticos, ocurridos en CORANTIOQUIA entre 2015 y 2019?

2. Marco Teórico

Autores como Bosco (1995) y Adell (1997), dividen la historia del hombre en función de cómo se realiza la transmisión, codificación y tratamiento de la información, exaltando los cambios radicales que produce en la organización social, la organización del conocimiento y las habilidades cognoscitivas del hombre, moldeando su propia identidad.

En la actualidad, las Tecnologías de la Información y la Comunicación (TIC), han transformado particularmente la forma de gestionar los procesos documentales en las entidades; gracias a que permiten automatizar y flexibilizar los procesos de almacenamiento, procesamiento y difusión de información, propiciando de esta forma la eficiencia y competitividad.

En referencia a una tendencia más cuantitativa, el Banco Mundial ha definido el nivel de acceso que los países tienen a las TIC, como uno de los cuatro pilares para medir su grado de avance en el marco de la economía del conocimiento (World Bank Institute, 2008); pero ¿Qué son las TIC?. Fernández (2005), las definió como "(...) innovaciones en microelectrónica, computación (hardware y software), telecomunicaciones y optoelectrónica -microprocesadores, semiconductores, fibra óptica - que permiten el procesamiento y acumulación de enormes cantidades de información, además de una rápida distribución de la información a través de sistemas informáticos en red, es decir, a través de conjuntos de dispositivos electrónicos vinculados físicamente entre sí y con un protocolo en común (...)". Una revisión del concepto de TIC se presenta en Cobo (2009).

Es importante identificar que el concepto de TIC se refiere a materiales concretos, que tienen su origen y encuentran su uso, gracias a la informática entendida esta como la disciplina científica que estudia el tratamiento automático y racional de la información mediante el uso de ordenadores (De Pablos *et al*, 2004).

De hecho, la palabra informática se origina en un acrónimo acuñado en 1962, el cual se compone con la contracción de las palabras información automática (De Pablos *et al*, 2004). Así, el calificativo de informático, se le puede aplicar a aquellos archivos que están codificados en un formato físico, que permite su tratamiento automático a través de ordenadores. En este sentido los calificativos informático y digital pueden considerarse sinónimos.

De otro lado, Se hace mención al significado preciso de los términos archivo digital y archivo informático, como contraparte de los archivos físicos tradicionales; lo anterior, teniendo en cuenta que la gestión documental de los primeros, es la parte que se expone como de interés y análisis en esta investigación. Bajo este contexto es de advertir que los archivos físicos, no pueden tratarse de forma automática con ordenadores, a menos que se copien a un soporte digital.

¿Gestión documental electrónica?

La fusión de las TIC y la disciplina informática aplicada a la gestión de archivos, permite hablar de una nueva forma de gestión documental, lo cual nos contextualiza en la figura de los sistemas de gestión documental (World Bank Institute, 2008).

En la actualidad las grandes entidades no pueden pretender ser competentes si no estructuran adecuadamente un sistema de gestión documental informático. Si bien es cierto que la gestión de documentos informáticos, entraña algunos riesgos y desventajas inherentes (como se comentará posteriormente), estos sistemas de gestión documental informática, se han convertido en una exigencia de la época para las empresas (Cobo, 2009; De Pablos *et al*, 2004), toda vez que la gestión de archivos en formato digital flexibiliza, potencia y optimiza los procesos de gestión documental de forma casi ideal.

Para lograr el objetivo de tratar automáticamente y de forma racional un gran conjunto de archivos, es necesario organizar estos de forma lógica y establecer mecanismos que permitan accederlos y manipularlos.

Es ante esta necesidad que, se hace necesario el emplear las herramientas tales como las denominadas bases de datos, las cuales están definidas como “una colección de información organizada, de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que se solicite” (Reyes, 2017).

Delitos cibernéticos

La unión entre los sistemas electrónicos y la gestión documental con el objetivo de realizar procesos más completos, pueden abrir las puertas o dar paso a ocasionar actos indebidos, tales como el robo de información; por ello, a través de la historia de la humanidad, se ha hecho consiente que, a la par de la evolución hacia las nuevas tecnologías, se a crecentan y desarrollan también, las conductas delictivas vinculadas a las mismas y en el caso de las TIC, no ha ocurrido ninguna excepción.

Hoy se han incorporado al lenguaje común, palabras como delito informático, ciberdelito, ciberdelincuencia y ciberataque, las cuales hacen referencia al uso de TIC para procesar datos digitales, con el fin de obtener beneficios, pero socavando los derechos de otros usuarios del sistema informático; de ahí que, la definición de los conceptos sobre los vocablos enunciados, se ha tornado conflictiva, particularmente en el campo judicial (Hernández, 2009).

Uno de los principales mecanismos para la realización de ciber ataque, son los virus informáticos, los cuales son creados con el fin de robar datos, recopilar información, dañar el sistema, entre otros intereses (Reyes, 2017).

Un virus puede definirse de forma básica, como un archivo digital que contiene instrucciones para conseguir que un sistema informático realice un tratamiento automático de la información, distinto a los tratamientos programados por los diseñadores y administradores de dicho sistema (Canes, 2011). La implantación de un virus informático requiere de un vector (que puede ser por ejemplo una página web, un correo malicioso, un archivo infectado, o un hardware extraíble (Canes, 2011).

La forma más básica para acceder a los datos personales llega con un correo de remitentes que normalmente no envían información por este medio, por ejemplo, la Fiscalía (Caracol Radio, 2019).

Los llamados virus, aprovechan la vulnerabilidad de los sistemas y de los equipos de información, para alcanzar el objetivo del ataque. Un tipo particular de virus son ransomware, cuyo objetivo consiste en cifrar la información resguardada en un equipo de cómputo y exigir un pago a cambio de la herramienta para recuperar los archivos comprometidos (Reyes y Salinas, 2017).

Además de los ransomware, existen una diversidad de clases de virus, como por ejemplo los gusanos, programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones en el ordenador; los troyanos, cuyo objetivo principal es introducir e instalar otras aplicaciones en el equipo infectado para permitir el control desde otro tipo de equipos y robar información privada o de carácter empresarial; los Cookies que son pequeños archivos de texto, que se guardan en el navegador del usuario cuando se visitan páginas, pueden ser una amenaza para la privacidad del usuario.

Seguridad informática

Como contraparte a la ciberdelincuencia se ha postulado la rama de la informática denominada de forma descriptiva Seguridad Informática. Anteriormente la seguridad de la información estaba entendida como la aplicación de un conjunto de medidas de orden físico y lógico a los sistemas de información, para evitar la pérdida de la misma; siendo ésta una tarea de responsabilidad exclusiva de los departamentos de informática de las organizaciones (Velasco, 2008).

Según Aguilera (2011), se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad.

Por su parte, Aguirre (2006), afirma que la seguridad informática puede definirse como el conjunto de métodos y de varias herramientas, para proteger el principal activo de una organización, como lo es la información o los sistemas ante una eventual amenaza que se pueda suscitar.

Se puede considerar que el concepto de seguridad informática, entendido como un proceso que deben gestionar las entidades, lo gesta el Departamento de Industria y Comercio del Reino Unido, en coalición con empresas del sector privado, al formular la Norma BS7799, a principios de los noventa (Velasco, 2008). Dicha norma no pretendía ser más que un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información (Velasco, 2008).

A finales de los noventa, esta norma fue actualizada y complementada, lo cual dio como resultado una norma que establecía las recomendaciones para que una empresa evaluara y certificara su sistema de gestión de seguridad de la información. Esta nueva versión de la norma se convirtió en la norma ISO 17 999 de diciembre de 2000, la cual estaba alineada con las directrices de la OCDE (Organización para la Cooperación y el Desarrollo Económico) en materia de privacidad, seguridad de la información y Criptología, hecho de gran trascendencia, pues le otorgaba un carácter global a la norma (Velasco, 2008). En el 2002, la norma adquiere la denominación de ISO 27 001, luego de una nueva actualización (Velasco, 2008).

En la actualidad la ciberdelincuencia y la seguridad informática libran una acelerada carrera armamentista, en la que es difícil saber cuál va a la delantera. La seguridad informática, como rama de la informática, se ha puesto firmemente de frente mediante el desarrollo de un variado conjunto de técnicas y estrategias de carácter preventivos, detectivos y correctivos (Romero, 2018). No obstante, las cifras de ocurrencia de ciberdelitos se mantienen en crecimiento (Portafolio, 2017; Reyes y Salinas, 2017).

Adicional a los riesgos por ciberataque, otra tipo de riesgos informáticos son las eventuales consecuencias negativas que, sobre los procesos de gestión documental mediante el uso de TIC, pueden tener la obsolescencia, programada y no programada, de los soportes físicos y virtuales.

La obsolescencia programada ha sido definida como “(...) La determinación o programación del fin de la vida útil de un producto, de modo que, tras un periodo de tiempo calculado de antemano por el fabricante o por la empresa durante la fase de diseño de dicho producto o servicio, éste se torne obsoleto, no funcional, inútil o inservible (...)” (Arroyo, 2015).

3. Metodología

La investigación en las ciencias sociales, se sustenta en dos enfoques principales el cuantitativo y el cualitativo, los cuales se pueden combinar para obtener un tercer enfoque, el mixto, más fortalecido (Hernández, *et al*, 2010; Thomas, *et al*, 2005).

La fusión de los dos enfoques se sustenta en que ambos resultan muy valiosos y han realizado notables aportaciones al avance del conocimiento (Hernández, *et al*, 2003); pero a su vez, ambos tienen múltiples falencias que han sido ampliamente reseñadas (Castro, 2010). Adicionalmente, ambos enfoques tienen similitudes metodológicas esenciales (Grinnell, 1997). Así, ninguno es intrínsecamente mejor que el otro y cada uno sirve a una función específica para conocer un fenómeno y para conducir a la solución de los diversos problemas y cuestionamientos (Hernández, *et al*, 2003).

Por ello, para el desarrollo de la presente investigación (cuyo objetivo fue identificar el origen de los posibles riesgos y daños en la gestión de documentos informáticos ocurridos en CORANTIOQUIA durante los últimos años), se eligió precisamente un enfoque mixto, el cual es definido como un proceso de indagación donde se recolectan, analizan y vinculan datos

cuantitativos y cualitativos en un mismo estudio o una serie de investigaciones para responder a un planteamiento (Ruiz, *et al*, 2013).

Dentro del enfoque cualitativo se han fundamentado una significativa variedad de desarrollos metodológicos, tales como la historia de vida, la fenomenología, la teoría fundamentada, la etnografía y el estudio de caso (Creswell, 1998).

Para esta investigación se eligió el Método de Estudio de Caso, como componente de investigación cualitativa, al considerar que ofrece importantes resultados e información que no puede ser encontrada por medio de los métodos cuantitativos y que es muy valiosa para la toma de decisiones en las empresas, además de ser uno de los métodos más utilizados en la investigación cualitativa (Castro, 2010).

El método de estudio de casos es particularmente apropiado para ciertos tipos de problemas, donde la investigación y la teoría se hallan en sus fases preliminares; este método es utilizado para resolver problemas prácticos delicados, donde las experiencias de los participantes son importantes y el contexto de la situación es fundamental (Bonoma, 1985). En este mismo contexto, se ha afirmado que el uso de la estrategia del estudio de casos presenta grandes posibilidades en la explicación de fenómenos contemporáneos ubicados en su entorno real (Yin, 1989; Eisenhardt, 1989).

Con el método de estudio de caso, se busca establecer la realidad de una población objeto de estudio, mediante el análisis documental y la indagación de lo experimentado por ésta (Martínez, 2006). Al elegir la metodología de estudio de caso en una investigación social, contable, económica o fiscal, se intenta realizar inferencias válidas, a partir del estudio detallado de acontecimientos que no se desarrollan en un laboratorio, sino en el contexto de la vida social e

institucional (Ruiz, *et al*, 2013). Para desarrollar esta metodología, se recolecta información de múltiples fuentes, tales como documentos, archivos, entrevistas y observaciones (Creswell, 1998).

En esta investigación, se realizó un análisis documental de los archivos corporativos relacionados con su planteamiento, incluyendo en ellos la respuesta a un derecho de petición dirigido ad hoc a CORANTIOQUIA. El derecho de petición se interpuso a través de correo e incluía cinco ítems, de los cuales dos indagaban sobre los procesos de migración de datos realizados por CORANTIOQUIA en los últimos años, otros dos más interrogaban sobre la ocurrencia de ciberataques sufridos por la entidad en dicho periodo de tiempo y el otro restante solicitaba información sobre las políticas de gestión documental electrónica y de seguridad informática vigentes en la Corporación.

Los ítems del derecho de petición se adjuntan en la sección Anexos. Las preguntas fueron contestadas mediante oficio por parte de los funcionarios del Área de Informática de CORANTIOQUIA; adicionalmente, se realizó una búsqueda en los archivos de la entidad, logrando rastrear un memorando en el cual se trataban asuntos concernientes a esta indagación, tal y como será presentado y analizado en la sección de Resultados.

Probablemente al escoger el enfoque cualitativo, se alcancen los objetivos propuestos; no obstante, si no se tiene la certeza o la confianza suficiente, es recomendable ir más allá y utilizar el enfoque cuantitativo para ofrecer claridad y confianza a los resultados (Ruiz, *et al*, 2013).

Los estudios de corte cuantitativo pretenden la explicación de una realidad social vista desde una perspectiva externa y objetiva (Ruiz, *et al*, 2013). El enfoque cuantitativo, utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis que han sido establecidas previamente; la mayor confianza la tiene en la medición numérica y frecuente

el uso de la estadística para establecer con exactitud patrones de comportamiento en una población (Stoecker, 1991, Miles & Huberman, 1994, Grinnell, 1997).

La intención es buscar la exactitud de mediciones o indicadores sociales con el fin de generalizar sus resultados a poblaciones o situaciones amplias. Bajo esta metodología se trabaja fundamentalmente con el número, el dato cuantificable (Galeano, 2004).

De otro lado, se ha señalado que, bajo la perspectiva cuantitativa la recolección de datos es equivalente a medir (Gómez, 2006), y de acuerdo con la definición clásica del término, medir significa asignar números a objetos y eventos de acuerdo a ciertas reglas (Ruiz, *et al*, 2013).

Por estas razones, en complemento al enfoque cualitativo del estudio de caso mediante análisis documental, se realizó una encuesta no probabilística de participación voluntaria y anónima, con el objetivo de lograr identificar las prácticas y percepciones de los funcionarios a cargo de los archivos e identificar posibles riesgos inducidos, por prácticas comunes en la gestión documental electrónica.

Se utiliza la herramienta de la encuesta, en la medida que es un procedimiento que permite explorar cuestiones que tienden a la subjetividad y al mismo tiempo, permite obtener esa información de un número considerable de personas (Ruiz, *et al*, 2013; así mismo, permite explorar la opinión pública y los valores vigentes de una sociedad, temas de significación científica y de importancia en las sociedades democráticas (Grasso, 2006).

Es así como, el instrumento de la encuesta, ha sido descrito como la búsqueda sistemática de información en la que el investigador pregunta individualmente a un conjunto de investigados sobre los datos que desea obtener y posteriormente reúne estos datos individuales para obtener, durante la evaluación, datos agregados (Díaz, 2001; Mayntz, *et al*, 1975). Para ello, el cuestionario

de la encuesta debe contener una serie de preguntas o ítems respecto a una o más variables a medir (Ruiz, *et al*, 2013).

Es importante resaltar que, la técnica de la encuesta se utiliza en los trabajos de investigación mixta, aplicando el enfoque cuantitativo a los resultados de la investigación; es una herramienta igual que la entrevista, pero la intención y la forma de tratar los resultados las hace diferentes (Ruiz *et al*, 2013).

Básicamente se consideran dos tipos de preguntas en las encuestas: cerradas y abiertas (Gómez, 2006). Las preguntas cerradas contienen categorías fijas de respuesta que han sido delimitadas, pudiendo incluir dos posibilidades (dicotómicas) o incluir una amplia variedad de alternativas (Gómez, 2006). Este tipo de preguntas permite facilitar previamente la codificación (valores numéricos) de las respuestas de los sujetos (Gómez, 2006). Las preguntas abiertas no delimitan de antemano las alternativas de respuesta y se utilizan cuando no se tiene información previa sobre las posibles respuestas o cuando las alternativas de respuesta son muy diversas (Gómez, 2006). Estas preguntas no permiten precodificar las respuestas, la codificación se efectúa después que se tienen las respuestas (Gómez, 2006).

En esta investigación o estudio, se dirigió la encuesta a los funcionarios de las diferentes dependencias de CORANTIOQUIA, que por sus funciones acceden a los archivos digitales de la Corporación y gestionan de alguna forma estos documentos.

