DISEÑO DE UN PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA CAMPAÑAS ELECTORALES CON PRESUPUESTO AJUSTADO

TRABAJO DE GRADO

ANDRÉS FELIPE ROMERO MURIEL

Código

0121160556

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

DISEÑO DE UN PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA CAMPAÑAS ELECTORALES CON PRESUPUESTO AJUSTADO

TRABAJO DE GRADO

ANDRÉS FELIPE ROMERO MURIEL

Código

0121160556

Asesor

ALEJANDRO CASTIBLANCO CARO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Bogotá D.C., 02 de junio de 2017

AGRADECIMIENTOS

A mi esposa, madre y familia quienes con su confianza y esfuerzo me permitieron emprender este nuevo rumbo encaminado hacia el enfoque profesional de mis deseos.

A los profesores y personas que comparten su tiempo, conocimiento y experiencia alimentando las necesidades de crecimiento profesional y humano.

A la Universidad Politécnico Grancolombiano por apostarle a los nuevos modelos pedagógicos que a través de la apropiación de las nuevas tecnologías generan inclusión social alineándose con las metas actuales enfocadas en la disminución de brechas digitales como foco para el desarrollo.

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

INTRODUCCIÓN

En la actualidad el gran avance de la tecnología ha tenido un gran impacto en todos los frentes permitiendo que en todos los campos se agilicen y perfeccionen tareas mejorando la calidad de procesos, productos y servicios; por tal motivo ha sido muy bien recibida por todas la personas, organizaciones y grupos, ubicando a la humanidad en un escenario de globalización digital que facilita el acceso e intercambio de información. Estas mismas ventajas que ha traído también ha puesto en manifiesto nuevos retos para protegerla dado que se ha convertido en un activo primordial el cual puede ser aprovechado con fines adversos; esto ha dado pie al fortalecimiento de modelos y técnicas enfocados en la seguridad de la información y su aplicación en espacios donde anteriormente no era indispensable, haciendo necesario que los profesionales en esta área identifiquen escenarios donde la seguridad de la información esté ausente o no se aplique de manera adecuada con el fin de concientizar a los actores relacionados de la necesidad de su implementación como también de adaptar modelos y técnicas a estos nuevos ambientes para así reducir los riegos a los que están expuestos.

1. RESUMEN EJECUTIVO

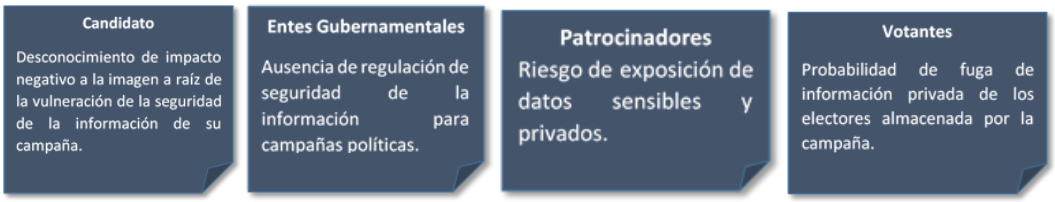
Se describe de manera concisa la información referente al anteproyecto planteado y los resultados obtenidos que justifican la elaboración del presente proyecto.

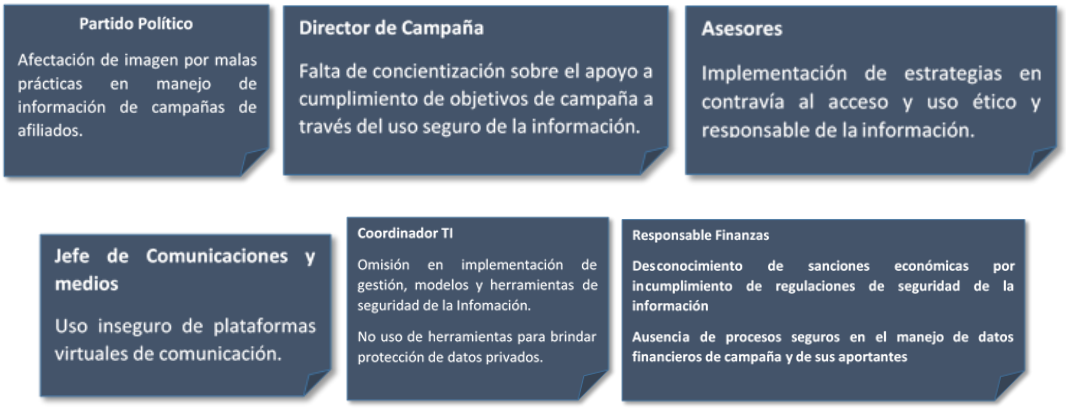
El objeto de estudio es el entorno de la seguridad de la información en campañas políticas que se plantea debido a las condiciones actuales donde la información juega un papel fundamental lo cual se ha venido evidenciando como se apreció en las elecciones presidenciales en Colombia en el año 2014 donde se infiltraron las comunicaciones del grupo negociador de paz del gobierno en la habana para desprestigiar la campaña de reelección, a su vez, se infiltro información confidencial de la campaña opositora publicando un video de su candidato reunido con el supuesto hacker que realizaba las interceptaciones como describe El Espectador (2016).

También se presentan casos similares a nivel internacional como asevera Pardo (2016) en las elecciones presidenciales de Estados Unidos donde se filtraron los correos de la campaña de la candidata por el partido demócrata Hilary Clinton lo cual pudo haber afectado su imagen y su nivel de votación, esta situación saca a flote nuevos riesgos ya que se plantea que el posible actor responsable de la divulgación fue Rusia generando una nueva amenaza ya que debido a incidentes de seguridad de la información en campañas electorales se pone en riesgo la seguridad nacional.

La evaluación enfocada en validar la necesidad de elaboración del proyecto en el campo propuesto por el planteamiento del problema se desarrolló a través de un análisis partiendo del problema de *ausencia o malas prácticas en seguridad de la información en campañas electorales* primero identificando los actores relevantes para formular las causas por los que cada uno considera se genera esta situación y los cuales se describen en la figura 1.

Figura 1. Mapa de Actores y Causas

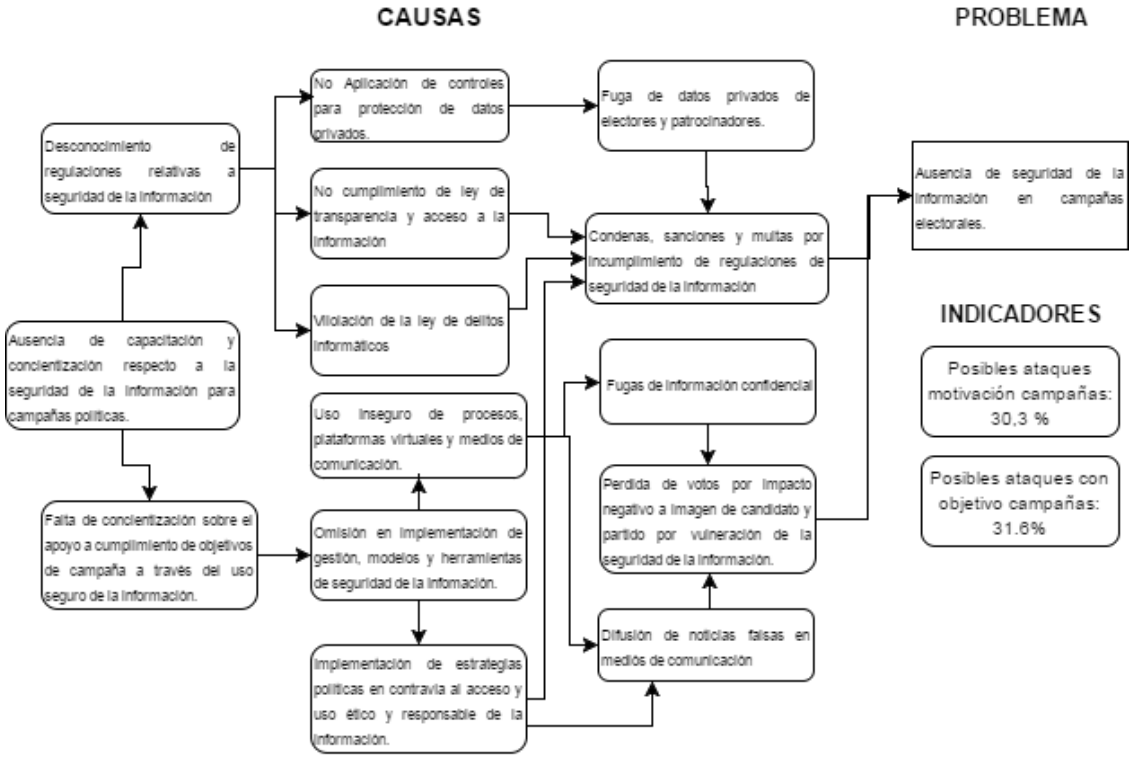




Fuente: Propia

Un resumen del escenario para proporcionar un panorama más claro a través de las causas que llevan al problema es ilustrado en la figura 2.

Figura 2. Flujograma Explicativo



Fuente: Propia

Habiendo realizado el análisis de todos los factores involucrados en este escenario como actores, causas, problema e indicadores se identifica como opción para emprender el problema la selección de controles de mitigación de riesgos de seguridad de la información enfocados al ámbito administrativo como la capacitación de usuarios, comunicación de regulaciones, formulación de procesos, guías y políticas, debido a su impacto positivo sobre la seguridad de la información

y a que se pueden ajustar para su implementación en poco tiempo y estaría al alcance de la mayoría de campañas sin discriminar por su capital económico, pero sin dejar a un lado la implementación de tecnología pero aprovechando herramientas gratuitas o de bajo coste las cuales pueden ser muy útiles, como también el uso de dispositivos económicos, con una implementación justificada pero que sea de un uso simple ya que de lo contrario se estaría obligando a la campaña a contratar expertos para administrarlos, es acá donde el especialista en seguridad es clave ya que puede aportar todo lo que involucra capacitación y paralelamente basado en sus conocimientos y experiencias puede guiar a la campaña para la aplicación de las herramientas adecuadas que proporcionen seguridad pero que no represente un gasto que perjudique el capital necesario, el cual es muy reducido en cuanto a tiempo, dinero y personal, para la obtención de su meta la cual es alcanzar el mayor número de votos o de visibilidad posible.