La encuesta consta de ocho preguntas, tendientes a identificar en los funcionarios conocimientos básicos de seguridad informática y la incorporación de los conocimientos en las labores de gestión documental. La encuesta fue respondida por un total de 17 funcionarios. El formato de encuesta se adjunta en la sección Anexos.

La información recopilada fue analizada y contrastada para identificar puntualmente los daños y riesgos por ciberataques y procesos de migración de datos experimentados por CORANTIOQUIA en los últimos años. Una vez identificados los daños y riesgos, se exploró y analizó el borrador del proyecto de resolución administrativa titulado “Por la cual se adopta la Política General de Seguridad de la Información y las Políticas de Seguridad de la Información”, para identificar si en dicho documento se da atención a los riesgos y daños identificados en este estudio, y si las estrategias consignadas tienden a minimizarlos en el futuro. Es de aclarar que se eligió dicho documento, puesto que durante el proceso de indagación, mediante análisis documental, se identificó que CORANTIOQUIA aún no cuenta con una política informática oficialmente aprobada.

Con el mismo objetivo se revisó el documento Programada de Gestión Documental de CORANTIOQUIA, para lograr identificar, si en el documento en comento se prevé la necesidad de protegerse ante los riesgos asociados a los procesos informáticos de gestión documental, o si presenta explícitamente estrategias tendientes a minimizar dichos riesgos y daños y si dichas estrategias están en concordancia con las prácticas declarada por los funcionarios encuestados.

4. Resultados Y Discusión

Con el ánimo de brindar mayor claridad, a continuación, se presentan por separados los resultados de los componentes cualitativo y cuantitativo del enfoque mixto seguido en el presente estudio. En primer lugar se presenta y analiza la información cualitativa recopilada mediante el derecho de petición respondido por funcionarios del Área de Informática de CORANTIOQUIA.

Es de recordar que dicho derecho de petición indagó sobre tres aspectos o categorías, los cuales se presentan y analizan por separado, a saber: la ocurrencia de ciberataques sufridos por CORANTIOQUIA en los últimos años; los procesos de migración de datos realizados por la entidad en dicho periodo de tiempo; y las políticas de gestión documental electrónica y de seguridad informática vigentes en la Corporación. En segundo lugar se presenta y analiza la información recopilada mediante el enfoque cuantitativo para el cual se hizo uso de la encuesta como instrumento para la obtención de información. Los datos obtenidos mediante esta, se analizan visualmente mediante gráficas y luego se discuten sus posibles implicaciones. Finalmente, se consideró pertinente identificar si el Proyecto de Políticas de Seguridad de la Información de CORANTIOQUIA, actualmente en desarrollo, con el fin de determinar si atiende a los daños y riesgos identificados en este estudio.

4. 1. Componente Cualitativo

Los funcionarios del área de informática de CORANTIOQUIA brindaron información concisa y puntual sobre los aspectos solicitados en el cuestionario del derecho de petición, dando a conocer aspectos importantes sobre los riesgos y daños en la gestión de documentos informáticos en CORANTIOQUIA desde el año 2015. Adicionalmente, se encontró información relevante en un memorando del 2015, que sirvió para complementar la información recopilada mediante el derecho de petición. A continuación, se presentan y analizan las ideas más relevantes recopiladas en las tres categorías indagadas: ciberataques, migración de datos informáticos, y políticas de seguridad de la entidad.

4. 1. 1. Ciberataques

Con la indagación a los funcionarios del área de informática de CORANTIOQUIA sobre la ocurrencia de ataques cibernéticos a las bases de datos, se conoció que “La base de Corporativa no ha sufrido ataques, pero archivos de tipo Word sí. Se presentó en el 2015 y 2016 secuestro de información por Ransomware.”.

Sin embargo y pese a esta declaración de los funcionarios informando la ausencia de ataques a la base de datos, se logró recabar el memorando con fechado del 9 de julio de 2015, el cual tiene por asunto “Para su conocimiento y fines pertinentes, anexo copia de la denuncia presentada el pasado 25 de junio ante la Fiscalía General de la Nación, relacionada con el ataque de virus informático a la información de la base de datos Sirena.” (Subrayado fuera del texto). Sirena es una de las bases de datos de mayor relevancia para CORANTIOQUIA, y permite a sus funcionarios, mediante la creación de un perfil, consultar expedientes, revisar asignaciones de los funcionarios, agendar actividades, entre otras muchas funciones, cumpliendo cabalmente con la definición de una base de datos: colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que se solicite.

Al leer la copia de la denuncia se obtienen detalles sobre lo sucedido, como por ejemplo que “(...) se reportaron fallos en la aplicación Sirena en el cual el sistema no generaba los formatos propios de la aplicación. (...) se encontró que la ruta donde se encuentran las plantillas de estos formatos, tenía cambiado la extensión del archivo. (...) en esta ruta se encuentra un archivo con un mensaje en el que se informa que los documentos fueron encriptados con una llave de encriptación y que si queríamos recuperar dicha información deberíamos pagar por ello.”. Queda claro, entonces, que este fue un caso de secuestro de información por medio de Ransomware a la base de datos Sirena.

Teniendo en cuenta que los funcionarios del área de informática no mencionaron ataques a las bases de datos, sino a archivos Word, y que esta omisión no puede haberse generado por un equívoco en el uso del concepto de *base de datos*, este sería un caso adicional, para un total de al menos tres incidentes de ciberataque durante el periodo 2015 a 2017, sin duda una dura muestra de la vulnerabilidad de CORANTIOQUIA a las amenazas informáticas y un llamado perentorio a fortalecer sus políticas de seguridad informática para minimizar los riesgos.

Al interrogar a los funcionarios del área de informática de CORANTIOQUIA sobre la magnitud de los daños ocasionado por los incidentes de ciberataques anteriormente descritos, estos informaron que “En el 2015 se logró recuperar la información porque se tenía respaldo en cintas y por fuera de la Corporación” mientras que “En el 2016 no se recuperó mucha información, porque cuando nos dimos cuenta ya habían pasado varios días y los respaldos estaban sobrescritos”.

Los funcionarios reportan, además, que especialmente en 2016 las dificultades generadas fueron grandes, pues se trataba de información relevante y en muchos casos debió ser nuevamente elaborada, aunque algunos funcionarios también recuperaron parcialmente su información por copias de los mismos funcionarios o correos electrónicos, es decir, por respaldos casuales, no como parte de un protocolo establecido en la política de seguridad informática o en el Plan de Preservación Digital.

Por otro lado, en el caso de 2015, descrito en la denuncia presentada ante la Fiscalía General de la Nación, se reporta que “(...) se logró recuperar información hasta enero de 2015. Para el resto no se contaba con respaldo. Se ha intentado descifrar esta información con algunos códigos, pero esto ha sido infructuoso.”.

4. 1. 2. Procesos de migración de datos

En cuanto a la pérdida de información por procesos de migración de datos, los funcionarios del área de informática de CORANTIOQUIA reportaron que la entidad usa el motor de base de datos ORACLE desde el 2002, sin interrupción. Sin embargo, aclaran que sí se han realizado cambios de versión, habiéndose realizado el último en el 2018, para lo cual se hace un respaldo total de la base de datos que se sube sobre la nueva versión. Esta estrategia de hacer previamente un respaldo total a la base de datos, ha resultado efectiva para proteger la información de la Corporación de los posibles daños por la obsolescencia de los soportes virtuales y los consecuentes procesos de migración de datos, toda vez que no reportan pérdida de información por los procesos de cambio de versión.

4. 1. 3. Programa de Gestión Documental

A partir de la información suministrada por los funcionarios del área de informática de CORANTIOQUIA se logró identificar que tan solo en mayo de 2017 se aprobó el Programa de Gestión Documental, cuyo proceso de implementación se planificó hasta el 2019. Las metas que se reportaron con respecto la seguridad de la información digital son la “Elaboración, implementación y seguimiento del Plan de Preservación Digital a largo plazo que aplica a documentos digitales y/o electrónicos de archivo” y “Definir los mecanismos para salvaguardar los documentos electrónicos de manipulaciones o alteraciones en la actualización, mantenimiento y consulta o por fallas que se presenten en la herramienta informática que administre los documentos electrónicos de archivo de CORANTIOQUIA”.

De allí se infiere que durante el periodo de tiempo comprendido entre 2015 y 2017 la entidad no contó con un Plan de Preservación Digital oficialmente establecido, puesto que tan solo en ese último año se iniciaron las acciones relacionadas con su fase de diseño. Por la misma razón,

también se infiere que durante dicho periodo CORANTIOQUIA no habría contado con mecanismos claramente definidos para salvaguardar la información electrónica ante riesgos por ciberataque u obsolescencia de los soportes físicos y virtuales.

La ausencia de un Programa de Gestión Documental (PGD) implementado y optimizado, que incluya un Plan de Preservación Digital y ponga en acción mecanismos de seguridad informática, sin duda maximiza los riesgos ante posibles ciberataques o casos de obsolescencia de los soportes físicos y virtuales. Sin un (PGD) bien establecido, que atienda a las necesidades de la gestión de documentación electrónica, es difícil garantizar la organización, conservación, integridad, autenticidad, fiabilidad y accesibilidad de los archivos digitales. Es esta una deuda pendiente por parte de CORANTIOQUIA que afortunadamente, a la fecha empieza a ponerse al día.

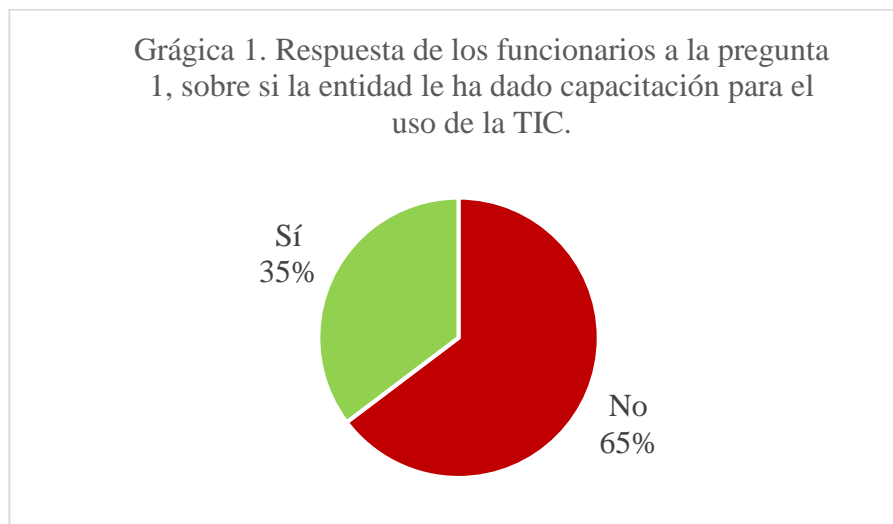
4. 1. 4. Política de seguridad informática

La información suministrada por los funcionarios del área de informática de CORANTIOQUIA permitió también identificar que para junio de 2019 la entidad aún no contaba con una política de seguridad informática oficialmente aprobada, sino tan solo con un documento borrador en espera de aprobación por la Dirección General y susceptible de modificaciones. Lo consignado en dicho documento con relación a los riesgos por ciberataques y por obsolescencia, será discutido luego del análisis de la información recopilada en la encuesta, con el objetivo de identificar además si este atiende tanto a los incidentes de ataques reportados, como a los riesgos identificados a partir de las declaraciones de los funcionarios encuestados.

4. 2. Componente cuantitativo

Como ya se indicó, se dirigió la encuesta a los funcionarios de CORANTIOQUIA de varias dependencias que por sus funciones debieran acceder a los archivos digitales de la Corporación y gestionarlos de alguna forma y fue contestada por un total de 17 funcionarios. La encuesta constó de ocho preguntas tendientes a identificar si los funcionarios tienen conocimientos básicos de seguridad informática y si en sus labores de gestión documental incorporan dichos conocimientos. El formato de encuesta se adjunta en la sección Anexos. A continuación se presentan una a una, de forma gráfica, las respuestas obtenidas de los funcionarios encuestados y se analizan sus implicaciones.

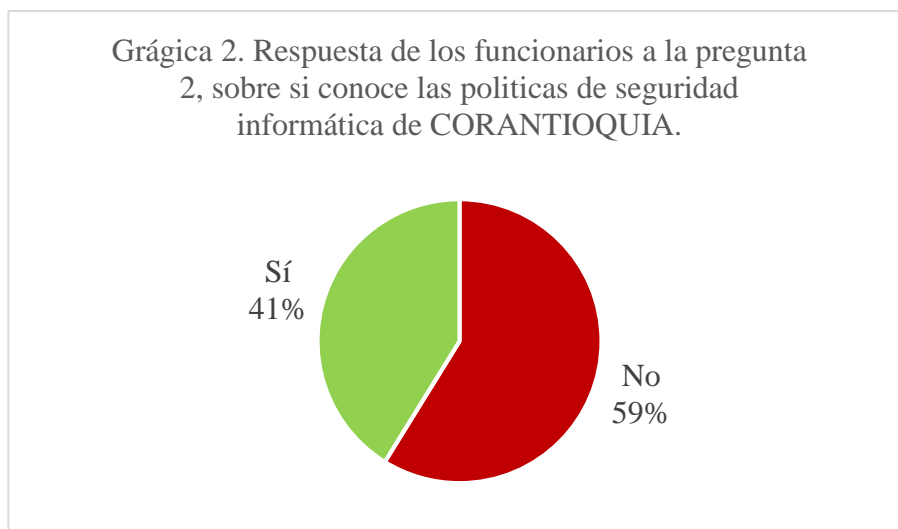
Pregunta 1: ¿La Corporación le ha brindado capacitación sobre el uso adecuado de las Tecnologías de la Información y la Comunicación (TIC)? Esta pregunta se planteó de forma cerrada, dicotómica, con las opciones de respuesta Sí y No.



De acuerdo a las frecuencias de respuesta, la mayor parte de los funcionarios (65%) consideran que la Corporación no le ha brindado capacitación sobre el uso adecuado de las Tecnologías de la Información y la Comunicación (TIC). De ser cierta esa afirmación, esto sería

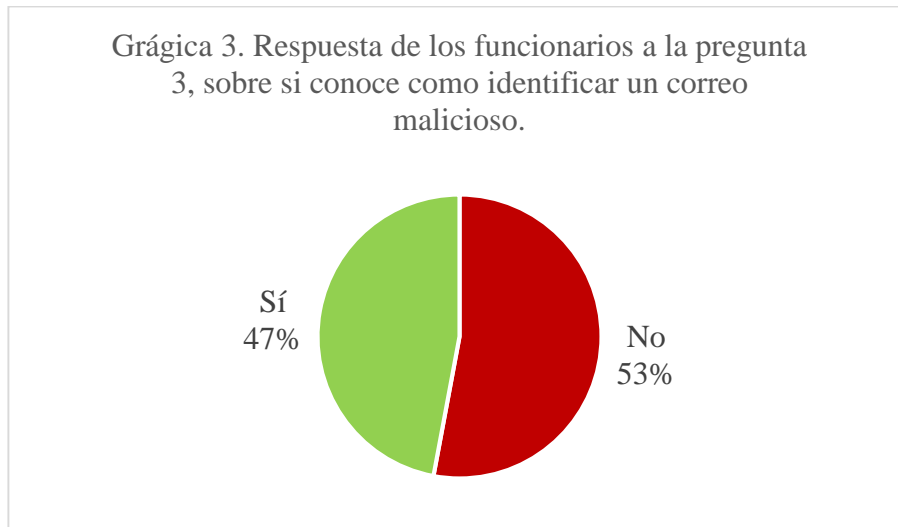
una primera debilidad identificada y su subsanación debería convertirse en objetivo de CORANTIOQUIA, para mejorar el grado de seguridad con que los funcionarios realizan la gestión de documentos informáticos a través de las TIC. Aun así, no se puede ignorar que un porcentaje significativo de funcionarios (35%) manifiestan que la Corporación sí les ha brindado capacitación al respecto. Quizás en algunas áreas o dependencias se haya brindado capacitación y en otras No. Sí bien esto último atenuaría la situación, debe reiterarse que la entidad debe trazarse el objetivo de capacitar adecuadamente en el uso de las TIC a todos los funcionarios que gestionen documentos informáticos, puesto que las debilidades de uno solo de ellos, en cuanto a estrategias de seguridad informática, pueden acarrear considerables daños para los archivos de la entidad.

Pregunta 2: ¿Conoce si la Corporación tiene políticas de seguridad informática? Esta pregunta se planteó de forma cerrada, dicotómica, con las opciones de respuesta Sí y No.



Si bien un porcentaje significativo de los funcionarios (41%) manifiestan conocer la política de seguridad informática de su entidad, la mayor parte (59%) declara desconocerla. Este es otro llamado de atención para que la Corporación CORANTIOQUIA se trace el objetivo de fortalecer el nivel de conocimiento de sus funcionarios sobre el manejo seguro de las TIC.

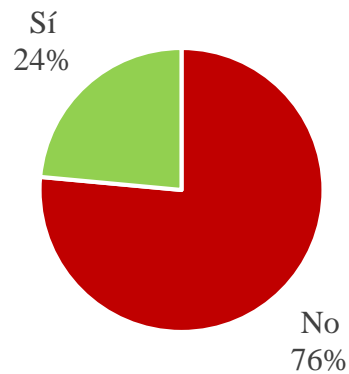
Pregunta 3: ¿Reconoce un e-mail sospechoso? Al igual que las dos anteriores, esta pregunta se planteó de forma cerrada, dicotómica, con las opciones de respuesta Sí y No.



Cerca de la mitad de los funcionarios (47%) manifiesta saber cómo identificar un correo malicioso mientras que la otra mitad declara ser vulnerable a este tipo de amenazas que como se expresó anteriormente, es uno de los mecanismos más comunes para la implantación de virus informáticos (Canes, 2011; Caracol Radio, 2019). Esto refuerza la necesidad ya manifiesta de brindar mayor capacitación a los funcionarios de CORANTIOQUIA en cuanto al uso adecuado de las TIC.

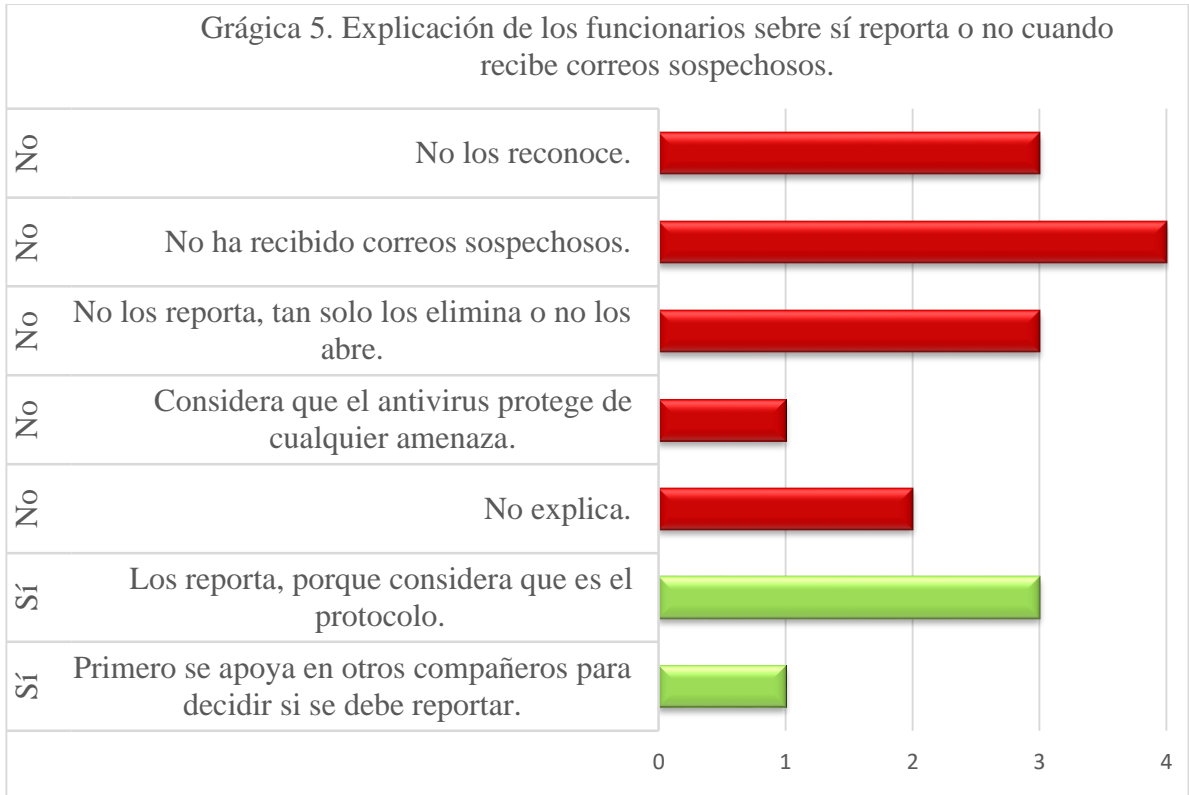
Pregunta 4: ¿Informa al Área de las TIC cuando llegan correos sospechosos? Esta pregunta se planteó de forma semi cerrada, puesto que, aunque presentaba dos opciones de respuesta, Sí y No, adicionalmente se solicitaba explicación de los motivos de elección de la respuesta.

Gráfica 4. Respuesta de los funcionarios a la pregunta 4, sobre si informa al área correspondiente cuando recibe correos sospechosos.

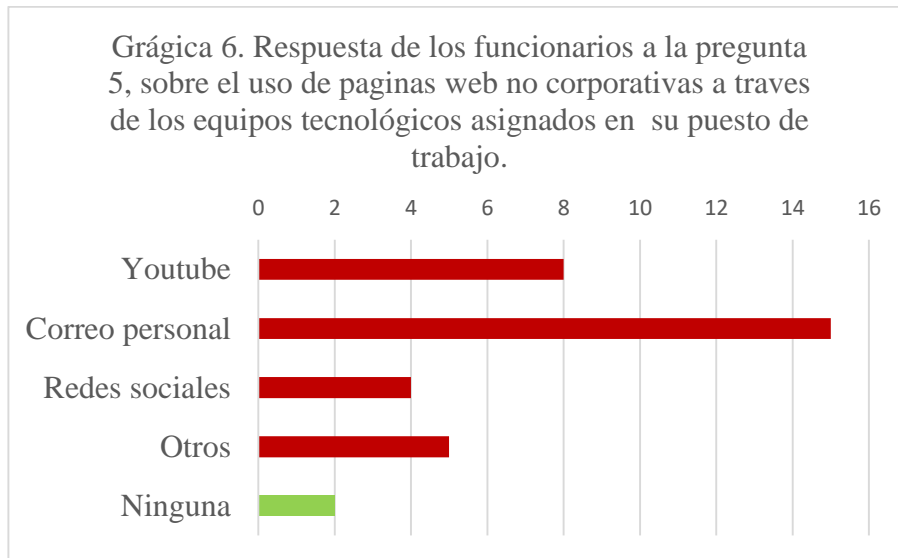


Un porcentaje minoritario (24%) de funcionarios declara que en caso de recibir correos sospechosos los reporta al área responsable de la seguridad informática, mientras que la gran mayoría (76%) no los reporta. Las diferentes explicaciones que los funcionarios adicionaron en cuanto a su práctica de reportar o no los correos sospechosos, fueron codificadas en siete categorías, las cuales se presentan en la Grafica 5. En una de las categorías tres funcionarios manifiestan que sí reportan los correos sospechosos, al considerar que éste es el protocolo a seguir. Por ejemplo, un funcionario manifestó que “Cuando lo detecto sospechoso, se lo reenvío a Soporte y ellos analizan y rastrean de dónde viene y luego me dan información de lo que encontraron”. En complemento, en otra categoría un funcionario declaró que, antes de reportar, se apoyan en los compañeros para decidir si es procedente reportarlo al personal encargado de la seguridad informática (“Cuando algo así sucede cualquiera de los compañeros hacen la alerta y se canaliza la inquietud a la sede central (...”). Estas afirmaciones de los funcionarios permiten inferir que sí hay un canal de atención a este tipo de riesgos informáticos y que este es atendido adecuadamente siempre y cuando los funcionarios reportan los correos sospechosos. Esto último, se vuelve contrastante con el hecho de que un porcentaje significativo de funcionarios (23%) considera

innecesario hacer el reporte o que no hay un protocolo o canal establecido para atender estas amenazas. Así por ejemplo, un funcionario manifestó que “Normalmente no se informa porque no han dado una ruta a seguir cuando ocurre algo así (...)”.



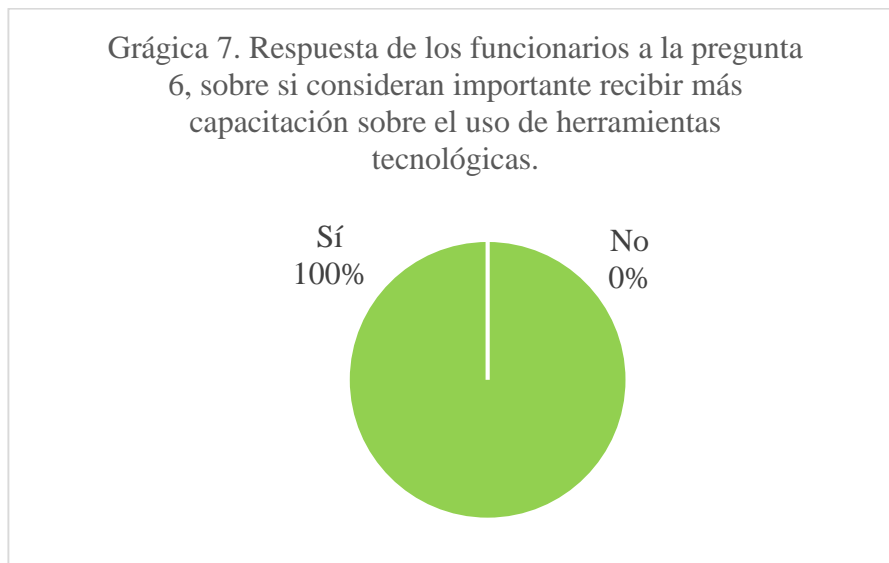
Pregunta 5: ¿Ingresa a páginas web diferentes a las Corporativas, cuáles? Esta pregunta se planteó de forma semi cerrada, con cuatro opciones de respuesta no excluyentes (YouTube, Correo personal, Redes sociales, Otros/ Cuál), la última de las cuales era abierta, puesto que permitía a los funcionarios adicionar cualquier otra opción que no hubiese sido prevista.



Llama la atención que tan solo una pequeña minoría de funcionarios (12%) manifiesta no usar páginas web diferentes a las corporativas, cuando ésta debiera ser una regla de cumplimiento general. La página web no corporativa más utilizada por los funcionarios (88%) es el correo personal, aun cuando la entidad le asigna a cada uno un correo corporativo.

Entre las páginas reportadas por los funcionarios en la categoría Otros, se enunció una amplia variedad de páginas, relacionadas con las funciones de los cargos desempeñados, tales como “Secop II, Sigep, Procuraduría, Registraduría, ANLA, Ministerios de Ambiente y Desarrollo, Servicio geológico colombiano, IDEAM, IGAC, La Página del Senado, de la Corte Constitucional y del Consejo de Estado”. Pero, adicionalmente, también se declaró el uso de páginas que son más de uso personal y que no corresponden a las actividades laborales a cargo, tales como “Bancolombia, Bancos, Google, Compras Online, periódicos, universidades, Whatsappweb y Spotify. Esto indica que en la práctica no se siguen políticas mínimas de uso de las TIC en los puestos de trabajo, lo cual sin duda constituye una puerta abierta para posibles ataques informáticos.

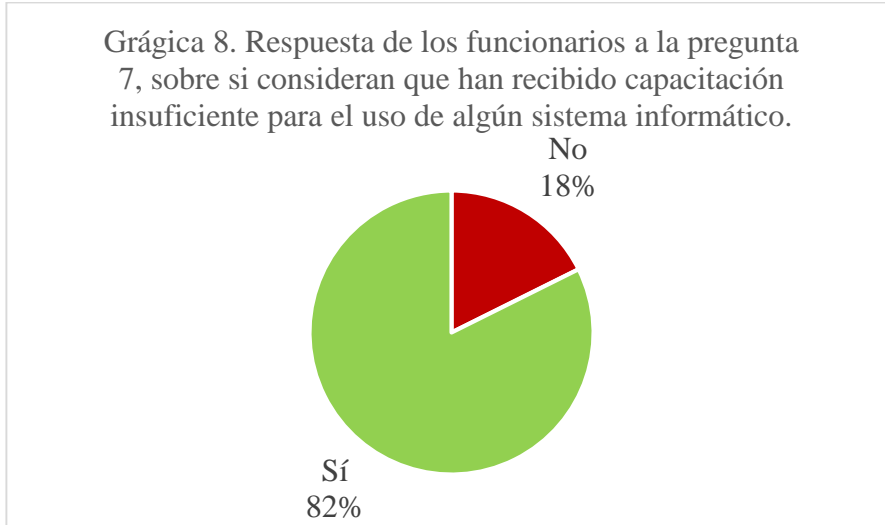
Pregunta 6: ¿Considera usted importante que la Corporación realice capacitación en el uso adecuados de las herramientas tecnológicas para el desarrollo de sus actividades? Esta pregunta se planteó de forma semi cerrada, puesto que, aunque presentaba dos opciones de respuesta, Sí y No, se solicitaba justificación de los motivos de elección de la respuesta.



Todos los funcionarios (100%) reconocen la necesidad de fortalecer su nivel de capacitación en el uso de las TIC, como corresponde después de haber ido identificando las constantes debilidades al respecto mediante el análisis de los resultados de las preguntas anteriores de esta encuesta. Entre las justificaciones que expresaron los funcionarios, para considerar importante la ejecución de más capacitaciones, están por ejemplo, “Es muy necesario este tipo de capacitaciones pues la obsolescencia en la tecnología ocurre cada vez en menos tiempo y los funcionarios quedamos desactualizados” y “Me parece muy importante y capacitar a todo el personal por todos los riesgos que existen y la información tan importante que manejamos”.

Pregunta 7: ¿Ha sentido alguna vez que es insuficiente la capacitación que recibió para utilizar algún sistema informático? Al igual que la anterior, esta pregunta se planteó de forma semi

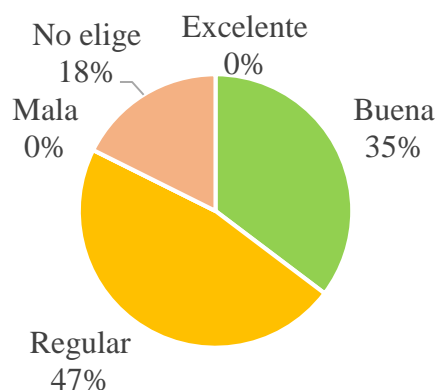
cerrada, puesto que, aunque presentaba dos opciones de respuesta, Sí y No, se solicitaba justificación de los motivos de elección de la respuesta.



La mayoría de los funcionarios (82%) manifiesta inconformidad con el grado de capacitación que se le ha brindado sobre alguno de los sistemas informáticos que usa en su cargo, como es natural, al revisar los resultados de las preguntas anteriores de esta encuesta. Esta es una reiteración de la necesidad que tiene CORANTIOQUIA de fortalecer el nivel de conocimiento que tienen sus empleados con respecto al uso eficiente y seguro de las TIC.

Pregunta 8: ¿Cómo considera usted la seguridad informática que maneja la Corporación?: Esta pregunta se planteó de forma cerrada, con cuatro opciones de respuesta excluyentes: Excelente, Buena, Regular y Mala.

Gráfica 9. Respuesta de los funcionarios a la pregunta 8, sobre cómo considera la seguridad informática en CORANTIOQUIA.



Ningún funcionario manifestó que la seguridad informática de la corporación fuese mala o excelente, por el contrario, la mayor parte consideró que en este aspecto la corporación se desempeña de buena manera (35%) o de forma regular (47%). Adicionalmente, un grupo de funcionarios (18%) prefirió no comprometerse con la elección de una de las opciones de respuesta. Básicamente, pueden interpretarse los resultados de esta valoración como que los funcionarios perciben que, aunque la corporación ejecuta algunas medidas de seguridad informática adecuadas, tiene muchas oportunidades de mejora y necesidades de fortalecimiento.

A modo de síntesis del enfoque cuantitativo realizado mediante la encuesta, se puede señalar que la mayoría de los funcionarios expresan reiteradamente la necesidad de recibir mayor capacitación sobre el uso seguro y eficiente de las TIC y que, como consecuencia de la falta de capacitación y de socialización de políticas de seguridad informática, muchos de los funcionarios realizan prácticas riesgosas, tales como la desatención de amenazas por correos sospechosos y el uso de páginas web no corporativas.

4.3. Análisis al proyecto de política de seguridad de la información.

Al revisar el proyecto Política General de Seguridad de la Información de CORANTIOQUIA, lo primero que se hace evidente es su amplia consideración del ámbito legal y normativo sobre la materia en cuestión. Así, se hace mención a la Ley 1341 de 2009 (en la cual se estableció el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones), el Decreto número 1083 de 2015, adicionado por el Decreto número 415 de 2016 (en el cual se establece la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones) y el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones número 1078 de 2015 (en el cual se plasma el Modelo de Seguridad y Privacidad de la Información (MSPI), versión 3.0, adoptado por el Ministerio de Tecnologías de la Información y las Comunicaciones). De igual manera, se mencionan como fuentes de referencia las Normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013 Seguridad y Privacidad de la Información. Ante una fundamentación tan sólida y amplia es de prever la formulación de una Política de Seguridad Informática pertinente, actualizada y robusta.