Con toda la información resultante se plantea como solución al problema el diseño de un plan de tratamiento de riesgos de seguridad de la información que se pueda ajustar a la mayoría de campañas electorales por lo que los posibles controles a seleccionar deben tener un mayor enfoque administrativo, aquellos tecnológicos deben ser libres o de bajo costo para cumplir con las condiciones especiales del entorno electoral; para diseñar el plan de tratamiento se aplicarán los pasos propuestos por los modelos de gestión de riesgos de seguridad de la información para análisis de contexto, identificación de activos, vulnerabilidades y amenazas, estructuración y cálculo de riesgos, con la finalidad de que el plan este alineado en reducir los riesgos que puedan afectar los activos críticos y por ende los objetivos principales de una campaña política.

Para cumplir con esta propuesta se fijan unos objetivos alcanzables y medibles al proyecto teniendo como objetivo general:

- Diseñar un plan de tratamiento de riesgos de seguridad de la información que pueda ser usado como referencia para implementar medidas de mitigación de riesgos en los procesos de planeación y ejecución de campañas políticas de presupuesto ajustado en Colombia.

Para cumplir con este objetivo general se especifican aquellos objetivos necesarios para dar forma a todo el proyecto

- Describir la metodología propuesta que describa los pasos llevados a cabo para realizar el análisis de riesgos.

- Realizar y documentar el análisis de contexto para identificar los activos de información críticos inmersos en el escenario de las campañas electorales.

- Identificar los riesgos de seguridad de la información asociados a los activos y realizar un análisis y evaluación del riesgo a través de la metodología enunciada en el objetivo anterior para elaborar un registro de riesgos con los resultados obtenidos.

- Elaborar un plan de tratamiento de riesgos de la seguridad de la información donde se propongan los controles necesarios para mitigar los riesgos listados en el registro de riesgos.

Con los objetivos definidos es posible limitar el alcance de la propuesta la cual se enfoca a las campañas electorales en Colombia que produzcan, procesen, almacenen y transmitan información; abarca el diseño de un plan de tratamiento de riesgos de seguridad de la información a través de un proceso sistemático realizando estudio de contexto, identificación de activos, análisis y evaluación del riesgo y finalmente con la propuesta del plan de tratamiento de riesgos, esto con el fin de que los controles propuestos estén alineados con los objetivos de una campaña teniendo en cuenta que las contramedidas elegidas deben ser de costos moderados y su implementación no debe ser compleja dado que las condiciones del escenario cuenta con recursos económicos, temporales y humanos limitados; por lo tanto con los objetivos propuestos se desea obtener productos documentados como lo son el análisis de contexto, metodología del análisis de riesgos, el registro de riesgos y finalmente el objetivo del proyecto que es la propuesta del plan de tratamiento de riesgos con lo que se busca generar un documento de referencia para asegurar la información en las campañas electorales.

El proyecto no contempla la implementación de los controles seleccionados dado que los factores temporales de las campañas como temporadas electorales y tiempos de ejecución no coinciden con el periodo establecido para la realización de este proyecto.

2. JUSTIFICACIÓN

Con la masificación de las tecnologías de comunicación han surgido nuevos riesgos que han afectado el entorno político como lo son las fugas de información confidencial y privada como se ilustra en El Espectador (2016) y Pardo (2016) y la distribución de noticias falsas, como afirma Franco (2017) con el objetivo de influenciar a los electores con mentiras tornándose las redes sociales en una herramienta fundamental como se observa desde el 2015 y se testifica en ABC (2015) donde el 40% de usuarios de Facebook lo usa como fuente principal de noticias, sin dejar a un lado los hechos que acontecieron en las elecciones presidenciales del año 2014 en Colombia donde uno de los partidos contrato un hacker para filtrar información confidencial del gobierno; por lo anterior surge la necesidad de observar este entorno desde un punto de vista de seguridad de la información debido a la falta de regulación y estudios dirigidos específicamente a este campo, necesidad que dejan ver gran cantidad de artículos como por ejemplo Cordero (2016) donde se puede apreciar el hueco existente en cuanto al aseguramiento de datos de las campañas y sumado a esto están las estadísticas de ciber ataques del año 2017 presentadas por Passeri (2017) de donde se extraen los datos de las tablas 1 y 2 y se deduce de estos valores que hay una posibilidad de que las campañas electorales estén dentro de la motivación para un 30,3% de ataques y sería un posible objetivo para un 31.6 % valores que salen de relacionar el ciber espionaje y el hacktivismo en la tabla 1 y gobierno y organizaciones de la tabla 2 ya que las campañas políticas están inmersas en esas categorías.

Tabla 1. Motivación Ciberataques 2017

Motivación detrás de los ataques	Porcentaje
Ciber Crimen	64.5%
Ciber Espionaje	22.4%
Hacktivismo	7.9%
Guerra Cibernética	5.3%

Tabla 2. Objetivos Ciberataques 2017

Distribución de Objetivos	Porcentaje
Industria	28.9%
Gobierno	25%
>1	9.2%
Individuos	7.9%
Organizaciones	6.6%

Con el fin de ver el comportamiento en cuanto a protección de datos se analizan los valores presentados en Duran (2016) que muestra las estadísticas de sanciones en Colombia evidenciando la seriedad con que se debe aplicar la norma de protección de datos personales ya que entre el 2012 y 2015 se han aplicado un total de $9.073 millones en multas, el valor de estas sanciones podría dejar sin presupuesto e inactiva una campaña política fácilmente o podría suspender el proceso de registro de votantes el cual es fundamental para cumplir con las estrategias de comunicación.

Como resultado de evaluación de los indicadores de ciber ataques y las crecientes multas por violación a la ley de habeas data se infiere que hay un alto grado de probabilidad de que una campaña política pueda ser objeto de un ataque o incurran en una violación regulatoria debido a malas prácticas por lo que se identifica la necesidad de la realización del proyecto.

3. MARCO TEÓRICO

3.1 Campañas Políticas

En las democracias una campaña política es el proceso realizado por un partido político o un grupo de individuos para influir, reforzar o modificar preferencias de ciudadanos aptos para ejercer su derecho al voto.

Con el fin de aclarar los conceptos asociados a las campañas electorales en Colombia se definen a continuación los términos más relativos al proyecto extrayendo las definiciones tal como se presentan en la web de la Registraduría ya que estos conceptos son los que se definen oficialmente en el país debido a que la Organización Electoral, la cual está conformada por el Consejo Nacional Electoral y la Registraduría Nacional del Estado Civil, es la responsable de garantizar la legitimad, transparencia y efectividad del proceso electoral del país.

3.1.1 Elecciones

Una elección es el medio a través del cual se hacen efectivos los derechos políticos de los ciudadanos de elegir y ser elegidos. Es el proceso de toma de decisiones democrático en el que los ciudadanos votan por una opción ante una pregunta de carácter relevante, o por los candidatos o partidos políticos preferidos, para gobernantes (elecciones uninominales) y miembros de corporaciones públicas (elecciones plurinominales), siendo sus representantes en el gobierno.

En Colombia actualmente mediante el proceso de votación se eligen: Presidente y vicepresidente, Congreso (Senado y Cámara), Parlamento Andino, diputados, gobernadores, concejales, alcaldes, ediles.

3.1.2 Candidato

Persona que se postula con el aval de un partido o movimiento político con personería jurídica, o con el respaldo de un grupo significativo de ciudadanos, para ser elegida en un cargo público de elección popular.

3.1.3 Inscripción De Candidatura

Acto voluntario con el que el candidato adquiere un compromiso político y jurídico con la sociedad el cual debe ser realizado por ciudadanos que aspiren a participar como candidatos en elecciones de Presidente, Congreso, Gobernación, Alcaldía, Asamblea, Consejo, etc., que deberán inscribir sus nombres en las condiciones y términos establecidos por la Ley.

3.1.4 Modos de Inscripción

Un candidato se puede inscribir con el aval de un partido o movimiento político con personería jurídica reconocida por el Consejo Nacional Electoral o con el apoyo de un grupo significativo de ciudadanos, caso en el que se requiere aportar el total de firmas correspondiente y la póliza de seriedad.

3.1.4.1 Inscripción por Aval

Los partidos o movimientos políticos con personería jurídica reconocida por el Consejo Nacional Electoral otorgan el aval a un ciudadano que los representará en una elección popular. El aval es otorgado por el representante legal del partido o movimiento político o por quién él delegue de manera expresa. El aval debe contener la corporación y cargo que se avala, la identificación del avalado o avalados, el período constitucional que cubre, la relación de todos los integrantes de la lista de acuerdo con el número de curules a proveer en la respectiva circunscripción según sea el caso, o la corporación a que aspire, la modalidad de voto y la ciudad en la que se inscribe.

3.1.4.2 Inscripción por Firmas

Los candidatos de los grupos significativos de ciudadanos se deben inscribir a través de un comité integrado por tres ciudadanos, quienes se deben registrar ante la correspondiente autoridad electoral. De acuerdo con el Artículo 28 de la Ley 1475 de 2011 la inscripción del Comité se debe hacer “cuando menos un mes antes de la fecha de cierre de la respectiva inscripción y, en todo caso, antes del inicio de la recolección de firmas de apoyo a la candidatura o lista. Los nombres de los integrantes del Comité, así como la de los candidatos que postulen, deberán figurar en el formulario de recolección de las firmas de apoyo”.

3.2 Seguridad de la información

Introducción a conceptos generales involucrados en el tema de seguridad de la información con la finalidad de que en los capítulos posteriores se tenga claridad sobre los términos usados.

La seguridad de la información se refiere a la protección de los datos desde una perspectiva transversal lo que significa que no se adopta solamente desde un punto de vista técnico sino que también se abarca desde el ámbito administrativo con controles enfocados en capacitación y políticas, entre otros, siempre destinados a aportar medidas alineadas con los objetivos del negocio; el objetivo de la seguridad de la información teniendo en cuenta lo anterior es velar por la confidencialidad, integridad y disponibilidad de los datos, entendiéndose por confidencialidad como el acceso a la información solo por quien tenga permiso para ello, por integridad como la modificación por quien esté autorizado y no sea objeto de alteración y

disponibilidad como el acceso a los datos por los usuarios habilitados cuando sea requerido.