Así por ejemplo, en dicho proyecto se dicta un amplio abanico de medidas para la minimización de riesgos por ciberataques, entre los que destacan la estructuración de un Comité de Seguridad de la Información que respalde y apoye las iniciativas de seguridad, el fortalecimiento del software antivirus, la restricción de acceso a los usuarios de las bases de datos, la exclusividad de instalación y actualización de software por el área de seguridad informática, la sensibilización del personal en temas de seguridad, la prohibición de usos no laborales de los sistemas informáticos, la limitación del uso de archivos con extensiones peligrosas, el establecimiento de un protocolo y ruta para el reporte de incidentes de ciberataques o sospechosos,

la prohibición de ingreso a sitios web peligrosos (como Dropbox, Mega, etc), la regulación del uso de medios de almacenamiento extraíbles (CDs, DVDs, USB, etc.). Sin duda un repertorio muy variado e incluso de medidas contra los ciberataques, al que es difícil proponerles adiciones disponibles en la actualidad.

Con respecto a la atención de los riesgos por migración de datos ante la obsolescencia de los soportes virtuales, en el proyecto se señala que “Para todos los cambios en los sistemas de producción se deben desarrollar procedimientos adecuados de devolución (Rollback), según lo indica el procedimiento de cambios, los cuales permitan devolverlos rápida y oportunamente a las condiciones previas al cambio más reciente en el software” y que “se deberán realizar respaldos periódicos del software y la información importante en los sistemas de información de la Entidad, (...) con la frecuencia apropiada para cada sistema de información, (...) y validar que las copias sean correctas y realizar pruebas de funcionamiento periódicas”. En cuanto a los riesgos por obsolescencia de los soportes físicos, el proyecto contempla que “Se deberán realizar pruebas periódicas para asegurar que los equipos y los medios de almacenamiento no se deterioren para asegurar que cumplan con su función cuando se necesiten.”. Estas medidas retoman y refuerzan las que ya han venido siendo aplicadas por el área de informática de la Corporación, y que según se identificó, han resultado exitosas hasta la fecha.

También se identifica que el proyecto da debida atención a los riesgos identificados en la presente indagación a partir de las declaraciones de los funcionarios encuestados, a saber, el uso de los sistemas y equipos informáticos de la entidad para usos no corporativos, la desatención por parte de los funcionarios de incidentes sospechosos de ciberataques y las falta de sensibilización del personal en cuanto a prácticas adecuadas de seguridad informática en su trabajo.

Sobre el uso de los equipos y sistemas informáticos de la entidad, en el proyecto se estipula que “los equipos de cómputo pertenecientes a CORANTIOQUIA deben ser utilizados únicamente para propósitos corporativos (...)” y “Se debe restringir el acceso a sitios peligrosos, donde se pueda compartir información en línea (como Dropbox, Mega, etc) o que puedan afectar la productividad del funcionario”. Es deber reiterar que estas medidas son más que pertinentes ante los resultados de la presente investigación, según los cuales tan solo una pequeña minoría de funcionarios (12%) manifiesta no usar páginas web diferentes a las corporativas mientras la gran mayoría declara usar una amplia variedad de dichas páginas. Estos resultados llevan a recomendar, al respecto, evaluar la posibilidad de medidas que de forma activa restrinjan el acceso a páginas web peligrosas y no corporativas, en vez de dejarlo a voluntad del personal, caso en el cual debe hacerse un proceso efectivo de sensibilización.

El análisis de la encuesta de la presente investigación muestra que existe confusión y desconocimiento sobre cómo actuar frente a incidentes sospechosos de ciberataques. Al respecto el proyecto de Política de Seguridad Informática consigna que “La Entidad debe establecer un procedimiento formal para el reporte de eventos de Seguridad de la Información”. Especificando que “Este procedimiento debe contar con los niveles de escalamiento pertinentes. Se debe contar con un punto único de contacto y cada funcionario debe cumplir con el reporte de los eventos tan pronto le sea posible”. Adicionalmente se señala que “Cualquier usuario que sospeche de una infección por un software malicioso debe apagar inmediatamente el computador involucrado, desconectarlo de cualquier red, contactar al Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones y evitar cualquier intento de eliminar el virus”.

En cuanto a capacitación, uno de los requerimientos más señalados por los funcionarios encuestados en esta investigación, el proyecto de Política de Seguridad Informática contempla que

“El Grupo Interno de Trabajo de Talento Humano debe asegurar que cada funcionario en la fase de inducción reciba una sensibilización en seguridad de la información y su importancia para la Entidad”. Especificando además que “La Entidad debe incluir en la inducción o sensibilización sobre seguridad de la información, temas sobre cómo identificar y reportar incidentes de seguridad y su responsabilidad respecto a estos temas”. Para ello se prevé que “Se deben realizar campañas sobre el buen uso de Internet para concientizar a las personas sobre los peligros de descargar archivos, acceder a sitios desconocidos o de baja confianza y aceptar los mensajes sobre instalación de software que brinde el navegador y el acceso a sitios seguros”.

De esta manera se espera alcanzar un ideal en el que “Todos los funcionarios deben ser responsables del manejo adecuado de la información dentro y fuera de la Entidad, de su comunicación y divulgación, deben conocer la política general y las políticas específicas de la seguridad de la información y estar en la obligación de cumplirlas” y “Todos los funcionarios, contratistas, proveedores y/o terceros de la Entidad deben tener conciencia sobre los procedimientos de reporte de los diferentes tipos de eventos y las debilidades que puedan tener impacto en la seguridad de los activos de información de los que hacen uso”.

5. Conclusiones y Recomendaciones

Por un lado, mediante el Estudio de Caso se recopiló investigación cualitativa valiosa sobre el historial de ataques cibernéticos y los procesos de migración de datos llevados a cabo por la corporación durante los últimos años, así como de las políticas que debería orientar a la entidad en su gestión documental informática, mientras que por otro lado, la encuesta no probabilística permitió sondear la percepción de los empleados sobre la seguridad informática de su entidad e

identificar su nivel de apropiación de algunas medidas básicas para la prevención de ciberataques. En conjunto, el enfoque investigativo mixto resultó una herramienta de indagación eficaz, en la que los componentes cualitativo y cuantitativo se complementaron, para permitir el cumplimiento de los objetivos de la presente investigación, tal como se explicitará a continuación.

En cuanto a la ocurrencia de ciberataques, la revisión documental permitió identificar que CORANTIOQUIA presentó un total de al menos tres incidentes durante el periodo 2015 a 2017. Esta es una muestra de la vulnerabilidad de entidad a las amenazas informáticas y un llamado perentorio a fortalecer sus políticas y herramientas de seguridad informática para minimizar este tipo de riesgos. Parte de la información afectada en estos eventos de ataques cibernéticos se recuperó gracias a copias informales, no planificadas con base en la política de seguridad informática de la corporación, mientras que otra parte se perdió definitivamente y debió ser reelaborada, en la medida de lo posible, con el consiguiente costo y esfuerzo inherente. Esto último insta a evaluar la posibilidad de establecer un respaldo a la información, ya sea total o para la información más sensible y esencial.

El análisis documental también permitió identificar que la entidad realiza periódicamente procesos de migración de datos, requeridos para la actualización de las versiones de motor de base de datos, siendo el último de ellos en 2018. De forma positiva, estos procesos no han conllevado a problemas por pérdida o afectación de información gracias a la realización preventiva de un respaldo total de la base de datos que se sube sobre la nueva versión, siendo entonces una estrategia efectiva que debe mantenerse en la política de seguridad informática de CORANTIOQUIA.

De igual manera, mediante el estudio de caso se logró detectar que tan solo en mayo de 2017 se aprobó el Programa de Gestión Documental de CORANTIOQUIA, cuyo proceso de implementación se planificó hasta el 2019, lo cual sin duda constituye una falencia importante para

la entidad en materia de gestión documental. Es esta una deuda pendiente por parte de CORANTIOQUIA que afortunadamente, a la fecha empieza a ponerse al día.

Mediante la encuesta no probabilística se identificó que porcentajes significativos de los funcionarios encargados de gestionar información como parte de sus labores cotidianas, desconocen o presentan confusión en cuanto a los protocolos a seguir ante situaciones sospechosas de ciberataques y que incurren en prácticas que favorecen la vulnerabilidad ante las amenazas informáticas. Los mismos funcionarios manifiestan sentirse poco capacitados en temas de seguridad informática. Esta situación es preocupante, puesto que los usuarios son la parte de los sistemas de información más vulnerable a este tipo de amenazas (Romero, 2018).

Según se logró establecer, mediante el estudio de caso, para junio de 2019 la entidad aún no contaba con una política de seguridad informática oficialmente aprobada, sino tan solo con un documento borrador en espera de aprobación por la Dirección General y susceptible de modificaciones. Teniendo en cuenta esto, los inconvenientes arriba descritos pueden verse como una afectación mínima ante los niveles de riesgo a los que posiblemente debe haber estado sometida la entidad. Sin una guía oficial que oriente a los funcionarios es comprensible su confusión y es previsible que realicen por desconocimiento prácticas que menoscaban la seguridad de la información frente a las numerosas amenazas cibernéticas.

Afortunadamente, en la actualidad la entidad está en proceso de aprobar su Política General de Seguridad de la Información que cuenta con una fundamentación sólida y amplia, y comprende una Política de Seguridad Informática pertinente, actualizada y robusta, en la cual se da atención a los diferentes riesgos y debilidades detectadas en la presente investigación. Es recomendable que la entidad gestione con celeridad la implementación de esta política, para dejar atrás su actual

estado de vulnerabilidad y que se comprometa a hacer efectivas las diferentes estrategias de prevención, detección y corrección de daños en la gestión documental electrónica que en ella se establecen, haciendo un énfasis en la capacitación de sus funcionarios en prácticas seguras para el uso de los sistemas informáticos.

6. Bibliografía

Adell, J. (1997). *Tendencias en educación en la sociedad de las tecnologías de la información*. EDUTEC, Revista Electrónica de Tecnología Educativa, 7. Recuperado de http://nti.uji.es/docs/nti/Jordi_Adell_EDUTEC.html

Aguilera, P. (2011). *Redes seguras (Seguridad informática)*. Editex.

Aguirre, J. (2006). *Libro electrónico de seguridad Informática y Criptografía*: Universidad Politécnica de Madrid.

Arroyo, A. (2015). *Obsolescencia Programada*. Recuperado de: <http://adrianistan.eu/obsolescencia-programada/latex/obsolescencia-programada.pdf>

Bonoma, T. (1985). *Case Research in Marketing: Opportunities, Problems, and a Process*. Journal of Marketing Research, 22 (2), 199-208.

Bosco, J. (1995) *Schooling and Learning in an Information Society*. En U.S. Congress, Office of Technology Assessment (ed.), *Education and Technology: Future Visions*, OTA-BP-EHR-169. Washington, DC: U.S. Government Printing Office, September

Canes, D.; Pérez, Y. y Callis, S. (2011). *Acerca de los virus informáticos: una amenaza persistente*. MEDISAN v.15 n.2

- Castro, E. (2010) *El estudio de casos como metodología de investigación y su importancia en la dirección y administración de empresas*. Revista Nacional de Administración, 1 (2), 31-54.
- Cobo, J. (2009). *El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento*. Zer 14-27, pp.295-318
- Corporación Autónoma Regional del Centro de Antioquia (2017) *Sistema de Gestión Integral – SGI. Manual de Gestión Ambiental*. 21 pp. Recuperado de: <http://www.corantioquia.gov.co/SiteAssets/PDF/Transparencia/Procedimientos%20y%20Lineamientos/MANUAL%20DE%20GESTI%C3%93N%20AMBIENTAL.pdf>
- Creswell, J. (1998). *Qualitative Inquiry and Research Design. Choosing Among Five Traditions*. Thousand Oaks. Sage Publications.
- De Pablos, C., López Hermoso, J., Martín Romo, S. y Medina, S. (2004). *Informática y comunicaciones en la empresa*. Madrid: ESIC. 14 p.
- Díaz, V. (2001). *Diseño y elaboración de cuestionarios para la investigación comercial*. Esic editorial.
- Eisenhardt, K. (1989). *Building Theories from Case Study Research*. Academy of Management Review, 14(4), 532-550.
- El Tiempo. (2018). *Denuncias por delitos informáticos crecieron el 31 % el año pasado*. Recuperado de: <https://www.eltiempo.com/justicia/delitos/denuncias-por-delitos-informaticos-crecieron-en-2017-172294>

Enter.Co. (2019). *Colombia, el país con más ransomware en latinoamerica, en 2018*. Recuperado de: <https://www.enter.co/especiales/empresas/colombia-ataques-ciberneticos-18/>

Fernández, R. (2005) *Marco conceptual. de las nuevas tecnologías aplicadas a la educación*. Universidad de Castilla. Recuperado de: <http://www.uclm.es/profesorado/ricardo/DefinicionesNNTT.html>

Galeano, M. (2004). *Diseño de Proyectos en la investigación cualitativa*. Ed. Universidad EAFIT.

Gómez, M. (2006). *Introducción a la metodología de la investigación científica*. Ed. Brujas.

Grasso, L. (2006). *Encuestas: elementos para su diseño y análisis*. Encuentro Grupo Editor.

Grinell, R. (1997). *Social work research & evaluation: Quantitative and qualitative approaches*. 5.ed. E.E. Peacock Publishers.

Hernández, L. (2009). *El delito informático*. Eguzkilore, nº 23. 227 – 243 pp.

Hernández, S.; Fernández, C. y Baptista, L. (2003). *Metodología de la Investigación*. Ed. Mc Graw Hill.

Hernández, S.; Fernández, C. y Baptista, L. (2010). *Metodología de la Investigación*. Ed. Mc Graw Hill.

Caracol Radio. (2018). *Cada hora se denuncian tres delitos informáticos*. Recuperado de: https://caracol.com.co/radio/2018/09/16/judicial/1537118516_798052.html

Martínez, C. (2006). *El método de estudio de caso: estrategia metodológica de la investigación científica*. Pensamiento & Gestión, 1 (20), 165-193.

Mayntz, R.; Holm, K. y Hübner, P. (1975). *Introducción a los métodos de la sociología empírica*. Ed. Alianza.

Miles, M. y Huberman, A. (1994). *Qualitative Data Análisis*. 2 ed. Sage Publications.

Organización de las Naciones Unidas. (2015). *13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal*. Recuperado de: https://www.unodc.org/documents/congress/Documentation/IN_SESSION/ACONF222_L6_s_V1502123.pdf

Portafolio. (2017). *Así roban la información de las empresas los piratas informáticos*. Recuperado de: <https://m.portafolio.co/innovacion/asi-roban-la-informacion-de-las-empresas-los-piratas-informaticos-506522>

Reyes, J. (2017). *Wanna Cry Ransomware*. Firma Invitada, 32-37.

Reyes, R. (2017). *Apuntes de fundamento de base de datos*. Universidad Autónoma del Estado de México. Recuperado de: http://ri.uaemex.mx/bitstream/handle/20.500.11799/69937/secme-28215_1.pdf?sequence=1

Reyes, V. y Salinas, G. (2017). *WannaCry: Análisis del movimiento de recursos financieros en el blockchain de bitcoin*. Research in Computing Science. 147–155 p.

Romero, M.; Figueroa, G.; Vera, D.; Álava, J.; Parrales, G.; Álava, C.; Murillo, A. y Castillo, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. Editorial Área de Innovación y Desarrollo. 121 pp.

- Ruiz, M.; Borboa, M. y Rodríguez, J. (2013). *El enfoque mixto de investigación en los estudios fiscales*. Tlatemoani, 13, 1-25.
- Semana. (2017). *El cibercrimen en 2017: la amenaza crece sobre Colombia*. Recuperado de:
<https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979>
- Stoecker, R. (1991): *Evaluating and rethinking the case study*. Social Review, 38-261, 88-112.
- Thomas, J.; Nelson, J. y Silverman, S. (2005). *Research Methods in Physical Activity*. Fifth edition. Human Kinetics.
- Velasco, A. (2008). *El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la Norma ISO 27 001*. Revista de Derecho, (29), 333-366.
- World Bank Institute (2008). *Measuring Knowledge in the world's economies, Knowledge for development program*. pp. 1-12
- Yin, R. (1989). *Case Study Research: Design and Methods, Applied Social Research*. Newbury Park CA: Sage.

7. Anexos

Formato de Cuestionario

Anexo 1



UNIVERSIDAD DE ANTIOQUIA

ESCUELA INTERAMERICANA DE BIBLIOTECOLOGÍA

ARCHIVÍSTICA- 2019

Público: cuestionario dirigido a los funcionarios de Corantioquia.