3.2.1 Estándares de Seguridad de la Información

Entendiéndose como estándar el conjunto de pasos y reglas a seguir que son necesarios para fomentar el funcionamiento homogéneo de un sistema, lo cual para el entorno de seguridad de la información significaría el conjunto de reglas para implementar seguridad en diferentes ámbitos pero con resultados similares en cuanto a su efectividad; así las cosas, hay gran variedad de estándares y modelos que pueden ser adoptados o ajustados dependiendo del sector, tamaño y enfoque donde se desee implementar seguridad, entre los más destacados esta ISO 27001 el cual es certificable, el NIST proveniente de Estados Unidos y que tiene un enfoque más técnico, MAGERIT estándar español que sobresale en cuanto a la clasificación de activos de información, Octave y COBIT que está enfocado gobernabilidad y en la tecnología como soporte para alcanzar los objetivos del negocio; para dar un enfoque que esté relacionado específicamente con lo que se plantea en el proyecto se da una breve introducción del estándar ISO 27001.

3.2.1.1 ISO 27001

Es un estándar internacional formulado por la Organización Internacional de Normalización (ISO) y describe una metodología de implementación y gestión de seguridad de la información en cualquier tipo de organización desde una perspectiva sistemática, organizada y continua apoyándose en la metodología PHVA (Planear, Hacer, Verificar y Actuar).

La metodología PHVA consta de 4 fases y es la que convierte la gestión de seguridad de la información en un proceso continuo, el estándar proporciona las tareas que se deben realizar en cada una de las faces iniciando por la fase de planeación donde se enuncian las actividades como definición de objetivos y alcance, análisis de contexto organizacional y partes interesadas, identificación y valoración del riesgo, en la fase hacer están las actividades que llevan el plan al mundo real y su objetivo es la implementación de los controles seleccionados, por último están las fases verificar y actuar donde se establecen actividades para medir indicadores de seguridad, auditorías, análisis de brecha el cual proporciona la diferencia entre los estados de donde se desea estar y donde se encuentra realmente la seguridad y otras técnicas que permiten aclarar el panorama con el propósito de tomar medidas de mejora y correctivas para dar un fortalecimiento continua al proceso iniciando nuevamente desde la fase 1.

Para certificarse con este estándar la organización ya debe haber puesto en marcha un tiempo considerable el sistema de gestión de la seguridad de la información para que la entidad certificadora a través de una auditoría pueda verificar si se realizaron todas las tareas, registros y documentación requeridos como también se evalúa si el sistema está realmente funcionando.

3.2.2 Gestión de Riesgos

Para la definición de este punto es necesario aclarar previamente de una manera breve algunos términos iniciando por vulnerabilidad la cual se refiere a una debilidad presente en un activo o sistema de información, amenaza como el agente que puede aprovecharse de la vulnerabilidad, impacto es la afectación y consecuencias que se presentarían si la amenaza se hace efectiva, probabilidad es el nivel de posibilidad que existe de que lo anterior suceda y el riesgo es el nivel de exposición de un activo que de hacerse efectiva una amenaza ocasionaría un efecto adverso.

La gestión de riesgos es la estrategia que se lleva a cabo para identificar activos de información, vulnerabilidades y amenazas, para así evaluar el impacto y la probabilidad permitiendo calcular el valor del riesgo ya sea de manera cualitativa o cuantitativa, lo cual proporciona la información necesaria para realizar el tratamiento del riesgo ya sea mitigándolo a través de controles, aceptándolo o trasladándolo, el resultado de la gestión de riesgos es su tratamiento; existen varios modelos que proporcionan guía para la implementación de este proceso como ISO 27005, Nist 800-30, Octave, entre otros.

3.3 Regulaciones

3.3.1 Ley de Protección de Datos Personales

La ley 1581 de 2012 la cual tiene como objetivo regular el tratamiento de datos personales en Colombia es muy importante tenerla en cuenta en el contexto de este proyecto ya que el registro de votantes tanto como para recolección de firmas para la participación en una contienda electoral de un candidato independiente como también para el desarrollo de la campaña como soporte a la estrategia de comunicación que permite tener una línea directa de comunicación con los votantes registrados lo cual causa que las campañas almacenen y procesen datos que están regidos por esta ley.

3.3.1.1 Clases de Datos

Se debe tener presente la categorización de los datos para conocer cuáles son los que son objeto de la norma.

3.3.1.1.2 Datos Personales

Elementos que en conjunto sirven para identificar de manera única a una persona, entre los datos que encajan en esta categoría se tiene correo electrónico, teléfono, dirección, fotos, entre otros.

3.3.1.1.3 Información Pública

Es aquella que por su carácter público no tiene reserva y hacen parte de esta categoría datos como el número de identificación, antecedentes, estado civil, entre otros.

3.3.1.1.4 Información semipública

Son los datos personales que pueden ser accedidos por personas o entidades con una autorización de ingreso a la base de datos que los contiene, hacen parte de esta categoría los datos financieros y crediticios.

3.3.1.1.5 Información Privada

Información que no es pública y solo puede ser accedida por el estado o terceros mediante orden judicial o administrativa como ejemplo de este tipo de datos se tiene información financiera y contable, clínica y correspondencia privada.

3.3.1.1.6 Información Reservada

Es aquella que hace parte del espacio íntimo del individuo como preferencias sexuales, ideología política, creencias religiosas, gustos, entre otras; la única manera de acceder a esta información así se cuente con orden judicial es que el titular de su autorización.

3.3.1.2 Responsabilidades y Sanciones

Los aspectos más importantes que se deben tener en cuenta acerca de las responsabilidades asumidas por una persona o entidad que cuenta con información que sea de carácter reservado, privado o semiprivado son que la recolección de datos debe estar autorizada por su titular, dicha autorización debe ser registrada y evidenciable, en el momento de la recolección de los datos el titular debe ser informado de la finalidad de su recolección y tratamiento, el manejo que se le da a dicha información debe ser acorde con la finalidad para la cual fue recolectada, se debe disponer de un procedimiento para atender solicitudes de titulares en cuanto a suministrar, modificar o eliminar la información almacenada cumpliendo con los plazos definidos por la ley que generalmente van desde diez a veinte días hábiles dependiendo del caso y se deben disponer de medidas técnicas y administrativas para proporcionar seguridad a los datos en cuanto a su confidencialidad, integridad y disponibilidad.

Los aspectos relacionados con el no cumplimiento de estas regulaciones pueden desencadenar sanciones como:

i) Multas hasta por dos mil salarios mínimos mensuales legales vigentes.

ii) Suspensión de actividades relacionadas con el tratamiento de datos hasta por seis meses.
iii) Cierre temporal de operaciones de tratamiento de datos personales a causa de no correcciones durante suspensión.
iv) Cierre definitivo de operación de tratamiento de datos.

Las sanciones aquí dispuestas pueden afectar de una manera importante al desarrollo de una campaña en términos económicos y operacionales; la graduación de las sanciones depende de la dimensión del daño en que se incurra, beneficios obtenidos, reincidencia, desacato a entes reguladores, resistencia a investigaciones o reconocimiento por parte del infractor antes de ser sancionado; para ampliación de información remitirse a la Ley Estatutaria No. 1581 documento fuente de esta definición.

3.3.2 Ley de transparencia

Es la ley 1712 de 2014 denominada Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, la cual para el escenario propuesto se evalúa en el aspecto concreto de partidos políticos en procesos electorales, la ley en este entorno tiene como objetivo promover la transparencia y el acceso a la información pública que los grupos participantes almacenen y procesen con el fin de fomentar la organización y el control interno y a su vez de rendir cuentas respecto a contabilidad y financiación.

La información mínima que debe ser presentada por parte de las campañas son los estatutos partidistas, las plataformas programáticas, los presupuestos anuales, los informes de campañas y las declaraciones de patrimonio, ingresos y gastos, entre otros; hay excepciones de información que no debe ser divulgada como la clasificada debido a que está cobijada por la ley de habeas data la cual solo se publicara por solicitud de información con fines estadísticos (fecha de afiliación, sexo, edad, ciudad y país de residencia, entre otros), suprimiendo los datos personales; también hace parte de estas excepciones información reservada la cual puede tener un efecto adverso hacia intereses públicos.

El no cumplimento de las disposiciones de la ley de trasparencia por parte de los grupos político acarrearía sanciones como:

i) La suspensión o privación de la financiación estatal y/o de los espacios otorgados en los medios de comunicación social que hacen uso del espectro electromagnético.
ii) La suspensión de su personería jurídica, hasta por cuatro años.
iii) Prisión de dos a ocho años si se incurre en ocultamiento, destrucción y modificación de información pública que este bajo proceso de solicitud.

Los partidos políticos también están en obligación de publicar información respecto a los candidatos avalados con el objetivo de dar garantía a la ciudadanía de que cumplen con los requerimientos para ejercer cargos públicos.

La herramienta que se pone a disposición de los partidos, grupos y candidatos para rendir cuentas sobre financiación al estado es la aplicación de “Cuentas Claras” del Consejo Nacional Electoral la cual contiene un módulo para ser consultada por el público en general y otro para los grupos y candidatos declarantes alimentándola con datos financieros.

Con la intención de no extenderse sobremanera y si se desea profundizar sobre la ley de trasparencia en campañas políticas se puede revisar el documento base de esta explicación, Navas (2015), donde se identifica de manera detallada todos los requisitos para dar un debido cumplimiento a esta regulación.

3.3.3 Ley de Delitos Informáticos

La ley 1273 que regula y sanciona los atentados contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, se presenta en este apartado debido a que en la actualidad las campañas políticas han sido afectadas por acciones que se sancionan en esta ley por lo cual debe ser conocida para tener un entendimiento de los riesgos de adoptar acciones no éticas en este sentido en procesos electorales o para saber qué derechos se tienen cuando se es víctima; se presentan los delitos que se relacionan más al entorno del proyecto extraídos de la Ley No. 1273 (2009) la cual también puede ser consultada para ampliar el tema.

3.3.3.1 Acceso abusivo a un sistema informático

Contempla el acceso sin autorización a un sistema a través de cualquier método ya sea por técnicas de hacking o suplantando un usuario, también tiene responsabilidad un usuario legítimo que cede de manera voluntaria su usuario para que otro no autorizado ingrese al sistema, en este artículo no se tiene en cuenta la finalidad por la cual se ingresó o las acciones que se realizan una vez este adentro lo que significa que solo el hecho de ingresar ya es delito; las sanciones son 48 a 96 meses de prisión y multa de 100 a 1.000 smmlv (Salarios mínimos mensuales legales vigentes).

3.3.3.2 Obstaculización ilegitima de sistema informático

Hace referencia a que a raíz de alguna acción se cause una no operatividad de un sistema o red de comunicación afectando su disponibilidad, un ejemplo muy común en la actualidad es un ataque de denegación de servicios; las sanciones son 48 a 96 meses de prisión y multa de 100 a 1.000 smmlv.

3.3.3.3 Intercepción de datos informáticos

Delito consecuencia de interceptar una comunicación sin orden judicial ya sea en el origen, destino, interior o a través de ondas electromagnéticas y tiene una pena de 36 a 72 meses de prisión.

3.3.3.4 Daño Informático

Causado por destruir, borrar, deteriorar, alterar o suprimir datos, sistemas de información sus partes o componentes; este artículo no completa si la acción que desencadeno el delito fue con o sin intención por lo que un error humano podría ser condenado por igual; las sanciones son 48 a 96 meses de prisión y multa de 100 a 1.000 smmlv.

4. METODOLOGÍA

En este apartado se describen los pasos que se aplican para el desarrollo del plan de tratamiento de riesgos identificando estándares y metodologías aplicadas para dicho fin.

El procedimiento que se lleva a cabo para el levantamiento de información necesaria para realizar el análisis de riesgos se basa en los pasos definidos por el estándar ISO 27001, por tal motivo y por las condiciones temporales y del modelo de organización que hacen parte de este escenario se realiza solo la fase de planeación y no se incluyen todos los pasos de la norma ya que se adaptan aquellos requeridos para las necesidades del proyecto.

Para cumplir con los objetivos propuestos se estudia la norma ISO 27001 con el fin de identificar los pasos que puedan ser aplicados en el escenario y aportar información importante a la resolución del proyecto, con estos pasos identificados como esenciales se tiene el estudio de contexto, identificación de activos, análisis de amenazas y vulnerabilidades, estructuración de riesgos y finalmente la valoración del riesgo.

Para llevar a cabo el análisis de contexto se lleva a cabo la lectura de documentos y artículos especializados en el tema de planeación y estrategia de campañas electorales como también se busca información a través de entrevistas a expertos en el tema, con esto es posible darle forma a este escenario a través de la propuesta de una estructura organizacional y mapa de procesos para tener un conocimiento más profundo y consecutivamente identificar los activos críticos para el escenario que tengan un impacto en los procesos fundamentales para el óptimo desarrollo de este escenario.

Con los activos identificados se procede a analizar los procesos y contenedores por donde este fluye para así encontrar las amenazas y vulnerabilidades que lo aquejan y así estructurar los riesgos asociados a estos activos de tal manera que estén alineados con los objetivos de las campañas para que al momento de ser conocido por personal con una posición de alto nivel en una campaña electoral vea más que justificable la aplicación de un control para brindar protección contra ese riesgo.

Con los datos asociados al riesgo como amenazas y vulnerabilidades y la información sobre el activo se adapta una metodología para valorar el activo a través del impacto que cause su ausencia a la organización, de igual manera se identifica estudian metodologías de cálculo de probabilidad para seleccionar aquella o aquellas que más se adapten a este ámbito y aplicarla, ya con esto se tienen los datos necesarios para calcular el nivel de riesgo y su criticidad para así ya tener el camino libre y proponer los controles necesarios para mitigar dichos riesgos siempre teniendo en cuenta las bases del proyecto que apuntan a seleccionar medidas enfocadas en lo administrativo o herramientas libres o de costo moderado ya que

este fue el resultado y hacia donde apunto el análisis realizado en el anteproyecto; ya teniendo claros los controles a usar se procede a formularlos y estructurarlos con lo que finalmente es posible proponer el plan de tratamiento de riesgos; en todo el proceso aquí descrito se obtienen cuatro productos iniciando por la propuesta de la metodología a aplicar de análisis de riesgo, el análisis del contexto del entorno de las campañas políticas y sus activos críticos, el registro de riesgos y finalmente el plan de tratamiento de riesgos con la descripción detallada de los controles que brindan soporte a este plan..

Por lo anterior descrito se da una ampliación a la información sobre esta metodología responsable de la resolución del proyecto en el Anexo 1 relativo a la metodología de análisis de riesgo que es el primer producto de este proyecto y es afín a lo descrito en este capítulo pero donde sea entra a describir este proceso de una manera más profunda y precisa planteando así un modelo para ser usado en el entorno electoral ya definiendo los parámetros con los que se podrá realizar los cálculos para obtener un resultado objetivo.

5. RESULTADOS Y DISCUCIÓN

En este apartado se describen los resultados obtenidos de la aplicación del trabajo de grado y se describe en relación a los productos obtenidos los cuales fueron propuestos previamente y dan cumplimiento a los objetivos establecidos para este proyecto.

5.1 Metodología del Análisis de Riesgos

Con la aplicación del primer producto del proyecto, relativo a la metodología de análisis de riesgos descrita en el anexo 1 y la cual fue la columna vertebral para el desarrollo de todo el procedimiento lo que permitió obtener de una manera sistemática y objetiva los otros productos esperados de este trabajo de grado aportando información primordial desde el entendimiento del ámbito de las campañas electorales hasta la identificación y valoración de los riesgos que afectan los activos de información involucrados y que juegan un papel importante permitiendo medir la criticidad de estos para proponer los contramedidas responsables de reducirlos riesgos, por lo tanto la formulación de la metodología de una forma clara, objetiva y emparejada con los objetivos estratégicos del escenario fue la que permitió obtener los otros productos de una manera óptima y cumplir con el objetivo específico de *"describir la metodología propuesta que describa los pasos llevados a cabo para realizar el análisis de riesgos".*

5.2 Análisis de Contexto

Este documento es el resultado del estudio y análisis de todo el contexto de las campañas electorales a través del estudio de artículos, documentos y opinión de expertos en el tema con lo que se logró desglosar los objetivos estratégicos, realizar un mapa de procesos y describir la estructura organizacional con los roles y funciones que contiene; el levantamiento de esta información fue crucial para obtener los activos críticos inmersos en este entorno y mirarlos desde una perspectiva donde se tiene en cuenta los procesos y los actores involucrados para poder identificar amenazas y vulnerabilidades de una manera objetiva y siempre alineados con los objetivos de este escenario.

El registro de lo anterior descrito es el segundo producto que aporta el proyecto y cumple con el objetivo específico *"Realizar y documentar el análisis de contexto para identificar los activos de información críticos inmersos en el escenario de las campañas electorales*", este documento puede ser consultado en la sección de anexos del presente documento específicamente en el anexo 2 y contiene la

descripción de los objetivos de una campaña, estructura organizacional, procesos, infraestructura y los activos de información resultantes.

5.3 Registro de Riesgos

Este producto se refiere al listado de los riesgos identificados con su valor de impacto, probabilidad y el nivel de riesgo; este registro se obtiene gracias al análisis de contexto y al seguimiento de la metodología propuesta de análisis de riesgos lo que permitió identificar de una manera clara las amenazas y vulnerabilidades de los activos y sus contenedores, estructurar los riesgos siempre teniendo en cuenta su afectación en cuanto al alcance de los objetivos esenciales de una campaña electoral, calcular con un método cualitativo el impacto, la probabilidad y el nivel de riesgo resultante con lo que se pudo categorizarlos respecto a su criticidad y así cumplir con el objetivo específico de *"Identificar los riesgos de seguridad de la información asociados a los activos y realizar un análisis y evaluación del riesgo a través de la metodología enunciada en el objetivo anterior para elaborar un registro de riesgos con los resultados obtenidos"* y dejar las puertas abiertas para el estudio de selección de controles adecuados responsables de mitigarlos.

El producto específico relativo al registro de riesgos se puede consultar en el Anexo 3 en la tabla 12, pero en este anexo también se puede revisar todo el procedimiento enunciado en este punto el cual contiene el análisis de riesgos con la identificación de amenazas, vulnerabilidades, riesgos, cálculo de impacto, probabilidad y nivel de riesgo.

5.4 Plan de Tratamiento de Riesgos

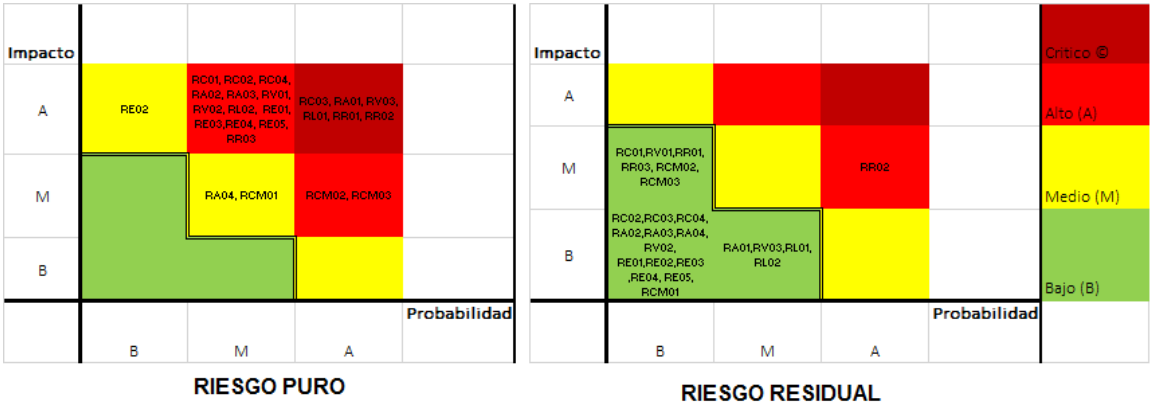
Este producto es el registro que lista los controles propuestos, el riesgo al que se aplica, responsable, plazo de implementación y recursos necesarios que da cumplimiento al objetivo específico de *"Elaborar un plan de tratamiento de riesgos de la seguridad de la información donde se propongan los controles necesarios para mitigar los riesgos listados en el registro de riesgos"*; este documento se obtiene gracias a la efectividad de los productos anteriores que permiten tener un conocimiento acertado sobre activos, amenazas, vulnerabilidades y criticidad además del resultado del análisis metodológico efectuado en el anteproyecto con lo que fue posible seleccionar los controles para disminuir el nivel de riesgo desde un enfoque administrativo o que no requiera una inversión alta en tiempo y recursos para que realmente sean implementados; este plan es el resultado de todo el proyecto y su importancia radica en que una campaña política sea capaz a través de su lectura de aplicar seguridad de la información a su funcionamiento desde su planeación lo cual se logra con su formulación clara y dirigido a un público diverso.