Objetivo: identificar los problemas de seguridad informática que tienen la Corporación.

Los datos suministrados por usted serán consolidados como parte de la investigación

que adelanto para la obtención del título Archivista de la Universidad de Antioquia.

Marque con una X la respuesta.

Información general

1. Sexo: Femenino_____ Masculino_____
2. Cargo: Auxiliar de Servicios Generales
3. Cuántos años lleva en la corporación laborando De 1 a 3 ___ De 4___6 De 7 en adelante _____

Cuestionario

1. ¿La Corporación le ha brindado capacitación sobre el uso adecuado de las Tecnologías de la Información y la Comunicación (TIC)?:
Sí_____ No_____

2. ¿Conoce si la Corporación tiene políticas de seguridad informática?

Sí_____ No_____

3. ¿Reconoce un e-mail sospechoso?

Sí _____ No_____

4. ¿Informa al Área de las TIC cuando llegan correos sospechosos?

Sí_____ No_____

Explique: Porque a la fecha no he recibidos correos electrónicos que pueda identificar como sospechosos.

5. ¿Ingresa a páginas web diferentes a las Corporativas, cuáles?

YouTube_____ Correo personal _____ Redes sociales_____
Otros (indique _____cuáles)

6. ¿Considera usted importante que la Corporación realice capacitación en el uso adecuados de las herramientas tecnológicas para el desarrollo de sus actividades? Sí _____ No_____

Justifique: Es importante que la Corporación realice capacitaciones en este sentido porque existen herramientas que pueden ser muy útiles para nuestro trabajo, y que nos enseñen a utilizarlas de forma segura.

7. ¿Ha sentido alguna vez que es insuficiente la capacitación que recibió para utilizar algún sistema informático? Sí _____ No_____


Justifique: En la parte de herramientas informáticas he recibido poca capacitación.

8. ¿Cómo considera usted la seguridad informática que maneja la Corporación?:

Excelente_____ Buena _____ Regular_____
Mala_____

Anexo 2

Borrador Política de Seguridad Informática

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 1 de 57

Código Dependencia -

Por la cual se adopta la Política General de Seguridad de la Información y las Políticas de Seguridad de la Información


El Director General de la Corporación Autónoma Regional del Centro de Antioquia, en uso de sus facultades legales y estatutarias y en especial las que le confieren el artículo 29 de la Ley 99 de 1993 y el Decreto 1768 de 1994 y,

CONSIDERANDO

Que la Ley 1341 de 2009, estableció el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, incorporando principios, conceptos y competencias sobre su organización y desarrollo e igualmente señaló que las Tecnologías de la Información y las Comunicaciones deben servir al interés general y, por tanto, es deber del Estado promover su acceso eficiente y en igualdad de oportunidades a todos los habitantes del territorio nacional.

Que el Decreto número 1083 de 2015, adicionado por el Decreto número 415 de 2016, establece la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones, cuyo ámbito de aplicación, de acuerdo con el artículo 2.2.35.2, corresponde a las entidades del Estado de orden nacional y territorial, los organismos autónomos y de control.

Que el artículo 2.2.35.3 del Decreto número 1083 de 2015, adicionado por el Decreto número 415 de 2016, establece como objetivos del fortalecimiento institucional: "3. Desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la entidad y/o sector en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones (TIC). Así mismo, velar por el cumplimiento y actualización de las políticas y estándares en esta materia" y "11. Desarrollar estrategias de gestión de información para garantizar la pertinencia, calidad, oportunidad, seguridad e intercambio con el fin de lograr un flujo eficiente de información disponible para el uso en la gestión y la toma de decisiones en la entidad y/o sector".


	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 2 de 57

Que así mismo, una de las metas que pretende alcanzar el Programa Visión Colombia 2019, es el cumplimiento del objetivo "UN ESTADO AL SERVICIO DE LOS CIUDADANOS", el desarrollo de la estrategia "AVANZAR HACIA UNA SOCIEDAD INFORMADA", la cual dispone que: "En 2019 la información deberá ser un derecho efectivo y un instrumento de difusión y apropiación del conocimiento, que promueva el desarrollo económico, la equidad social y la democracia. En ese contexto, Colombia deberá alcanzar estándares adecuados de generación de información confiable y oportuna, y de uso colectivo. El Estado promoverá su disseminación, aprovechando el uso de las tecnologías de la información y las comunicaciones", cumpliendo con los estándares de gobierno, en especial los establecidos con relación a la seguridad que hace parte de los cuatro pilares: TIC para Servicios, TIC para datos abiertos, TIC para la Gestión y TIC para la seguridad.

Que mediante el Decreto número 2573 de 2014, "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea", se describen los lineamientos, se incorporan mejores prácticas y se orienta la implementación para lograr una administración pública más eficiente, coordinada y transparente, a través del fortalecimiento de la gestión de las Tecnologías de la Información y se reglamenta el Marco de Referencia de Arquitectura Empresarial para Entidades del Estado, el cual es un modelo de referencia puesto a disposición del Estado colombiano para servir como orientador estratégico de las arquitecturas empresariales, lo cual debe estar articulado con los lineamientos de seguridad de la información.

Que el artículo 2.2.9.1.2,1 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones número 1078 de 2015, establece como cuarto componente, para desarrollar los fundamentos de la estrategia que facilitarán la masificación de la oferta y la demanda del Gobierno en Línea, el de la Seguridad y privacidad de la Información.

Que el Modelo de Seguridad y Privacidad de la Información (MSPI), versión 3.0 de fecha 03/03/2015 adoptado por el Ministerio de Tecnologías de la Información y las Comunicaciones, reúne el conjunto de lineamientos, políticas, normas, procesos e instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación del modelo, así como la implementación de la Estrategia de Gobierno en Línea, establecida en el manual GEL. Esta nueva estrategia, que se plasma en el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones número 1078 de 2015, comprende cuatro grandes propósitos: lograr que los ciudadanos cuenten con servicios en línea de muy alta calidad, impulsar el empoderamiento y la colaboración de los ciudadanos con el Gobierno, encontrar diferentes formas para que la gestión en las entidades públicas sea óptima gracias al uso estratégico de la tecnología y garantizar la seguridad y la privacidad de la información de la entidad.

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 3 de 57

Que el mencionado MSPI del MINTIC, se fundamenta en los lineamientos de las Normas Continuidad del negocio SGCN (Norma ISO/IEC 22301:2012), y seguridad de la información SGSI (Normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013).

Que en Mérito de lo expuesto,

RESUELVE

Artículo 1º. Objeto: Adoptar la Política General de Seguridad de la Información y las Políticas de Seguridad de la Información en la Corporación Autónoma Regional del Centro de Antioquia CORANTIOQUIA como norma fundamental para el desarrollo de proyectos de tecnología con una gestión eficiente y optimización de los recursos, servicios TIC, y los sistemas de información.

Artículo 2º. Ámbito de aplicación: Las políticas aplican a los servidores públicos, contratistas, proveedores y/o terceros usuarios de la información impresa, digital, y la soportada sobre las tecnologías de información y las comunicaciones de la Corporación Autónoma Regional del Centro de Antioquia CORANTIOQUIA.

Artículo 3º. Políticas: La presente resolución adopta las siguientes políticas, que se describen en el documento anexo:

Política General de Seguridad y Privacidad de la Información, en cumplimiento del numeral 5.2 de la Norma ISO/IEC 27001:2013.


Políticas de Seguridad y Privacidad de la Información, en cumplimiento de los requerimientos del numeral A.5, Anexo A de la Norma ISO/IEC 27001:2013.

Artículo 4º. Implementación: Todas las dependencias de la Corporación Autónoma Regional del Centro de Antioquia CORANTIOQUIA deberán implementar las políticas adoptadas a través del presente acto administrativo, conforme a sus responsabilidades y competencias.

Artículo 5º. Vigencia: La presente Resolución rige a partir de la fecha de su expedición.

Dado en la ciudad de Medellín, el

PUBLÍQUESE Y CUMPLASE

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 4 de 57

ALEJANDRO GONZÁLEZ VALENCIA
Director General

Elaboró: xxxxxx
Revisó: xxxxx
Aprobó: xxxxxx


POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE CORANTIOQUIA

1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración de CORANTIOQUIA, con respecto a la protección de los activos de información integrados por los funcionarios y/o servidores públicos, contratistas, proveedores, la información, los procesos, las tecnologías de información incluido el hardware y el software que en su conjunto, soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Para asegurar la dirección estratégica de la Entidad, CORANTIOQUIA establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 5 de 57

- Mantener la confianza de los funcionarios, contratistas y proveedores.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información (SGSI).
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de CORANTIOQUIA.
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad


Esta política aplica a toda la entidad, sus funcionarios, servidores públicos, contratistas y proveedores de CORANTIOQUIA, y la ciudadanía en general.

Nivel de Cumplimiento de la Política

Todas las personas cubiertas por el alcance y aplicabilidad, deben dar cumplimiento del 100% de la presente política.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de CORANTIOQUIA:

1. CORANTIOQUIA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información (SGSI), soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o proveedores.
3. CORANTIOQUIA protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
4. CORANTIOQUIA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. CORANTIOQUIA protegerá su información de las amenazas originadas por parte del personal.

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 6 de 57

6. CORANTIOQUIA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. CORANTIOQUIA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. NOMBRE DE LA ENTIDAD implementará control de acceso a la información, sistemas y recursos de red.
9. CORANTIOQUIA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. CORANTIOQUIA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
11. CORANTIOQUIA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
12. CORANTIOQUIA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.


2. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE CORANTIOQUIA

2.1. Política de Organización de la Seguridad de la Información

OBJETIVO

Establecer las políticas que le permitirán a CORANTIOQUIA realizar la asignación de responsabilidades y gobernabilidad del Sistema de Gestión de Seguridad de la Información (SGSI).


ESTRUCTURA PARA LA SEGURIDAD DE LA INFORMACION

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 7 de 57

- Se debe establecer un responsable del liderazgo y coordinación del SGSI, y velar porque las directrices estratégicas de seguridad de la información se cumplan en la Entidad. Este rol se denominará Líder del Sistema de Gestión de Seguridad de la Información (SGSI).
- Se debe conformar un Comité de Seguridad de la Información que respalde y apoye las iniciativas de seguridad. Los miembros deben tener cierta relevancia en su cargo dentro de la organización y deben avalar y definir las directrices estratégicas de seguridad de la información. Este comité deberá reunirse por lo menos una vez por semestre. Las funciones de este comité son:
 - Revisión y aprobación de la política de seguridad y documentos asociados.
 - Seguimiento a incidentes de seguridad de la información.
 - Establecer planes de gestión de riesgos y análisis de resultados.
 - Definir planes de concientización.
 - Asegurar la implementación, mantenimiento y mejora continua del SGSI.
- Todos los funcionarios deben ser responsables del manejo adecuado de la información dentro y fuera de la Entidad, de su comunicación y divulgación, deben conocer la política general y las políticas específicas de la seguridad de la información y estar en la obligación de cumplirlas.
- En cada sesión del Comité de Seguridad de la Información se deberán realizar auditorías o revisiones al proceso de gestión de la seguridad de la información, es responsabilidad de todos los usuarios involucrados en las auditorías, la atención y colaboración para la ejecución de las mismas.
- Es de vital importancia que la Entidad establezca contactos con grupos especializados en seguridad de la información. El líder del SGSI o el que él determine, deberá estar inscrito en foros académicos de seguridad de la información para mantenerse al día sobre amenazas y vulnerabilidades que puedan afectar a la Entidad.
- El Coordinador del Grupo Interno de Trabajo de Recursos Físicos deberá establecer contactos con autoridades que pueden ser de apoyo en algún momento para la Entidad y debe pertenecer al Comité de seguridad de la información.

CONTRATISTAS, PROVEEDORES Y/O TERCEROS

- Se deben definir procedimientos para la autorización de acceso de contratistas, proveedores y/o terceros a los sistemas de información o servicios. Cada contratista, proveedor y/o tercero debe tener un responsable dentro de la

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 8 de 57

Entidad que asegure que conozca la política general y las políticas específicas de la seguridad de la información y cumpla con las directrices descritas en esta.

- En los contratos con contratistas, proveedores y/o terceros, CORANTIOQUIA deberá incluir una cláusula y un acuerdo de confidencialidad y no divulgación, que determinen las responsabilidades de las partes en cuanto al manejo de la seguridad de la información, así como las consecuencias y medidas a tomar por el incumplimiento de las mismas.
- Se deben identificar los riesgos que implica el acceso de contratistas, proveedores y/o terceros a la Entidad e implementar controles que reduzcan dicho riesgo. Todo acceso de un contratista, proveedor y/o tercero a los sistemas de información de la Entidad debe ser autorizado y seguir los procedimientos establecidos.
- En los acuerdos con terceras partes que impliquen cualquier tipo de interacción con información de CORANTIOQUIA se deben incluir todos los aspectos de seguridad relevantes y el compromiso a su cumplimiento.


2.2. Política de Seguridad del Recurso Humano

OBJETIVO

Asegurar que todos los funcionarios, contratistas, proveedores y/o terceros entiendan sus responsabilidades y sean conscientes sobre la seguridad de la información y su importancia dentro de la Entidad. Asegurar un ciclo laboral con transiciones seguras minimizando el riesgo de fuga de información.


TÉRMINOS Y CONDICIONES DE LA RELACIÓN LABORAL

- Los funcionarios, contratistas, proveedores y/o terceros con acceso a los activos de información de CORANTIOQUIA deben conocer, entender y seguir la política general y las políticas específicas de seguridad de la información de la Entidad.
- Todos los funcionarios, contratistas, proveedores y/o terceros deben informar acerca de los eventos que atenten contra la seguridad de la información de CORANTIOQUIA, así como los eventos potenciales u otros riesgos que sean de su conocimiento.

	<p>Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 9 de 57

- En la etapa de vinculación de funcionarios y contratistas a la Entidad, el Grupo Interno de Trabajo de Talento Humano debe verificar la identidad, ética profesional, antecedentes y conducta de los mismos.
- Todos los funcionarios, contratistas, proveedores y/o terceros que tengan acceso a información confidencial, deben firmar un acuerdo de confidencialidad y no divulgación, antes de tener acceso a los servicios de procesamiento de información y a la información en cualquiera que sea su estado y/o medio de almacenamiento. El Grupo Interno de Trabajo de Talento Humano debe asegurar que este acuerdo sea incluido en el contrato de los funcionarios. Cada área responsable por su contratista debe verificar y asegurar que se ha firmado ese acuerdo antes de iniciar la relación laboral.
- La Oficina de Control Interno deberá verificar el correcto cumplimiento, así como la existencia, de estos acuerdos de confidencialidad y no divulgación, a través de revisiones periódicas, auditorías o como lo considere pertinente.
- Como parte de su obligación contractual, funcionarios, contratistas, proveedores y/o terceros deberán aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y responsabilidades con la Entidad. En este se acepta el conocimiento y entendimiento la política general y las políticas específicas de seguridad de la información y su compromiso a cumplirla.
- Cada contrato debe declarar las sanciones que se aplicarán en caso que un funcionario, contratista, proveedor y/o tercero incumpla alguno de los requisitos de seguridad de la información establecidos en el contrato laboral, el acuerdo de confidencialidad y no divulgación, la política general o las políticas específicas de seguridad de la información.
- El Grupo Interno de Trabajo de Talento Humano debe asegurar que cada funcionario en la fase de inducción reciba una sensibilización en seguridad de la información y su importancia para la Entidad.
- El Grupo Interno de Trabajo de Talento Humano en conjunto con cada jefe responsable deben garantizar el adecuado retiro o cambio de funciones de los funcionarios, de manera que todos los permisos, accesos e información del cargo anterior sean retirados y eliminados de manera segura.
- El área encargada de cada contratista, proveedor y/o tercero debe garantizar el adecuado retiro o cambio de funciones de los mismos, de manera que todos los permisos, accesos e información sean retirados y eliminados de manera segura.

2.3. Política de Gestión de Activos

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 10 de 57

OBJETIVO


Definir la protección adecuada de los activos de información de la Entidad, definiendo el debido control sobre la información, incluyendo el inventario de todos los activos, su clasificación, propietarios y las directrices de tratamiento.

RESPONSABILIDAD SOBRE LOS ACTIVOS

- Todos los procesos incluidos en el alcance del Sistema de Gestión de Seguridad de la Información deben realizar el inventario de activos de información de su proceso, basados en el instructivo de inventario y valoración de activos de información definido por la Entidad. Todos los activos deberán estar debidamente identificados y clasificados. Además, deben asignar un propietario para cada activo y definir las regulaciones para el uso adecuado de dicha información.
- El líder del SGSI deberá validar que todos los procesos estén desarrollando las actividades de inventario y valoración de activos de información.
- La Oficina de Control Interno es responsable de realizar auditorías para verificar que los procesos mantienen actualizado su inventario de activos de información y que cumplen con el instructivo definido para tal fin.
- Los usuarios de la información son responsables, mientras tengan la información bajo su control o acceso, de mantener los niveles de protección y clasificación establecidos para la misma en todo momento, haciendo uso adecuado de los recursos a su disposición.

PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los activos de información son los procesos que tengan responsabilidad directa designada de la Entidad sobre los mismos. Además, dichos propietarios de los activos deben definir la prioridad y protección para el acceso a estos.
- Los propietarios de los activos de información, con la asesoría del líder del SGSI, son los que definirán los mecanismos de protección y los permisos de acceso a estos.
- Los propietarios de los activos de información son responsables de su valoración y encargados de garantizar que las personas que tengan acceso a estos, los traten de acuerdo a su valor para la organización.

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 11 de 57

- Los propietarios pueden entregar los activos de información para custodia a los procesos designados por la Entidad; sin embargo, la responsabilidad de su seguridad no se traslada a este último.

CLASIFICACIÓN Y ETIQUETADO

- Los activos de información serán clasificados teniendo en cuenta la valoración de los mismos y el procedimiento definido para tal fin.
- Los activos de información deberán ser etiquetados para que sean tratados de acuerdo con su nivel de importancia para CORANTIOQUIA y atendiendo el instructivo correspondiente.
- Los niveles de clasificación y protección establecidos para los activos de información de CORANTIOQUIA deberán ser mantenidos en todo momento. Por lo tanto, la Entidad garantizará los recursos requeridos para su adecuada protección.


2.4. Política de Control de Acceso

OBJETIVO

Definir el control de acceso a la información soportada por la infraestructura tecnológica y de telecomunicaciones de CORANTIOQUIA.

DIRECTRICES GENERALES DE CONTROL DE ACCESO

- El acceso a la información y los sistemas asociados deben estar debidamente controlados, asegurando que sólo el personal autorizado pueda tener acceso a la información, previa autorización formal por parte del dueño de la información.
- Se deberán mantener registros de las autorizaciones concedidas. Estas autorizaciones deben partir del principio de necesidad de saber, donde el usuario recibirá permisos solo para las actividades para las que fue contratado.
- Los accesos concedidos deben contar con una revisión periódica para verificar si realmente siguen siendo necesarios o necesitan modificación.
- Cualquier cambio de cargo o área que realice un funcionario debe incluir una revisión de los permisos a los que tiene acceso buscando revocar aquellos que no son necesarios en las nuevas funciones que va a realizar.

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 12 de 57

- Se deberán establecer mecanismos de control para los casos en que por funcionalidades requeridas sea necesario compartir información. Estos mecanismos pueden ser:

- Existencia de Autorización por parte del dueño de la información.
- Soporte de un método de autenticación.
- Exclusión de la información sensible.

- Se debe poder identificar el estado de los usuarios que están compartiendo la información y mantener un inventario de estos accesos.

- Se deberá mantener documentado el inventario de usuarios de los sistemas de información y los accesos y roles que se tienen en los diferentes sistemas de información y demás infraestructura tecnológica. Estos temas incluyen a los administradores de plataforma.

- Se deberán actualizar los accesos definidos debido a novedades a nivel del personal.

- Todo contratista, proveedor y/o tercero deberá tener acceso limitado a la información. No deberá tener alcance a ninguna información confidencial a no ser que sea autorizado explícitamente por el dueño de la misma, en cuyo caso se deberá firmar un acuerdo de confidencialidad y de no divulgación.


- Las cuentas asignadas a contratistas, proveedores y/o terceros deben tener un periodo de tiempo de vigencia o expiración asignado, que corresponde como máximo al tiempo de vigencia de contrato o alianza.

- La solicitud de acceso a los recursos informáticos brindados por CORANTIOQUIA solo será autorizado a personas que mantienen un vínculo con la Entidad. La incorporación de personas diferentes deberá ser autorizada por el responsable del contrato (en el caso de contratistas) o por el área que requiera que esta persona tenga acceso. (Estos accesos deberán responder el principio del mínimo privilegio).


- Las solicitudes de acceso deben contar, como mínimo, con la siguiente información:

- Recursos y Servicios a los que requiere acceso.
- Tiempo de acceso a esos recursos y servicios.
- Compromiso de notificación frente al cese de actividades.

(Novedades).

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 13 de 57

- El acceso a los componentes de la infraestructura tecnológica y de telecomunicaciones debe ser estrictamente controlado para prevenir el acceso no autorizado.
- Las cuentas de usuarios creadas deben ser únicas, personales e intransferibles, toda la responsabilidad de lo que suceda con esta cuenta recae sobre el usuario que tiene la cuenta.
- Se debe asegurar que el acceso a los servicios de red, datos y programas estén disponibles solamente para el personal específicamente designado por CORANTIOQUIA.
- Los responsables del ambiente tecnológico serán los únicos responsables de la ejecución de comandos especiales sobre componentes críticos, sea por medio de acceso local o remotamente.
- Antes de efectuar una solicitud, el usuario deberá identificar qué servicios requiere de los componentes de infraestructura tecnológica y de telecomunicaciones.
- Para cada servicio se debe seguir el procedimiento propio de control de acceso. En caso que este no exista deberá ser documentado y autorizado por el personal definido.
- Una vez se notifiquen modificaciones en el personal, se deberá evaluar si los accesos a los sistemas de información y componentes de la infraestructura tecnológica y de telecomunicaciones del usuario que se retira deben ser eliminados.
- En el caso de un cambio a los componentes de la infraestructura tecnológica y de telecomunicaciones el esquema de seguridad debe reevaluarse en su totalidad.
- Todo componente de la infraestructura tecnológica y de telecomunicaciones deberá tener un mecanismo que permita el registro de los usuarios de servicios informáticos y los derechos de acceso.
- Los procedimientos de ingreso (login) deben ser estrictamente observados y los usuarios que se retiran de sus puestos de trabajo deben primero bloquear el acceso a su estación de trabajo o cerrar la sesión (logoff).
- La autorización para acceder a los componentes de la infraestructura tecnológica y de telecomunicaciones debe ser autorizado por el dueño del ambiente tecnológico.

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 14 de 57


DIRECTRICES ESPECÍFICAS DE CONTROL DE ACCESO A LA INFORMACIÓN

Usuarios Privilegiados:

- Los usuarios privilegiados son los superusuarios creados por defecto en la instalación de los componentes de la infraestructura tecnológica y de telecomunicaciones.
- Los usuarios privilegiados son todos aquellos que realizan actividades de administración en la infraestructura tecnológica y de telecomunicaciones con los máximos privilegios que requiere su función.
- Los usuarios privilegiados son todos aquellos identificadores de usuario que requieren ser asignados a funcionarios cuyo cargo y/o funciones está relacionado con la administración funcional y/o tecnológica de sistemas de información.
- Los usuarios privilegiados solo serán otorgados a aquellas personas que lo requieran para el cumplimiento de sus funciones.
- Deberá existir una cuenta de acceso que será utilizada exclusivamente para monitoreo por parte del área de seguridad de la información o quien haga sus veces, para revisar el uso de estos usuarios privilegiados.
- Las personas que por sus funciones requieran acceso de usuario privilegiado deben solicitarlo siguiendo el procedimiento establecido por CORANTIOQUIA para solicitud de acceso a componentes de la infraestructura tecnológica y de telecomunicaciones.
- Ningún usuario privilegiado debe modificar información sin previa autorización de su dueño.
- Las cuentas de usuarios privilegiados deben ser de uso personal e intransferible.
- Las cuentas privilegiadas deben contar con una clave que debe ser almacenada en un lugar seguro y con acceso solamente a personal autorizado.

Usuarios Genéricos:

- Cualquier área de CORANTIOQUIA podrá solicitar la creación de usuarios genéricos en los diferentes componentes de la plataforma tecnológica justificando por escrito la necesidad de los mismos y asumiendo el conocimiento de las implicaciones de control que requiere la utilización de estos usuarios genéricos.

	<p>Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 15 de 57


- La creación de un usuario genérico debe ser autorizada por el dueño de la Información, el Jefe inmediato y el área de Seguridad de la Información o quien haga sus veces.
- Los usuarios genéricos solo deben establecerse con fines de consulta de datos, no de actualización (ingreso, eliminación y modificación).
- Todas las cuentas con permisos de ingreso, eliminación o modificación de información deben ser de carácter personal y sus contraseñas deben seguir los parámetros establecidos por la Entidad.

Usuarios con altos privilegios en Bases de Datos (Superusuarios):

- Los superusuarios de aplicativos que requieren acceso a las bases de datos son responsabilidad de los administradores de las bases de datos, quienes deberán monitorearlos.
- Al realizar la creación de cuentas, el administrador debe asegurarse que las transacciones que se realizan puedan ser asociadas con el sistema de información y el usuario que la realizó, para que de esta manera se puedan realizar seguimientos y auditorías.
- La creación de los superusuarios a nivel de bases de datos deberá ser definida y justificada técnicamente por los desarrolladores de los aplicativos y administradores de servicios informáticos.
- Debe evitarse la asignación de roles propios del administrador de la base de datos a los usuarios, desde el sistema operativo.

Actualización de accesos a componentes Tecnológicos:

- Debe existir un procedimiento formal para la creación, actualización y eliminación de accesos a los diferentes componentes de la plataforma tecnológica existentes en CORANTIOQUIA.
- Toda novedad presentada en la planta de personal de funcionarios, contratistas, proveedores y/o terceros de CORANTIOQUIA (ingresos, licencias, sanciones, comisiones, suspensiones, ascensos, renuncia, muerte y/o retiros) deberá ser reportada por la persona responsable de cada área.
- Los dueños de la información, serán los responsables de velar por que los roles y/o perfiles de acceso existentes sean acordes con las funciones realizadas por cada uno de los usuarios.

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 16 de 57

- El acceso a componentes tecnológicos por medios remotos para actividades de mantenimiento, soporte y monitoreo por parte del proveedor del componente, está permitido si la conexión remota cumple con los requerimientos de seguridad de CORANTIOQUIA.


2.5. Política de Seguridad Física y del Entorno

OBJETIVO

Minimizar los riesgos potenciales que puedan resultar en pérdida de información por robo o daño a los recursos informáticos, de manera accidental o por accesos no autorizados.

ESCRITORIO SEGURO

- Ningún usuario debe tener información confidencial de la Entidad en su puesto de trabajo, ni escrita en lugares visibles o fácilmente accesibles. Deben mantener su escritorio limpio y con la información bien almacenada. Deben mantener presente no publicar o dejar a la vista, documentos o datos sensibles, como por ejemplo:
 - Nombre de Usuario y contraseña.
 - Direcciones IP e información sobre la plataforma informática de CORANTIOQUIA.
 - Números de cuenta bancaria.
 - Propiedad Intelectual.
 - Información privada de personas naturales y/o jurídicas.
 - Cualquier activo clasificado como no público.
- En la jornada laboral u horas extras, cada funcionario, contratista, proveedor y/o tercero debe garantizar que los sistemas de información y elementos de procesamiento deben estar adecuadamente protegidos, teniendo presente que se debe guardar documentos confidenciales, discos externos, memorias USB, etc. en cajones bajo llave cuando no se estén utilizando.
- Cada usuario es responsable de proteger los sistemas de información a su cargo, computador, dispositivo móvil, memorias, etc. Los usuarios con computador portátil deben tenerlo asegurado al escritorio con una guaya de seguridad.
- Cada usuario debe asegurar que su computador o estación de trabajo no quede desatendida. Cuando el usuario no esté al frente de su estación de trabajo esta debe quedar bloqueada con el fin de evitar suplantación de identidad, ya que cada persona es responsable por lo que se haga con su usuario personal.


	<p>Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 17 de 57

ÁREAS SEGURAS

- El Grupo Interno de Trabajo de Recursos Físicos debe documentar y actualizar todos los procedimientos de acceso físico definidos para la gestión de la seguridad física en CORANTIOQUIA.
- El Grupo Interno de Trabajo de Recursos Físicos deberá llevar una bitácora de acceso de personal externo a las instalaciones de la Entidad. Esta bitácora deberá estar disponible al menos por seis (6) meses.
- Todos los funcionarios deberán portar su carné de identificación en un lugar visible, el personal externo deberá portar su identificación de visitante.
- Se deberá mantener una bitácora de ingreso a los sitios o áreas seguras, especialmente en las áreas de acceso restringido y centros de cómputo. Esta información deberá ser revisada y mantenida como registros de seguridad. Esta bitácora deberá estar disponible al menos por seis (6) meses.
- El acceso al centro de cómputo deberá ser autorizado por el Coordinador del Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones.
- El Grupo Interno de Trabajo de Recursos Físicos deberá proponer ante el Comité de Seguridad de la Información los controles para la protección de las amenazas externas y ambientales que se consideren pertinentes y adecuados a cada una de las áreas.
- El Grupo Interno de Trabajo de Recursos Físicos deberá documentar e informar el procedimiento pertinente para la utilización de las áreas de cargue y descargue de suministros o mercancía.
- Los accesos de personal externo a CORANTIOQUIA deberán estar autorizados por un funcionario de la Entidad. El funcionario autorizador deberá acompañar en todo momento al visitante, y será el responsable por las acciones realizadas por este dentro de la Entidad.

ÁREAS DE ACCESO RESTRINGIDO


- En las instalaciones de CORANTIOQUIA, se deben identificar áreas especiales que mantienen recursos de información o instalaciones sensibles o críticas para las operaciones diarias de la Entidad. Estas áreas deben mantener controles de acceso adecuados para su protección.

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 18 de 57

- El acceso a áreas seguras debe realizarse desde áreas internas. No deben tener forma de acceso desde el exterior.
- Cada una de las áreas de acceso restringido debe tener identificado formalmente un responsable de la misma, en el caso del centro de cómputo principal el responsable es el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones.
- Se debe mantener una bitácora de registros con el ingreso de cada persona al área restringida y en especial al centro de cómputo, y debe guardarse el histórico de por lo menos 6 meses. Esta bitácora debe contener la siguiente información
 - Nombre de quien autoriza.
 - El nombre del visitante autorizado,
 - Razón social (si corresponde) o motivo,
 - Fecha y hora del acceso, y la firma.
 - Duración de la autorización (única vez ó periodo determinado).
- Los responsables de cualquier tipo de área controlada tienen que mantener controles de acceso efectivos, en proporción a los recursos humanos y al valor de los activos a proteger.

PROTECCIÓN DE LOS EQUIPOS DE CÓMPUTO


- Se deberán establecer procedimientos de ingreso, transporte, movimiento, eliminación y retiro de los recursos tecnológicos.
- Se debe garantizar la disponibilidad de los recursos y servicios necesarios para la adecuada operación de los recursos tecnológicos que soportan la información de CORANTIOQUIA. (Por ejemplo: suministros de energía eléctrica, condiciones ambientales, control de acceso, entre otras).
- Se deben establecer las acciones necesarias para coordinar, apoyar, capacitar y responder frente a eventos o escenarios catastróficos que puedan afectar a las personas que laboran en la Entidad, así como los activos y medios que permiten procesar la información de la misma. Esta información debe ser incluida en el DRP.
- Antes de ingresar equipos a los centros de cómputo, se deben identificar al menos los siguientes requerimientos con el fin de tomar decisiones de acuerdo con lo que puede ofrecer el centro de cómputo y no afectar a los demás equipos allí ubicados.

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 19 de 57

- Consumo de potencia.
 - Carga Calórica generada.
 - Características de temperatura soportadas.
 - Área ocupada (Dimensiones).
- Los dispositivos de almacenamiento con información sensible deberán ser destruidos una vez su vida útil haya finalizado, esto deberá estar enmarcado en un programa de renovación y actualización tecnológica ejecutado por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones, con el fin de no conservar medios obsoletos que contengan información confidencial o sensible.
 - En el caso de terminar la vida útil de un equipo, ya sea por daño o porque se encuentra enmarcado en un proceso de renovación tecnológica, la información que este posea deberá ser destruida a través de mecanismos seguros, tales como equipos de desmagnetización para discos, herramientas de sobre-escritura de información, borrado a bajo nivel, y otros. Estas herramientas deben ser aprobadas por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones y utilizada por el personal de asistencia.
 - El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones debe definir un procedimiento para el retiro o traslado de equipos de las instalaciones de la Entidad. Todo traslado o movimiento de equipos informáticos debe hacerse siguiente este procedimiento.
 - En prácticas de arrendamiento de equipos, se deberán aplicar las medidas de borrado seguro de información de estos una vez se termine el periodo de alquiler. Estos elementos deberán ser contenidos en el procedimiento de devolución de equipos.