Este producto específico está disponible en el anexo 4 en la tabla 15, pero para su adecuada aplicación en el mundo real esta complementado por la formulación de los controles que lo respaldan y que se describen en el anexo 4 y está compuesto por las políticas de confidencialidad, email, tratamiento de datos personales, contraseñas, backup y redes sociales además de los protocolos de cifrado, comunicación estratégica no documentable y noticas falsas, estos documentos a su vez contienen las herramientas recomendadas a usar, dado el caso, para lograr su implementación; finalmente se espera que todo este paquete final relacionado con el plan de tratamiento de riesgos sea una herramienta a tener en cuenta por las campañas políticas del país para asegurar su información.

5.5 Riesgo Residual

En aras de la objetividad en cuanto al análisis de los resultados del proyecto se calcula el riesgo residual con la suposición de los controles ya implementados usando la metodología planteada, los cálculos se pueden observar en el anexo 5 correspondiente al libro de Excel donde se alojan todas las tablas desarrolladas, para este caso en especial se usaron las hojas de cálculo denominadas “Valoración Activos (2)”, “Probabilidad (2)” y “Riesgo residual”; a continuación se plasma la comparación del riesgo puro con el residual.

Figura 3. Riesgo Puro vs Residual



Como se puede observar en la figura 3 se logra llevar la mayoría de los riesgos al nivel de riesgo aceptable, esto es posible debido a que el impacto disminuye con la aplicación de controles y dado que la mayoría de veces en este caso el criterio de seguridad más importante es la confidencialidad el impacto de la filtración de un archivo con la información cifrada no tiene gran afectación; otra característica notable es que la motivación de un atacante puede disminuir solo por conocer que en la campaña se aplican estrategias para aseguramiento de la información y

también por estar al tanto de ley de delitos informáticos de la cual su socialización en estos entornos debe ser encabezada por el gobierno.

El único riesgo que no se pudo llevar a los niveles deseados es el relativo a disminución de popularidad por circulación de noticias falsas en redes sociales debido a que las herramientas disponibles en la actualidad no son suficientes por lo tanto la probabilidad sigue siendo muy alta dado que analizando objetivamente este punto se debe hacer una reeducación de todas las personas ya que pasamos de una época donde todo el material publicado escrito era fiable ya que los únicos con capacidad para producirlo eran medios bien conformados, en cambio en la actualidad cualquiera puede publicar lo que desee por lo que es necesario iniciar acciones sobre todo desde los centros educativos promoviendo conocimientos sobre cómo identificar fuentes fiables de información y la responsabilidad personal sobre lo que se publica y corresponde a los gobiernos establecer sanciones a quien evidenciablemente circule información falsa que pueda traer consecuencias negativas sobre algo; ya para las personas adultas se debe hacer campañas con este mismo fin creadas por las mimas plataformas electrónicas y el gobierno ya que se deben tomar medidas sobre este aspecto basándose en los últimos hechos donde una cantidad muy representativa de personas se basa en esta información no confiable para decidir su intención de voto desestabilizando la democracia.

6. CONCLUSIONES

En este apartado se presentan las conclusiones relativas al aspecto pedagógico y académico que dejo como resultado el desarrollo del proyecto.

6.1 La importancia de una análisis real y profundo del contexto de la organización o entorno que se desea asegurar es esencial para identificar los activos que realmente estén alineados con las necesidades del negocio, por eso es recomendable evitar la necesidad de presuponer dichos activos basándose solo en la experiencia personal sin realizar un estudio previo porque lo más seguro es que no se identifiquen todos los activos involucrados teniendo como consecuencia una brecha de seguridad.

6.2 Definir una metodología de análisis de riesgos ajustándola a les necesidades del entorno es primordial para calcular áreas de impacto que verdaderamente sean las que el escenario abarca, por lo que es necesario no solo tener en cuenta las áreas estándar de impacto como económico, reputacional y legal que son las más usadas; lo mismo se debe tener en cuenta para la probabilidad saliéndose de solo considerar el número de veces que se ha materializado ese riesgo sino también teniendo en cuenta las capacidades del atacante y la facilidad de vulnerar el activo.

6.3 Es notable la efectividad de la aplicación de contramedidas de tipo administrativo como son las políticas ya que se puede brindar con una sola aseguramiento a muchos riesgos por lo cual se consideran transversales y puede ser la primer línea de defensa pero su funcionalidad depende de su adecuada socialización capacitación y que realmente se lleve a la práctica por lo que se debe monitorear periódicamente.

6.4 El plan de tratamiento de riesgos juega un papel muy importante en cuanto a que es el transductor entre las fases de planeación y hacer propuestas en ISO 27001 con la metodología PHVA, es decir, es el encargado de llevar lo planeado que está en papel al mundo real en la organización.

6.5 Seguir una norma como la ISO 27001 proporciona organización en el desarrollo e implementación del proyecto pero no quiere decir esto que por ser aplicada se tenga una seguridad de la información efectiva, esto radica en que el estándar proporciona los pasos que se deben seguir más no describe como llevarlos a cabo en aras de la aplicabilidad para que la norma este abierta a cualquier tipo de organización, por lo tanto, cabe la posibilidad de que se cumplan todos los pasos allí propuestos pero se halla identificado erróneamente los activos críticos por una mala definición de alcance o se realice un cálculo demasiado subjetivo de la valoración del riesgo terminando en la selección de controles no funcionales o no justificados y de igual manera se lograría la certificación; he ahí la importancia de unos conocimientos sólidos en cuanto a seguridad de la información del responsable de implementar la norma.

7. BIBLIOGRAFÍA

[1] El Espectador (2016) El “hacker” y la campaña de Óscar Iván Zuluaga. Recuperado de: http://www.elespectador.com/opinion/editorial/el-hacker-y-campana-de-oscar-ivan-zuluaga-articulo-665819.

[2] Pardo, P. (2016). Caos de filtraciones sobre los emails de Hillary Clinton. El Mundo. Recuperado de: http://www.elmundo.es/internacional/2016/10/30/58163bfde2704e8e2a8b45b2.html.

[3] Franco, M. (2017). La nueva defensa de los políticos del mundo: son ‘noticias falsas’. The New York Times. Recuperado de: https://www.nytimes.com/es/2017/03/29/fake-news-noticias-falsas-donald-trump/.

[4] ABC. (2015). Facebook, principal fuente de noticias en internet. ABC Tecnología. Recuperado de: https://www.nytimes.com/es/2017/03/29/fake-news-noticias-falsas-donald-trump/.

[5] Cordero, C. (2016). Political Campaigns and Cybersecurity Risk. Lawfare. Recuperado de: https://www.lawfareblog.com/political-campaigns-and-cybersecurity-risk.

[6] Passeri, P. (2017). February 2017 Cyber Attacks Statistics. Recuperado de: http://www.hackmageddon.com.

[7] Duran, P. (2016). Violaciones al habeas data fueron de $9.037 millones. La República. Recuperado de: http://www.larepublica.co/violaciones-al-habeas-data-fueron-de-9037-millones_352846.

[8] Electoral. Registraduría Nacional del Estado Civil. Recuperado de: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf.

[9] Ley Estatutaria No. 1581. (2012). POR EL CUAL SE DICTAN DISPOSICIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES. Congreso de Colombia. Recuperado de: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf.

[10] Navas, A. (2015). Transparencia y Acceso a la Información en Partidos y Movimientos Políticos Colombianos: Responsabilidades frente a la Ley 1712 de 2014. Secretaría de Transparencia Presidencia de la República. Recuperado de:

http://www.anticorrupcion.gov.co/SiteAssets/Paginas/Publicaciones/cartilla-partidos%20politicos.pdf.

[11] Ley No. 1273. (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"· Y SE PRESERVAN INTEGRALMENTE LOS SISTEMAS QUE UTILICEN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, ENTRE OTRAS DISPOSICIONES. Congreso de Colombia. Recuperado de: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf.

[12] Norma ISO/IEC 27001. International Organization for Standardization. 2013.

[13] Norma ISO/IEC 27005. International Organization for Standardization. 2011.

[14] Machaca, A. ANÁLISIS DE RIESGOS APLICANDO LA METODOLOGÍA OWASP. OWASP. Recuperado de: https://www.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf.

[15] Cobos, P. (septiembre 2014). Roles y responsabilidades en campañas electorales. Debate 21. Recuperado de: http://debate21.es/2014/09/24/roles-y-responsabilidades-en-campanas-electorales/.

[16] Gutiérrez, C. (2013). Infraestructura y organización de la campaña. Slide Share. Recuperado de: https://es.slideshare.net/CarlosGutArg/infraestructura-y-organizacin-de-la-campaa-27381814.

[17] Katz, B. (2014). Organizing Your Political Campaign. Aristotle. Recuperado de: http://aristotle.com/blog/2014/09/organizing-your-political-campaign-how-to-assemble-your-campaign-team/.

[18] Costa, L. (1994). Manual de Marketing Político. LCB-Marketing Político. Recuperado de: www.costabonino.com/manualmp.pdf.