MANTENIMIENTO DE EQUIPOS


- El mantenimiento de equipos deberá realizarse en una zona especial definida para este fin, manteniendo las características de control de acceso y seguridad de los equipos de acuerdo con la información que estos soportan.
- Se deberán tener procedimientos de mantenimiento documentados para los equipos de cómputo. Tanto para equipos servidores como para estaciones de trabajo.
- Para los equipos que por labores de mantenimiento deban ser llevados fuera de las instalaciones de CORANTIOQUIA, deberán establecerse medidas de control para evitar que la información sensible contenida sea divulgada. Por esta razón, la información contenida en estos, deberá ser retirada de los

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 20 de 57

dispositivos, con el fin de evitar que personal externo tenga acceso a la misma o pueda ser copiada. Estos elementos deberán estar contenidos en los procedimientos de mantenimientos de equipos.

CENTRO DE CÓMPUTO

- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones tiene la obligación de definir los requerimientos de seguridad física necesarios para los componentes tecnológicos en los centros de cómputo, almacenamiento, procesamiento y telecomunicaciones.
- Se debe elaborar un diseño detallado de los mecanismos de restricción de acceso físico, cuya administración permita un registro de los accesos tanto de personal autorizado como de visitantes.
- Se debe desarrollar una evaluación de riesgos de los activos informáticos ubicados en centros de cómputo, procesamiento y telecomunicaciones, que permita establecer el riesgo y los controles necesarios para mitigarlos
- Se deben incluir todos los controles mínimos ambientales que permitan proteger los componentes frente a riesgos ambientales como fuego y agua y aquellos de suministro de energía y aire, de acuerdo al análisis de riesgos definido.
- El personal externo que requiera desempeñar labores en el centro de cómputo ó centros de cableado ubicados en las instalaciones de la Sede Central, debe permanecer acompañado en todo momento por una persona designada por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones.
- Se debe mantener una bitácora de acceso a los centros de cómputo y cableado de todo el personal, indicando la fecha y hora de ingreso, así como el responsable que autoriza el ingreso.
- Se debe elaborar una política específica de acceso al centro de cómputo, donde se definan los procedimientos de ingreso, los cuidados que se deben tener, las obligaciones de cada persona que ingresa y las políticas que debe respetar.
- Las labores de mantenimiento y aseo de estos centros deberá estar sujeto a un procedimiento formal, donde se indique en qué puntos se pueden conectar equipos de aseo, como se maneja el material de limpieza y como se debe registrar la persona que realiza el aseo.

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 21 de 57


- Se deben verificar los riesgos potenciales que tienen este tipo de trabajos e informarlos a los responsables del centro de cómputo para que tomen las medidas necesarias para evitar daños en los equipos.
- Para los centros de cómputo de CORANTIOQUIA se deberá revisar la inclusión de los siguientes controles y prácticas frente a:

Sistema eléctrico:

- El centro de cómputo debe tener generador de respaldo (planta eléctrica autónoma).
- El centro de cómputo debe tener sistema ininterrumpido de potencia (UPS) de respaldo y mantenimientos periódicos de revisión de la vida útil de las baterías.
- El centro de cómputo debe tener sistema de aire acondicionado acorde a las necesidades de flujos de aire y temperaturas de acuerdo a las especificaciones de los equipos, este sistema debe contar con mecanismos de apagado automático en caso de incendios. Se deberá realizar una evaluación anual sobre las condiciones ambientales y de temperatura de estos centros (Cómputo y Cableado).
- El centro de cómputo debe tener un sistema de tierra independiente.
- El centro de cómputo debe mantener actualizado un plano de conexiones eléctricas de todos los equipos y las tomas eléctricas deberán encontrarse identificadas.
- El centro de cómputo debe tener sistema de alumbrado automático de manera que cuando en el centro no se encuentren personas, permanezca apagado.

Ubicación de equipos:

- Se deberá mantener un inventario de los equipos ubicados en cada uno de los centros de cómputo y de cableado de CORANTIOQUIA.
- Se deberá tener en cuenta la correcta ubicación para garantizar la correcta disipación de calor de los equipos.
- Se deben realizar periódicamente estudios de temperaturas en los centros de cómputo donde se encuentran almacenados los equipos.

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 22 de 57

Aire acondicionado:


- Deberá disponerse de los equipos de aire acondicionado necesarios (por lo menos dos para proveer respaldo) para mantener la temperatura y la humedad adecuadas para los equipos.
- Se deben hacer revisiones periódicas sobre los equipos de aire para evitar problemas relacionados con la condensación del aire, goteos de agua, por lo tanto se deberá tener especial cuidado en los drenajes necesarios cerca de estos.
- Los aires acondicionados deben conectarse a los sistemas eléctricos de emergencia (planta eléctrica), pues en caso de falta de electricidad, este servicio no puede suspenderse sin el consecuente daño a los equipos.
- Los aires acondicionados deberán poseer sistemas de automatización de arranque y de respaldo.
- El centro de cómputo deberá tener adecuados detectores de temperatura y humedad y un registro histórico de estas variables.
- Los equipos deberán tener soporte para interrupción inmediata en caso de incendios en el centro de cómputo.

Sistema de detección y extinción de incendios:

- Todo centro de cómputo deberá tener detectores de incendio adecuados y deberá seguir a la norma de la NFPA (National Fire Protection Association) NFPA 75: Protección de equipos electrónicos procesadores de datos por computador Referencia: XE 75 92E.
- Las puertas de salida de emergencia, los detectores de incendio, los sistemas de alarma visual y auditiva y los procedimientos de activación y desactivación de los sistemas deberán ensayarse al menos cada dos meses para comprobar su correcto funcionamiento.
- Deberá tenerse una señalización adecuada de todos estos elementos.

Mantenimiento:

- Todos los equipos necesarios para el adecuado funcionamiento del centro de cómputo deberán estar amparados con contratos de mantenimiento preventivo y correctivo. El Grupo Interno de Trabajo de Tecnologías de la

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 23 de 57

Información y las Comunicaciones deberá coordinar junto con el Grupo Interno de Trabajo de Recursos Físicos las actividades de mantenimientos mediante la programación anual de mantenimientos sobre los equipos de cómputo, los controles ambientales y de protección contra fuego, detección de humedad, plantas eléctricas, UPS, entre otros.


2.6. Política de Seguridad de las Comunicaciones y Operaciones

OBJETIVO

Asegurar la operación correcta y segura de los servicios de procesamiento de información mediante la definición de actividades orientadas a establecer controles de seguridad y la definición de estándares y lineamientos de seguridad para ser cumplidos por toda la organización.

ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES


- Antes de que cualquier sistema operativo, herramienta y/o software en general sea instalado en la Entidad, el personal designado para tal fin debe deshabilitar o renombrar todas las cuentas privilegiadas existentes por defecto o creadas por los proveedores.
- Los funcionarios deben abstenerse de instalar o desinstalar software en sus equipos de cómputo. Esta tarea solo debe ser realizada por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones.
- Los equipos de cómputo pertenecientes a CORANTIOQUIA deben ser utilizados únicamente para propósitos corporativos, el almacenamiento de información de carácter personal en los mismos no será responsabilidad de CORANTIOQUIA.
- Todos los sistemas de información deberán tener la hora sincronizada.
- Las configuraciones, protocolos o software que no sean utilizados, y que no sean necesarios para las labores diarias, deberán ser desinstalados o deshabilitados.
- Las extensiones, modificaciones o reemplazos a los sistemas operativos de producción deben ejecutarse antes bajo ambientes de desarrollo y pruebas, y deben tener aprobación del Comité de cambios.

	<p>Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 24 de 57

- El área de Seguridad de la Información o quien haga sus veces, debe realizar revisiones periódicas o evaluaciones de vulnerabilidades sobre los sistemas operativos de producción.
- Todos los sistemas operativos en producción, los sistemas de administración de bases de datos, Firewalls, IDS, IPS, aplicaciones y todo el software existente en la plataforma de CORANTIOQUIA, debe mantenerse en las versiones estables más recientes que mantengan compatibilidad con los demás componentes de los sistemas de información.
- Para todos los cambios en los sistemas de producción se deben desarrollar procedimientos adecuados de devolución (Rollback), según lo indica el procedimiento de cambios, los cuales permitan devolverlos rápida y oportunamente a las condiciones previas al cambio más reciente en el software.
- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones será responsable del monitoreo de la capacidad de la plataforma tecnológica procurando identificar oportunamente elementos que puedan conllevar a la no disponibilidad de la misma o la afectación de la información que soportan.
- Se debe realizar una revisión periódica de las reglas de los Firewalls, routers y switches de Core (mínimo cada 6 meses), de manera que siempre se tenga una configuración actualizada y adecuada. Se debe sacar un informe del resultado de la revisión de reglas con la información de la reglas borradas o cambiadas.
- El manejo de equipos de seguridad solo debe ser realizado por el área de Seguridad de la Información o quien haga sus veces.
- Los equipos de la infraestructura de telecomunicaciones solo deben ser manejados por el personal designado por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO

- Se debe contar con un software antivirus aprobado por el área de Seguridad de la Información (o quien haga sus veces), que se encuentre monitoreando y proteja todas las estaciones de trabajo existentes en la plataforma informática de CORANTIOQUIA. Este debe mantenerse al día y tener políticas de actualización de firmas y software.
- Cualquier usuario que sospeche de una infección por un software malicioso debe apagar inmediatamente el computador involucrado, desconectarlo


	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 25 de 57

de cualquier red, contactar al Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones y evitar cualquier intento de eliminar el virus.

- Solamente los Administradores de sistemas y/o personal autorizado por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones y el área de Seguridad de la Información (o quien haga sus veces) deben realizar las tareas de desinfección de los elementos de la red informática de CORANTIOQUIA.
- Los usuarios no deben transferir y/o bajar software a los equipos de cómputo de CORANTIOQUIA. Esta labor la debe llevar a cabo el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones con aprobación del área de Seguridad de la Información o quien haga sus veces.
- Cualquier sistema de almacenamiento como disquetes, CD-ROMs, cartuchos ópticos, cintas DAT, etc., provistos por entidades externas no deben ser utilizados en los sistemas de CORANTIOQUIA, a menos que éstos medios hayan sido analizados con el sistema antivirus de la Entidad y se asegure que no contienen ningún software malicioso.
- Todos los servidores y computadores de CORANTIOQUIA, deben estar en constante análisis por el antivirus definido. Se debe programar una tarea de análisis periódico de los sistemas y evaluación de resultados por parte del área de Seguridad de la Información o quien haga sus veces.
- Los usuarios no deben escribir, generar, compilar, copiar, almacenar, propagar, ejecutar o intentar introducir cualquier código de computador diseñado para auto replicarse, deteriorar o que obstaculice el desempeño de cualquier sistema de CORANTIOQUIA o de cualquier entidad externa.
- No deben ejecutarse actualizaciones a los programas de software instalados en los computadores asignados por CORANTIOQUIA para el desarrollo de las labores contratadas, éstas actualizaciones serán realizadas o dirigidas directamente por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones y el área de Seguridad de la Información o quien haga sus veces.

PROTECCIÓN DURANTE LA NAVEGACIÓN


- Se debe tener un sistema de control de navegación en Internet que proporcione análisis de sitios malicioso o con Malware y que permita implementar políticas de navegación basado en los grupos del directorio activo.

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 26 de 57

- Se debe restringir el acceso a sitios peligrosos, donde se pueda compartir información en línea (como Dropbox, Mega, etc) o que puedan afectar la productividad del funcionario.
- Se deben generar reportes periódicos donde se observe los usuarios que más consumen ancho de banda, los sitios más visitados, etc. Y con estos análisis tomar decisiones que mejoren el nivel de servicio de Internet.
- Se deben realizar campañas sobre el buen uso de Internet para concientizar a las personas sobre los peligros de descargar archivos, acceder a sitios desconocidos o de baja confianza y aceptar los mensajes sobre instalación de software que brinde el navegador y el acceso a sitios seguros.
- Se deberán establecer mecanismos de protección y autenticación para evitar que contratistas, proveedores y/o terceros no autorizados accedan a la infraestructura de Internet de CORANTIOQUIA.
- Se debe configurar una red independiente de acceso a Internet para los invitados, la cual debe manejar un portal cautivo donde se puedan autenticar. Estos accesos deben ser autorizados y se deben asignar por un tiempo definido. Esta red no debe tener acceso a la red interna de CORANTIOQUIA ni debe ser utilizada por funcionarios, contratistas, proveedores y/o terceros que trabajen en la Entidad tiempo completo y tengan usuario en el dominio.
- Ningún funcionario debe utilizar software obtenido desde Internet o de una persona u organización diferente a los distribuidores confiables o conocidos, a menos que el software haya sido examinado en busca de código malicioso y que haya sido aprobado por el área de Seguridad de la Información o quien haga sus veces.
- En ningún momento se debe almacenar información de la Entidad en servidores públicos en Internet.


SEGURIDAD DE MEDIOS

- Se debe establecer una política que defina los mecanismos de protección adecuados para los medios de almacenamiento (USB, CD-ROMs, Discos extraíbles, cintas, memorias, etc) que soportan la información de la Entidad y que disminuyan el riesgo contra la fuga de información.
- Cuando se requiera, por el desarrollo de las funciones, almacenar información en dispositivos móviles se deberá revisar la clasificación del activo de información a fin de verificar que esta pueda ser almacenada en este tipo de

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 27 de 57

dispositivos y se debe solicitar autorización al área de Seguridad de la Información o a quien haga sus veces y al Jefe respectivo.


- Se deben establecer mecanismos de borrado seguro para los equipos que se encuentren en estado obsoleto o cambien de usuario. Las actividades de borrado deben ser ejecutadas por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones con las herramientas aprobadas por el área de Seguridad de la Información o quien haga sus veces.
- Se debe establecer el tipo de protección que tendrán los medios que almacenan información de acuerdo a su clasificación, para evitar riesgos como divulgación, modificación, pérdida y destrucción de manera no autorizada.
- La protección y almacenamiento de la información debe ser definida y tratada de acuerdo a su nivel de clasificación en el inventario de activos.
- Se debe asegurar que todo dispositivo de almacenamiento (memorias, cintas, etc.), así como la información que este soporta, debe conservar las características iniciales con el paso del tiempo. (Evitar la pérdida de información por desactualización de las tecnologías que soportan ese tema).
- Se deben definir, de acuerdo a la sensibilidad de la información y su clasificación, los niveles de autorización y acceso para su manipulación y manejo en los medios de almacenamiento donde se encuentre soportada.
- Se deberán realizar respaldos periódicos del software y la información importante en los sistemas de información de la Entidad. Estos respaldos se deben realizar con la frecuencia apropiada para cada sistema de información. Se debe validar que las copias sean correctas y realizar pruebas de funcionamiento periódicas.
- Las copias de seguridad generadas en el Centro de Cómputo, deben residir en un centro de almacenamiento fuera del edificio donde este se ubique, manteniendo las condiciones requeridas para el almacenamiento. Se deberán mantener los controles y procedimientos necesarios para conocer el estado de cada copia de seguridad.
- Los periodos de retención de copias de seguridad deberán satisfacer los requerimientos de aseguramiento de la continuidad del negocio.
- Se deberán realizar pruebas periódicas para asegurar que los equipos y los medios de almacenamiento no se deterioren para asegurar que cumplan con su función cuando se necesiten.

	<p>Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 28 de 57


- Se deberá establecer un procedimiento para la eliminación de archivos y medios obsoletos con estándares de borrado seguro definidos por el área de Seguridad de la Información o quien haga sus veces.
- Se deberán implantar procedimientos para preparar, almacenar y probar periódicamente la integridad de las copias de seguridad y de toda la información necesaria para restaurar el sistema a una operación normal.
- Se deberán mantener copias de seguridad de todas las versiones de software, parámetros y configuraciones requeridas para una correcta restauración de la información contenida en los medios de almacenamiento.
- Se debe mantener un control de contenido de los medios utilizados, donde se registre información que permita la identificación correcta de la información allí contenida, por ejemplo: fechas, información, expiración, lugar de almacenamiento, etc.
- El dimensionamiento de los requerimientos para el manejo de la estrategia de copias de respaldo de la información, será definido por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones.

ADMINISTRACIÓN Y CONTROLES DE RED

- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones debe asegurar que las configuraciones de todas las máquinas conectadas a la red de CORANTIOQUIA cumplan con la política general y las políticas específicas de seguridad de la información.
- Los encargados de la arquitectura de la plataforma informática y los desarrolladores de los sistemas de información deben restringir el uso de interfaces de red externas y de protocolos a aquellos que hayan sido expresamente aprobados por el área de Seguridad de la Información. Y los accesos se deben restringir solo a quien los necesita.
- Cuando se haga control remoto para labores de soporte o mantenimiento por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones, el usuario solicitante deberá estar frente a su computador monitorizando las actividades desarrolladas.
- El personal del Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones no está autorizado para acceder a la información que se encuentra almacenada en los equipos a los cuales acceden. Solo deben hacerlo bajo autorización expresa del usuario.