[19] ODCA (2006). Manual de Campaña Electoral: marketing y comunicación política. Fundación Konrad Adenauer Stiftung. Recuperado de: http://www.kas.de/wf/doc/kas_9691-1522-1-30.pdf?110413174224.

8. ANEXOS

ANEXO 1

8.1 Metodología del Análisis de Riesgos

Lo plasmado en este capítulo corresponde al producto esperado del proyecto para cumplir con el objetivo específico de *"realizar y documentar el análisis de contexto para identificar los activos de información críticos inmersos en el escenario de las campañas electorales"* y consiste en la descripción de la metodología base aplicada para realizar de manera sistemática el análisis de riesgo describiendo los pasos y parámetros que se tendrán en cuenta para la aplicación de este proceso al escenario de las contiendas electorales, partiendo por el análisis de contexto para identificación de activos críticos de información, seguido por los pasos para identificar amenazas y vulnerabilidades relativas a estos, estructuración de riesgos, cálculo de impacto y probabilidad y por último la valoración de riesgos lo cual prepara el camino para proponer los controles y elaborar el plan de tratamiento de riesgos; este producto es importante ya que permite estandarizar un método para ser aplicado en un futuro en el mismo entorno o en cualquier campaña electoral especifica e identificar y tratar nuevos riesgos que puedan generarse debido al dinamismo del escenario y las tecnologías aplicadas.

8.1.1 Contexto

Se inicia por el análisis de contexto interno y externo del sistema objeto del proyecto con el fin de definir la estructura organizacional de una campaña política, sus roles y responsabilidades, procesos, objetivos estratégicos, partes interesadas y regulaciones aplicadas, este punto es fundamental debido a que del entendimiento acertado de estos apartes se logra definir un alcance apropiado y una identificación realista de los activos de información que estén alineados con los objetivos del negocio.

8.1.2 Alcance

El paso siguiente es la definición del alcance el cual basándose en los resultados del análisis de contexto definirá los procesos y sistemas a los cuales aplicara la implementación de seguridad de la información, el acotamiento del escenario es importante porque en la práctica en algunos escenarios asegurar todos los procesos y activos involucrados es imposible porque los costos económicos, temporales y humanos se desbordarían haciéndolo inviable y podría traer como consecuencia fallas de seguridad ya que cabría la posibilidad de implementar controles para riesgos que no afecten los objetivos de negocio mientras se descuidan algunos riesgos críticos generando una brecha de seguridad.

8.1.3 Objetivos

La definición de objetivos de seguridad de la información se apoyan en el análisis de contexto y la definición del alcance, en este caso en particular los objetivos ya se encuentran definidos en el numeral 1.3 debido a que ya previamente se había realizado un análisis similar para definir la viabilidad del proyecto lo que aporta la información necesaria para proponerlos.

8.1.4 Análisis de Riesgos

La norma ISO 27001 dado que está hecha para ser aplicada a cualquier tipo de organización no define la metodología para calcular los riesgos por lo que deja libre el modo de aplicar su análisis y evaluación ya que dependiendo del tipo de escenario se personaliza el o los modelos que más se ajusten, de igual manera el estándar propone unos pasos para el desarrollo de la gestión del riesgo para así definir que debe contener dicho proceso con el objetivo de que el sistema de gestión de seguridad de la información pueda ser certificado.

Son cuatro pasos los que se enuncian comenzando por la metodología en la cual se define las reglas que se van a tener en cuenta y el cómo se va a llevar a cabo, para que se aplique de una manera estandarizada para toda la organización; el siguiente paso es la implementación donde se define la identificación de los activos de información, se encuentran sus vulnerabilidades y amenazas y se evalúa el impacto y la probabilidad para calcular el nivel de riesgo, cabe anotar que la última actualización de la norma respectiva al 2013 no requiere la identificación de activos y amenazas pero esto no se contempla en este proyecto ya que se considera como esencial; después de la implementación está el tratamiento del riesgo para lo cual se debe priorizar los riesgos más críticos y seleccionar los controles para mitigarlos, también se puede optar por transferir, aceptar o evitar el riesgo y como último paso está el informe el cual significa la documentación de todo lo anterior descrito; las fases del análisis de riesgos del proyecto se guían de manera similar a la propuesta por la norma ISO 27005.

8.1.4.1 Amenazas y Vulnerabilidades

Ya se entra a definir los pasos específicamente para el diseño del plan de tratamiento de riesgos de la campaña electoral, para esto se aprovecha la información resultante del estudio de contexto para identificar los procesos primordiales para los objetivos de negocio y de ahí se extraen los activos de información críticos, se analiza el activo de información en cuanto a sus contenedores y formatos para extraer cuáles son sus amenazas y que vulnerabilidades podrían aprovecharlas; también se define el responsable del riesgo determinando el activo lo contiene y de que proceso hace parte este activo con el fin de que el rol responsable de dicho proceso se defina como el dueño del riesgo; así ya teniendo las amenazas y vulnerabilidades definidas se procede a estructurar

el riesgo el cual plantea el escenario donde la amenaza pueda sacar provecho de la vulnerabilidad.

8.1.4.2 Impacto y Probabilidad

En este punto se propone la metodología con la que se calcula el impacto y la probabilidad aspecto que es muy importante ya que se debe proponer de una manera tal que se pueda aplicar a cualquier campaña, la valoración de estos términos y del riesgo en general se hace a través de una metodología de estimación cualitativa la cual permite identificar de una manera rápida y efectiva los riesgos que generarían un mayor efecto adverso al alcance de los objetivos de la campaña electoral; la escala empleada para estimar las consecuencias posibles y su posibilidad de ocurrencia son Alto (A), Medio (Medio) y Bajo (Bajo), estos valores se mantienen en todo el proceso de análisis de riesgo para que tenga homogeneidad.

8.1.4.2.1 Impacto y Áreas

El cálculo del impacto por una posible materialización de un riesgo se hace determinando primero la importancia del activo para la organización, para esto se definen las áreas que pueden ser afectadas por la vulneración de este cómo se muestran en la tabla 3 y después se mide el nivel de afectación, entre valores de bajo, medio y alto, que tendría la perdida de confidencialidad, disponibilidad e integridad de cada activo en cada una de las áreas dispuestas, como se ve a manera de ejemplo en la tabla 4.

8.1.4.2.1.1 Reputacional

Para el entorno electoral la reputación del candidato es algo primordial ya que de ello dependerá su nivel de aprobación o desaprobación lo que resulta de manera lógica en un nivel de votación, esta puede ser afectada tanto por hechos anteriores a la campaña o por aquellos que se presenten en el proceso de elección popular y estén relacionados con sus actividades profesionales y también las que hacen parte de su entrono privado e íntimo.

8.1.4.2.1.2 Legal

Esta categoría está conformada por dos áreas las cuales pueden tener una afectación de violarse alguna de los objetivos de la seguridad de la información en cuanto a confidencialidad, integridad y disponibilidad y son la *ley de protección de datos* debido a que para la inscripción de una candidatura por firmas o para la estrategia de comunicación una campaña debe registrar, procesar y almacenar un gran volumen de datos cobijados por esta norma que de no cumplirse podrían paralizar las actividades de recolección de datos lo que acabaría con las aspiraciones de un candidato independiente ya que no se podría inscribir o también podría afectar la cobertura de la estrategia de comunicación la cual es primordial

tanto para reforzar partidarios como para adquirir nuevos votos; la otra regulación contemplada en este aspecto es la *ley de transparencia* la cual debe ser cumplida por todas las campañas ya que deben rendir cuentas respecto a su financiación y contabilidad de lo contrario se podría perder la personería jurídica y financiación estatal.

8.1.4.2.1.3 Salud y Seguridad

De las consecuencias que la perdida de confidencialidad, integridad y disponibilidad de algún activo puedan afectar la seguridad física del candidato o su grupo de trabajo.

8.1.4.2.1.4 Financiación

De las consecuencias de la perdida de confidencialidad, integridad y disponibilidad de algún activo que pueden afectar la confianza de los grupos, individuos o empresas que aportan dinero como apoyo a la campaña del candidato física del candidato o su grupo de trabajo, como también de las faltas que afecten la financiación estatal.

Tabla 3. Áreas y escalas de valoración de impacto

	Niveles		
Área de Impacto	**Bajo (B)**	**Medio (M)**	**Alto (A)**
Reputacional (R)	Escándalo de alcance institucional	Escándalo de alcance regional	Escándalo de alcance Nacional
Estratégico (ES)	No tiene repercusión	Brinda ventaja a competencia	Competencia puede afectar gravemente a campaña
Ley de protección de datos (PD)	Infracciones leves	Denuncias de usuarios ante campaña por malas prácticas	Suspensión de tratamiento de datos hasta por 6 meses
Ley de transparencia (LT)	Infracciones leves	Denuncias de usuarios ante campaña por malas prácticas	Suspensión de personería jurídica y financiación
Salud y Seguridad (S)	No representa riesgo	Posibilidad de acciones en contra de la integridad del candidato	Riesgo inminente contra la integridad del candidato
Financiación (F)	No representa riesgo	Perdida baja de patrocinadores y financiación	Perdida alta de patrocinadores y financiación

Tabla 4. Esquema Valoración de Activo

Activo de Información	Confidencialidad						Integridad						Disponibilidad					
	R	ES	PD	LT	S	F	R	ES	PD	LT	S	F	R	ES	PD	LT	S	F
Activo 1	B	B	B	B	B	B	M	M	M	M	M	M	A	A	A	A	A	A
Activo 2	B	B	B	B	B	B	M	M	M	M	M	M	A	A	A	A	A	A
Activo 3	B	B	B	B	B	B	M	M	M	M	M	M	A	A	A	A	A	A
Activo 4	B	B	B	B	B	B	M	M	M	M	M	M	A	A	A	A	A	A

Elaborando la tabla 4 con las consideraciones establecidas en la tabla 3 se define la valoración de los activos la cual es la base para calcular el impacto; finalmente para calcular el impacto se deben tener los riesgos definidos y a partir de estos se selecciona que criterio o criterios de información es el primordial en cuanto a su afectación, es decir el riesgo está relacionado de manera más estrecha a la confidencialidad, integridad o disponibilidad, después de definido este criterio se remite a la tabla 4 para el activo involucrado a ese riesgo y se extrae el valor más alto de cualquiera de las área de ese criterio, ese valor sería el impacto.

8.1.4.2.2 Probabilidad

El cálculo de la posibilidad de que la amenaza tome provecho de la vulnerabilidad asociada al activo de información se realiza basándose en la metodología propuesta por OWASP para la estimación de la probabilidad en análisis de riesgos, como se presenta en el documento de Machaca, y se aplica a cada uno de los riesgos estructurados, la medición para este caso se realiza a través de las cuatro categorías que más se ajustan al contexto del proyecto seleccionadas de las ocho que propone el modelo y las cuales se describen en los numerales siguientes y se observan en la tabla 5 a modo de ejemplo; para estimar el nivel de probabilidad para cada riesgo a cada categoría se le asigna un valor numérico desde cero (0) hasta nueve (9) donde 0 es la probabilidad o el valor más bajo y 9 el más alto, después de asignado cada valor se calcula el promedio y el resultado obtenido se convierte a valores cualitativos de bajo, medio y alto usando la tabla 6 con el fin de aplicar las mismas escalas de medidas.

Tabla 5. Probabilidad

Riesgo	Motivación	Capacidad	Facilidad	Conocimiento	Promedio	Probabilidad
Riesgo 1	1	1	1	1	1	B
Riesgo 2	2	2	2	2	2	B
Riesgo 3	3	3	3	3	3	B
Riesgo 4	4	4	4	4	4	M
Riesgo 5	5	5	5	5	5	M

Tabla 6. Escala Valores Probabilidad

	Baja (B)	Media (M)	Alta (A)
Probabilidad (P)	0 < P < =3	3 < P <= 6	6 < P <= 9

8.1.4.2.2.1 Motivación

La motivación está relacionada a la amenaza y es el grado de incitación que esta posee para realizar una acción en contra del activo relativo al riesgo.

8.1.4.2.2.2 Capacidad

Al igual que la motivación la capacidad está relacionada a la amenaza y significa el nivel de conocimientos y aptitudes que esta podría poseer para aprovecharse de la vulnerabilidad.

8.1.4.2.2.3 Facilidad

Esta categoría está relacionada a la vulnerabilidad y mide que tan simple es su aprovecharse de esta.

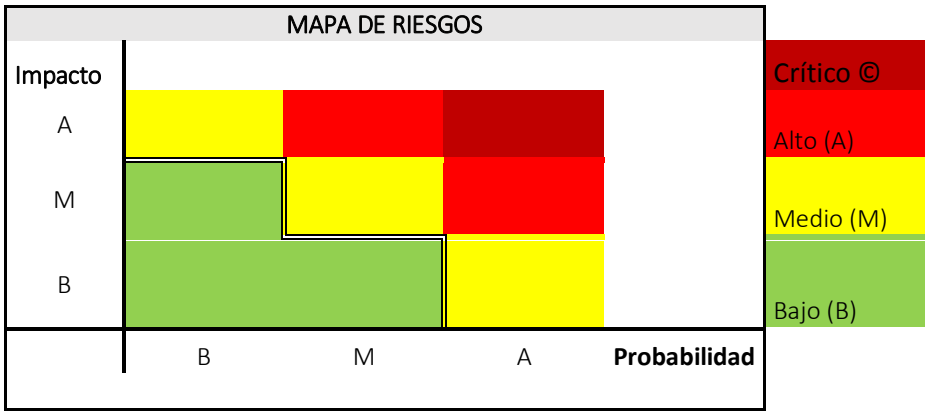
8.1.4.2.2.4 Conocimiento

Se valora que tan conocida es la vulnerabilidad lo que determinaría la visibilidad de esta ante las amenazas que la asechan y para este caso en el escenario política para este campo no solo se tiene en cuenta el nivel de conocimiento de la vulnerabilidad sino también el conocimiento de lo que podrían hacer a nivel político de vulnerarla, por ejemplo para una agenda de un candidato sería no solo conocer si es vulnerable si no también que podrían hacer con esta.

8.1.4.3 Riesgo

Ya definidas la probabilidad e impacto sobre los activos se calcula el riesgo y se analiza para clasificarlos e identificar los más críticos que deben ser abordados con mayor prioridad, dependiendo de la organización se debe definir el nivel de riesgo tolerable, el nivel de riesgo aceptable para este escenario es nivel bajo por tal motivo todo riesgo por encima de ese nivel debe ser tratado para ser trasladado hasta este nivel; para obtener el valor del riesgo se ubica el impacto y la probabilidad sobre el mapa de calor ilustrado en la tabla 7 y dependiendo del color donde se ubique el riesgo se le asigna su valor; con todo la información levantada en el análisis de riesgos hasta este punto se construye la tabla de registro de riesgos base para continuar con la propuesta de tratamiento de riesgos.

Tabla 7. Mapa de Riesgos



8.1.4.4 Plan de tratamiento de riesgos

A través de la categorización de los riesgos que deben ser tratados y el conocimiento de las amenazas y vulnerabilidades relacionados se seleccionan los controles responsables de mitigarlos teniendo en cuenta el propósito del proyecto que es usar medidas administrativas y herramientas gratuitas o de bajo costo en la medida de lo posible para hacer frente a los riesgos.

Con los controles identificados se elabora el plan de tratamiento de riesgos el cual lista todos los controles que se desean aplicar y se aportan detalles sobre su implementación como responsable, recursos temporales y de presupuesto necesarios; este documento es el objetivo del proyecto ya que este servirá como guía base en la planeación y construcción de una campaña política con su información asegurada.

ANEXO 2

8.2 Contexto campañas electorales

El primer paso a emprender de donde se extraen las bases para realizar un aseguramiento de la información alineado con los objetivos del negocio es el análisis de contexto del entorno foco de la implementación que para este caso es las campañas electorales en Colombia para lo cual se describirán cuáles son sus objetivos, estructura organizacional y procesos más comunes con la finalidad de extraer los activos de información más importantes que apoyan el alcance de las metas.

8.2.1 Objetivos

Cuando se piensa en una campaña política la primera idea que se tiene acerca de su principal objetivo es ganar las elecciones pero en la realidad eso difiere ya que dependiendo del tamaño del grupo o partido del candidato, recursos, ideología, entre otras no siempre la vista de la campaña esta puesta en el triunfo ya que se puede estar apuntando solo a ganar popularidad para unas futuras elecciones para otro cargo de elección popular, cuando los recursos son muy ajustados se puede tener como objetivo alcanzar un nivel de votos que permita hacer alianzas con el partido ganador o pueden presentarse campañas que su objetivo no sean los votos si no promover una ideología como por ejemplo un grupo ecologista o perteneciente a alguna religión, así las cosas se plantean los siguientes objetivos.

- Ganar las Elecciones
- Obtener un nivel significativo de votos
- Promocionar una idea

8.2.2 Estructura Organizacional

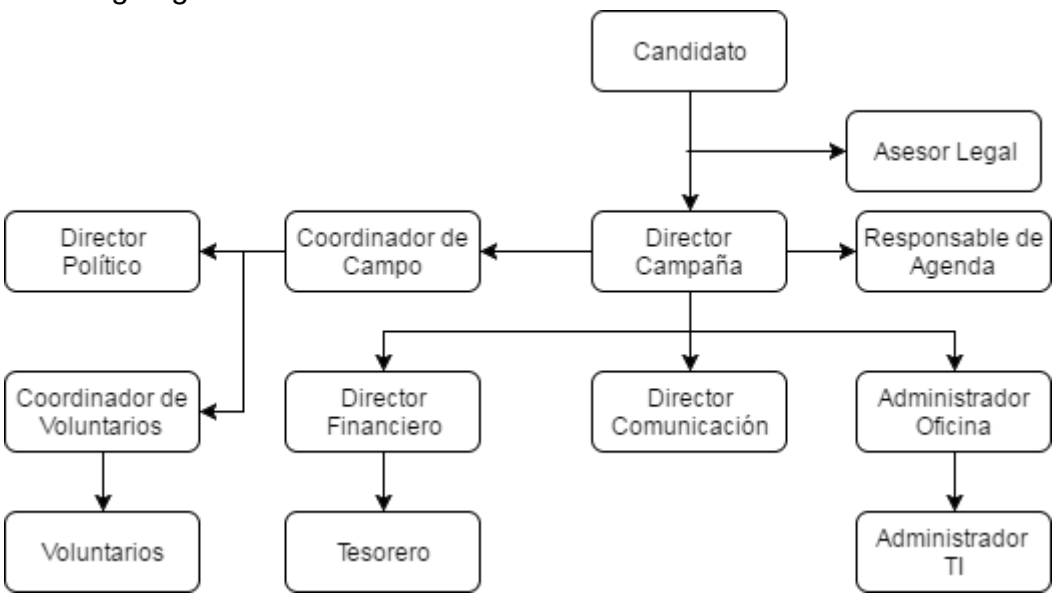
Par poder organizar y funcionar de una manera ágil y efectiva una campaña su estructura generalmente es vertical donde el candidato y el director de campaña son los que toman las decisiones de fondo y se difunden las ordenes de arriba hacia abajo para que las acciones puedan ser acatadas y emprendidas en el menor tiempo posible ya que este es el recurso más importante en este entorno.

Las características particulares de las campañas y que son de importancia para el campo de la seguridad de la información son la multiplicidad de cargos de un individuo, es decir que una sola persona puede asumir varios de los roles establecidos, se presenta también una circulación de personal alta, es decir personal voluntario o contratado ingresa o termina relaciones con la organización constantemente y la categorización del recurso humano en cuanto a la relación laboral con la organización es muy variante, hay poco personal contratado con

sueldo y hay un mayor volumen de voluntarios que ofrecen sus servicios sin ninguna remuneración o relación contractual.

En base al estudio de los planteamientos de especialistas sobre el tema como se ilustra en el artículo de Cobos (septiembre 2014) y en la presentación de Gutiérrez (2013) donde se identifican los roles y funciones comunes para las campañas con lo que se propone el organigrama general de la campaña electoral en la figura 4.