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 29 de 57

- Siempre se debe informar al usuario cuando se vayan a realizar labores sobre su equipo.
- Todos los computadores multiusuario conectados a Internet deben ser monitoreados con un sistema de detección de intrusos (IDS) aprobado por el área de Seguridad de la Información.
- Los servidores publicados a Internet deben ser ubicados en una zona desmilitarizada, protegida por un firewall.
- Todas las conexiones entre los computadores de CORANTIOQUIA e Internet o cualquier red pública, deben pasar a través de un firewall aprobado y los controles de acceso relacionados.
- El establecimiento de una conexión directa entre los sistemas de CORANTIOQUIA y computadores de organizaciones externas, debe ser a través del firewall de la Entidad y debe ser aprobado por el área de Seguridad de la Información.
- El área de Seguridad de la Información o quien haga sus veces debe mantener un inventario actualizado de las todas las conexiones de CORANTIOQUIA con redes externas.
- En lo posible no se deben utilizar protocolos de autenticación inseguros (como telnet, FTP, etc.), se debe tratar de utilizar protocolos que transmitan las credenciales cifradas. En caso de solo poderse utilizar protocolos inseguros se deben implementar listas de control de acceso con las máquinas que necesitan acceder al sistema y estos deben ser justificados y documentados (asumiendo el riesgo) ante el área de Seguridad de la Información o quien haga sus veces.
- Las redes inalámbricas que utilice CORANTIOQUIA, deben estar configuradas para utilizar cifrado fuerte en sus comunicaciones y autenticación contra el directorio activo.
- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones debe establecer mecanismos de autorización para controlar quien puede realizar llamadas y bajo qué condiciones.
- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones debe establecer controles de cifrado que permitan proteger la confidencialidad de las llamadas telefónicas.

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 30 de 57


- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones deberá proteger los componentes que hacen parte del servicio de Telefonía IP para evitar ataques a la misma.
- Ningún funcionario incluyendo a los administradores de la plataforma podrá interceptar o escuchar las llamadas de otros funcionarios de CORANTIOQUIA, salvo por orden judicial.
- Sólo se podrán grabar las llamadas cuando esto esté expresamente autorizado por la Entidad o autoridad competente y haya sido informado al personal que está interactuando en la misma.

DOCUMENTACIÓN DE LA SEGURIDAD DEL SISTEMA

- Toda la documentación que describe los sistemas de información o los procedimientos de sistemas de CORANTIOQUIA, debe ser revisada y aprobada por los respectivos coordinadores antes de ser liberada a terceras partes.
- Toda la documentación empleada por CORANTIOQUIA para reglamentar el uso, operación y administración de los sistemas de información no debe ser conservada, extraída o compartida por los funcionarios de la Entidad.
- Toda la documentación empleada por CORANTIOQUIA para reglamentar el uso, operación y administración de los sistemas de información debe mantenerse disponible para su consulta por parte de los autorizados y de igual manera los responsables de la misma deben garantizar su actualización.

INTERCAMBIO DE INFORMACIÓN Y DE SOFTWARE


- Los servidores de Internet no deben ser utilizados para almacenar información crítica de las actividades de CORANTIOQUIA.
- Todos los servidores de CORANTIOQUIA que manejan datos de usuarios con organizaciones o personas externas, deben emplear certificados digitales y deben utilizar cifrado para transferir información entre los sistemas involucrados.
- Toda información acerca de pagos, como números de cuentas corrientes, de tarjetas de crédito, claves, etc. debe permanecer cifrada durante su transporte y almacenamiento.

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 31 de 57

- Cada buzón de correo electrónico debe tener un espacio controlado por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones, según la política de uso definida.
- El correo corporativo no debe ser utilizado para fines personales ni para sacar información de la Entidad.
- Los administradores de sistemas de CORANTIOQUIA, deben establecer y mantener procesos sistemáticos para el registro, retención y destrucción de mensajes de correo electrónico y sus archivos de logs.
- Los administradores de sistemas de CORANTIOQUIA, deben establecer y mantener procesos sistemáticos para limitar el uso y/o transferencia de archivos con extensiones potencialmente peligrosas, detección de contenido malicioso o spam.
- La Entidad, por sí misma, está autorizada a desactivar y posteriormente cancelar las cuentas de correo electrónico que no presenten uso en 2 meses, a menos que el dueño del buzón se encuentre en vacaciones, licencia o incapacidad.


PROTECCIÓN Y RESPALDO DE LA INFORMACIÓN

- Para CORANTIOQUIA la información es considerada como un activo de valor estratégico, por esta razón se deberán implementar los mecanismos necesarios que garanticen un adecuado tratamiento en el ciclo de vida de la información, especialmente para los casos que requieren mantener la disponibilidad de la misma.
- Se deberá preservar la seguridad de la información dando cumplimiento a los principios de Confidencialidad, Integridad, Disponibilidad de CORANTIOQUIA, según el nivel de importancia de la misma.
- Los usuarios de CORANTIOQUIA, dueños de la información, son responsables de alojar la información que necesita ser respaldada en los lugares establecidos para ello.
- Los custodios son responsables de aplicar los controles para la protección de la información según su nivel de clasificación. Así mismo deberán alertar al dueño de la información cuando un activo digital de información requiera medidas especiales de protección.

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 32 de 57

REGISTRO HISTÓRICO DE ACTIVIDADES, INFORMACIÓN INCLUIDA EN LOS LOGS

- Todas las aplicaciones de producción que manejen información sensible de CORANTIOQUIA, deben generar logs que muestren cada modificación, incorporación y borrado de la información. Esto incluye modificaciones a los sistemas de producción y modificaciones a los sistemas fuente.
- Los sistemas que manejen información valiosa, sensible o crítica deben además contener y activar forzosamente el log sobre todos los eventos o procesos relacionados con la seguridad de acceso a los mismos. Ejemplo: Varios intentos de contraseña, intentos de uso de privilegios no autorizados, entre otros.
- Los de procesos relevantes deben de proveer información suficiente para soportar auditorías y contribuir a la eficiencia y cumplimiento de medidas de seguridad. Es importante que el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones acuerde con el dueño de la información sobre cualquier característica especial que estos logs deban incluir, de acuerdo a requerimientos internos o con autoridades externas.
- El acceso a los sistemas debe ser a través de usuarios personales y únicos. En el caso de usar usuarios de servicio o genéricos, se les debe asignar un responsable. Esto para hacer más fácil el registro de actividades.
- Se deben definir períodos para la depuración de logs, dependiendo de la plataforma, su capacidad, las necesidades del negocio y de las normas o regulaciones que puedan aplicar. Durante este período, el administrador del sistema y/o dueño de la información, se debe asegurar que éste no sea modificado, cerciorarse de que no sea leído por personal no autorizado y de igual manera garantizar su retención por el periodo necesario para el negocio o que obligue la ley. Estos aspectos son importantes para la corrección de errores, auditorías o revisión de brechas de seguridad.
- Las principales aplicaciones, plataformas de producción, bases de datos, equipos de red y cualquier otro elemento que contenga, maneja o procese información de usuarios o del negocio deben tener registro de logs activo de manera que permita identificar y detectar eventos o incidentes en la infraestructura de la Entidad.
- Todos los sistemas de CORANTIOQUIA, incluyendo los computadores y servidores, deben tener el horario y calendario sincronizado a un servidor central, el cual se debe sincronizar de una entidad externa. Esto para facilitar actividades de rastreo mediante los del sistema.

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 33 de 57

- Los mecanismos para detectar y registrar eventos de seguridad significativos, deben ser resistentes a los ataques. Estos ataques incluyen intentos de desactivación, modificación, o borrado del software de log. Esto incluye tomar las medidas necesarias para que, aun cuando el log sea apagado o modificado, esta suspensión o modificación quede registrada en el mismo.
- Los logs de todos los sistemas y aplicaciones deben ser conservados de forma tal, que no puedan ser revisados o visualizados por personas no autorizadas. Los funcionarios, contratistas, proveedores y/o terceros autorizados deben contar con una autorización del Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones.
- El Comité de Seguridad de la Información debe solicitar un adecuado manejo de los archivos log de los sistemas que los funcionarios, contratistas, proveedores y/o terceros del Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones manejan.


2.7. Política de Relaciones con los Proveedores

OBJETIVO

Establecer parámetros de contratación de terceros respecto a la seguridad de la información y su compromiso con la misma, definir la responsabilidad del gestor del contrato sobre la asignación y revocación de privilegios para los terceros y establecer directrices especiales que se deben tener en cuanto a la seguridad de la información cuando personas externas a CORANTIOQUIA utilizan los recursos de la Entidad.

COMPUTADORES DE CONTRATISTAS, PROVEEDORES Y/O TERCEROS CONECTADOS A LA RED

- En los contratos o acuerdos con contratistas, proveedores y/o terceros se debe incluir una cláusula o acuerdo de confidencialidad y no divulgación, donde se establezca la responsabilidad en cuanto al uso de la información propiedad de CORANTIOQUIA y al cumplimiento de la política general y las políticas específicas de seguridad de la Entidad. También debe incluir las consecuencias por el incumplimiento a cualquiera de estas dos.
- Se debe contar con un software tipo NAC (Network Access Control) que controle el acceso a la red por parte de contratistas, proveedores, terceros y personal invitado.
- El funcionario que facilite o permita la conexión de un equipo externo a la red corporativa, sin la autorización del Grupo Interno de Trabajo de Tecnologías

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 34 de 57


de la Información y las Comunicaciones asumirá las consecuencias que pudieran presentarse ante un incidente de seguridad.

- Para conectarse a la red de la Entidad, todo contratista, proveedor y/o tercero debe garantizar que su equipo está libre de virus, tiene instalado y actualizado un antivirus aprobado por la Entidad y los parches de seguridad del sistema operativo están al día. Además, la conexión de estos equipos a Internet, cuando están en la red de la Entidad, mediante otros dispositivos como módems o celulares está prohibida.
- En el caso de servicios de outsourcing y contratos de prestación de servicios, que utilicen equipos que están en la red de CORANTIOQUIA de forma permanente, el contratista, proveedor y/o tercero deberá enviar anualmente un certificado en el que garantice que las licencias de software de su propiedad que están siendo usadas en dichos equipos, fueron legalmente adquiridas y/o actualizadas.
- Los equipos de contratistas, proveedores y/o terceros que se conectan regularmente a la red de CORANTIOQUIA deben someterse periódicamente al chequeo básico de seguridad informático definido por la Entidad.
- Las personas que realicen visitas esporádicas a CORANTIOQUIA podrán solicitar el servicio de Internet de Invitados. Esta red debe estar separada lógicamente de la red de la Entidad y no debe tener acceso a ningún recurso interno.
- La red de invitados solo debe usarse por personal invitado a la Entidad, en ningún momento debe ser usada por funcionarios, contratistas, proveedores y/o terceros, los cuales deben usar las redes inalámbricas que tienen asignadas.

2.8. Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

OBJETIVO

Garantizar que la seguridad es parte integral de los sistemas de información, evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones, proteger la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas, garantizar la seguridad de los sistemas de ficheros o carpetas, mantener la seguridad del software del sistema de aplicaciones y la información, y reducir los riesgos originados por la explotación de vulnerabilidades y/o errores técnicos publicados.

	<p style="text-align: center;">Sistema de Gestión Integral -SGI- Resolución</p>	Código: F-GIC-26
		Versión: 02
		Página 35 de 57

REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones identificará y expondrá previo al desarrollo y/o implementación de sistemas de información, los requisitos de Seguridad.
- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones es responsable por la implementación de los requisitos de seguridad identificados y consensuados.
- Antes de la puesta en producción el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones someterá al sistema de información a las distintas pruebas de capacidad y seguridad.
- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones deberá definir las distintas políticas de respaldo y continuidad de los sistemas de información.

SEGURIDAD DE LAS APLICACIONES DEL SISTEMA


- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones identificará y/o propondrá controles apropiados de validación de los datos de entrada, el tratamiento interno y los datos de salida.
- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones desarrollará y/o usará herramientas de prueba idóneas que le permitan adelantarse a errores habituales como desbordamientos de memoria, llenado de tablas, consultas cíclicas e interminables.

CONTROLES CRIPTOGRÁFICOS

- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones identificará y/o propondrá controles criptográficos que permitan la protección de información sensible en los sistemas de información de CORANTIOQUIA (Por ejemplo: Tablas cifradas, uso del directorio activo como método de autenticación y autorización de usuarios, entre otros).

SEGURIDAD DE LOS FICHEROS O CARPETAS DEL SISTEMA

- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones identificará y/o propondrá controles que permitan la protección de información contenida en las distintas carpetas del sistema de información, carpetas

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 36 de 57

en el sistema operativo, ficheros en rutas no convencionales propias del aplicativo, entre otros.

- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones evitará exponer datos sensibles en ambientes de prueba.
- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones garantizará el adecuado almacenamiento de los códigos fuentes, además que deberán tener acceso restringido.

SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones identificará e implementará un adecuado proceso de cambio, actualización y soporte, en los que se incluyan tópicos como la documentación, el entrenamiento y preparación procedimental para usuarios, personal de soporte y administradores de los aplicativos.

GESTIÓN DE LAS VULNERABILIDADES Y/O ERRORES TÉCNICOS

- El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones identificará, recomendará e implementará la adecuada gestión de errores o vulnerabilidades, que le permita tomar medidas sistemáticas y cíclicas para mantener la aplicación o aplicaciones en un adecuado nivel de actualización tanto en parches, como en versiones del sistema.


2.9. Política de Gestión de Incidentes de Seguridad de la Información

OBJETIVO

Asegurar que los eventos y debilidades de seguridad de la información asociados con los sistemas de información se comunican de una manera que permita que se tomen acciones correctivas oportunas y responder a los incidentes en tiempo y forma apropiada para recuperar la actividad de la Entidad.

GESTIÓN DE LOS INCIDENTES Y LAS MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN

- La Entidad debe establecer un procedimiento formal para el reporte de eventos de Seguridad de la Información. Este procedimiento debe contar con los niveles de escalamiento pertinentes.

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 37 de 57

- Todos los funcionarios, contratistas, proveedores y/o terceros de la Entidad deben tener conciencia sobre los procedimientos de reporte de los diferentes tipos de eventos y las debilidades que puedan tener impacto en la seguridad de los activos de información de los que hacen uso. Se debe contar con un punto único de contacto y cada funcionario debe cumplir con el reporte de los eventos tan pronto le sea posible. El Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones debe saber clasificar el incidente como de seguridad y seguir el respectivo procedimiento.
- La Entidad debe incluir en la inducción o sensibilización sobre seguridad de la información, temas sobre cómo identificar y reportar incidentes de seguridad y su responsabilidad respecto a estos temas.
- La Entidad debe establecer un procedimiento formal sobre como recolectar y asegurar los rastros y la evidencia para auditoría y los demás entes de control que así lo requieran.
- Se debe elaborar un procedimiento de tratamiento de incidentes de seguridad, su documentación y el almacenamiento de evidencias de manera segura.
- Los procedimientos respecto a incidentes de seguridad de la información deben manejarse por el área de Seguridad de la Información o quien haga sus veces.


2.10. Política de Gestión de la Continuidad Tecnológica

OBJETIVO

Reaccionar a la interrupción de los sistemas críticos de la Entidad procurando su funcionamiento ante la ocurrencia de un evento que afecte la continuidad de los servicios tecnológicos que soportan la operación.

ASPECTOS DE LA GESTIÓN DE CONTINUIDAD TECNOLÓGICA

- La Entidad deberá realizar todas las definiciones del proceso de gestión de la continuidad del negocio, su marco de gobierno y los lineamientos tendientes a reducir al mínimo la materialización de un riesgo de no continuidad en los procesos críticos.
- La base para el desarrollo del proceso de gestión de la continuidad tecnológica ante la ocurrencia de un desastre (DRP), es el análisis de impacto al negocio BIA (Business Impact Analysis). En este análisis se debe definir el nivel de criticidad de los diferentes procesos y aplicaciones que los soportan, considerando

	Sistema de Gestión Integral -SGI- Resolución	Código: F-GIC-26
		Versión: 02
		Página 38 de 57

la cantidad de información que el proceso puede perder (RPO) y el tiempo que tardaría nuevamente en estar operativo (RTO) el proceso o aplicación luego de la ocurrencia de un desastre.

- Se deben tener documentados y en constante actualización los planes de recuperación (movilización y retorno) de las aplicaciones críticas de la Entidad. Adicionalmente se debe cumplir con el calendario anual de pruebas, incluyendo como mínimo una prueba unitaria (prueba en un ambiente controlado no productivo) y una prueba de operación real en el ambiente de DRP.
- Se debe familiarizar a los funcionarios que tienen roles o funciones dentro del DRP, en las características del proceso y las responsabilidades de su rol.