Figura 4. Organigrama



Fuente: Propia

8.2.2.1 Roles y Funciones

De acuerdo a lo planteado en el apartado anterior se identifican los roles y se describen sus funciones.

8.2.2.1.1 Director de Campaña

El director es el responsable de supervisar todos los aspectos de la campaña en el día a día, debe ser de plena confianza del candidato y es el que posee mayor acceso y contacto con este, desempeña funciones de contratación y administración del personal, coordinación e implementación de la mano con el candidato de la recaudación de fondos, hacer y administrar presupuesto, coordinar y monitorizar servicios externos (agencias publicidad, consultores, encuestadoras y proveedores).

8.2.2.1.2 Director Financiero

Responsable de la recaudación de dinero que permitirá a la campaña cumplir con sus metas, trabaja estrechamente con el candidato y el director de campaña, entre

sus funciones esta supervisar los eventos y reuniones que tienen como objetivo recaudar fondos; como el rol de director financiero puede ser asumido por el director de campaña.

8.2.2.1.3 Coordinador de Campo

El coordinador de campo es el responsable de desarrollar la estrategia para llevar el mensaje de campaña a los votantes con métodos como el puerta a puerta, llamadas directas, correos electrónicos y mensajes de texto, a su vez coordina el registro de votantes lo que resultan en la administración de un gran volumen de datos y sus tareas están más enfocadas a bases y oficinas descentralizadas.

8.2.2.1.4 Director de Comunicación

Es el responsable de la estrategia de comunicación por lo tanto es el que está a cargo de todas las interacciones de la campaña con los medios, preparar entrevistas, identificar oportunidades de medios, escribir literatura para la campaña y proponer discursos.

8.2.2.1.5 Tesorero o Contador

El tesorero o contador de la campaña es un rol muy importante y de mucha responsabilidad debido a que supervisa los aspectos financieros y de contabilidad de la campaña, monitorea contribuciones, administra registros financieros y es también responsable de cumplir con las regulaciones correspondientes como para el caso de Colombia con la ley de transparencia, en campañas pequeñas aprueba gastos y apoya la preparación y monitoreo del presupuesto, debe tener experiencia en campañas y por su criticidad respecto a la información a la que tiene acceso es recomendado que sea contratado a tiempo completo o un voluntario de gran confianza o que sea familiar del candidato.

8.2.2.1.6 Coordinador de Voluntarios

Trabaja con el director de campo para identificar, reclutar, administrar y motivar los voluntarios que soportan las actividades diarias de campaña, ayuda a coordinar el trabajo de los voluntarios aprovechando sus aptitudes y habilidades; este rol puede ser asumido por el coordinador de campo.

8.2.2.1.7 Director Político

Trabaja con grupos objetivos específicos con el fin de adherir a la campaña líderes entre los cuales se pueden encontrar sindicales, comunales, educadores, etnias, entre otras para organizar su participación en la campaña, trabaja en colaboración con el director de campaña a través de la construcción de relaciones con organizaciones que representan esas comunidades

8.2.2.1.8 Responsable de Agenda

La función principal del responsable de la agenda es asegurar que el candidato sea informado sobre cada evento con direcciones apropiadas, información de contacto, resumen de los objetivos y retos de la presencia en cada acto y recoger información recolectada por otros miembros de campaña en cada evento

8.2.2.1.9 Administrador de Oficina

Es el responsable de mantener la oficina principal y coordinar aspectos administrativos de campaña como administrar personal, infraestructura, suministros y muchas otras actividades

8.2.2.1.10 Administrador TI

Es la persona que coordina y administra todo lo relacionado con la tecnología de la campaña como mantenimiento de la página de internet, administración de la base de datos, red, y computadores.

8.2.2.1.11 Asesor Legal

Es la persona que cuenta con conocimientos en la parte legal enfocada en elecciones y finanzas de campaña y brinda asesoría al equipo en todas las acciones y aspectos relacionados.

8.2.3 Procesos

Se pueden definir como se expone en el artículo de Katz (2014) en el contexto de las campañas electorales tres procesos los cuales son fundamentales para la operación de las actividades y el cumplimiento de regulaciones y que se definen a continuación y se ilustran en la figura 5.

8.2.3.1 Financiación

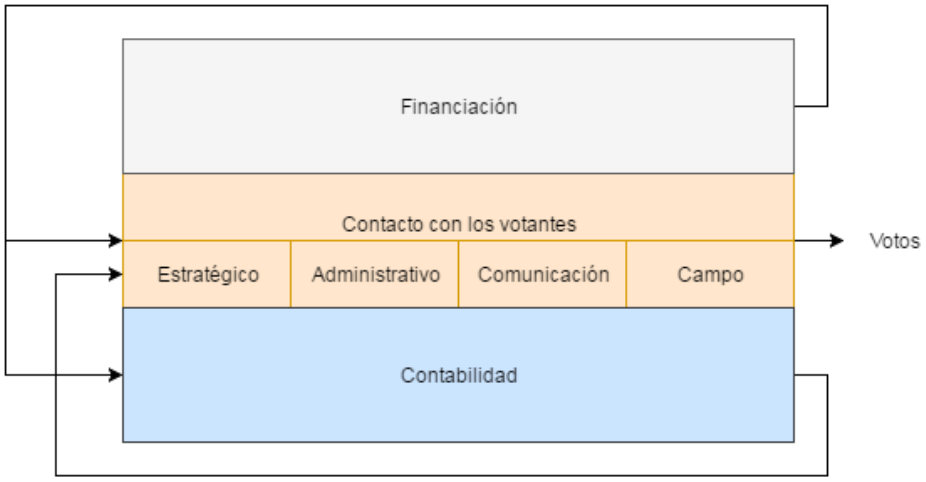
Este proceso es base y es el responsable de darle impulso a la campaña a través de recolección de fondos los cuales soportan todas las actividades de la campaña, sin este proceso la campaña quedaría paralizada; el responsable de este proceso es el director financiero.

8.2.3.2 Contacto con los votantes

La importancia de este proceso radica en que es el enfocado a proyectar todas las estrategias y planes hacia los votantes con el objetivo de que conozcan el candidato o sus ideales y dirigir su intención de voto hacia este, de este proceso hacen parte el coordinador de campo, director de comunicación, director político, responsable

de agenda, administrador de oficina y administrador TI, es decir, este proceso es el que reúne todo el esfuerzo y presupuesto para llegar a los votantes por los diferentes medios y estrategias que se dispongan; se puede discriminar internamente dentro de este proceso los subprocesos de comunicación, operaciones de campo, estratégico y administrativo en este último es donde se incluye la administración TI; se puede inferir al incluir tantos procesos que el responsable de este proceso en general es el director de campaña.

Figura 5. Mapa de Procesos



Fuente: Propia

8.2.3.3 Contabilidad

Como se viene mostrando desde la definición de roles la contabilidad es un proceso crítico debido a que es el que indica el estado económico para tomar decisiones estratégicas en base a la generación de reportes de presupuesto, caja menor y rastreo de fondos recolectados siempre cumplimiento con las regulaciones aplicadas; su responsable es el tesorero o contador.

8.2.4 Infraestructura

Un aspecto importante a tener en cuenta son las características relacionadas con la infraestructura física como la selección de la ubicación y locales ya que esta debe ser el resultado de una planeación previa a la contienda electoral ya que en el periodo después del inicio del proceso de elecciones no permite dedicar tiempo a modificaciones en infraestructura tanto física como tecnología por lo que es de gran importancia seleccionar los elementos más apropiados, en este punto en el proceso de campaña es donde se debe concebir la evaluación e implementación del plan de tratamiento de riesgos de seguridad de la información objeto de este proyecto para que se conciba de manera unificada con la selección de tecnología, infraestructura física y recurso humano.

Ya entrando más en el tema de las características de los locales se deben seleccionar lugares abiertos para fácil acceso de los militantes del candidato y voluntarios como del público en general, se usan locales satélites para campañas de mayor envergadura enfocados en tareas de comunicación como distribución de material electoral, como también para reclutamiento, capacitación y socialización, la visibilidad de estos espacios es un factor importante para promocionar la imagen del candidato.

8.2.5 Activos de Información

Ya planteada la estructura organizacional, procesos, roles y funciones extraídos a través del análisis de libros especializados como Costa (1994) y ODCA (2006) lo que aporta una parte de la información necesaria para identificar activos de información involucrados; esta información se complementa a través del conocimiento aportado por el Ingeniero y periodista Álvaro Muriel a raíz de su experiencia en participación en múltiples campañas políticas para alcaldía, gobernación y senado en el departamento del Quindío (Muriel, A. Comunicación telefónica, 29 de Abril de 2017), por lo anterior se logra identificar los activos de información críticos de una campaña electoral que se describen en los siguientes numerales y se presentan en la tabla 8.

8.2.5.1 Contabilidad

La contabilidad es un activo muy valioso en cuantos aspectos regulatorios y para la misma operación de la campaña ya que se dependen de los informes de esta para poder emprender estrategias que requieren gastos económicos; este activo pertenece al proceso de contabilidad y su propietario es el contador, los estados contables de hacerse públicos pueden afectar la confianza de los patrocinadores como también pueden dar una ventaja estratégica a las campañas competidoras, cabe anotar que la ley de transparencia exige hacerlos públicos pero esto se realiza después de pasadas las elecciones.

8.2.5.2 Agenda

Reuniones y presentaciones tanto privadas como públicas, estas pueden ser con el objetivo de promover la intención de voto favorable hacia el candidato como también pueden estar enfocadas en acordar aportes a la campaña por parte de patrocinadores; este activo de información está involucrado en los procesos de financiación y de contacto con los votantes y el propietario el responsable de agenda y los custodios son el director financiero, director de comunicación, director de campaña, director político y candidato ya que estos son los encargados de acordar este tipo de eventos.

8.2.5.3 Registro de Votantes

Base de datos recolectada con la información de todos los individuos que apoyan la campaña y los que serían potenciales votantes normalmente se maneja un gran volumen de información la cual incluye datos personales los cuales son necesarios para realizar estrategias de comunicación, el propietario de este activo es el coordinador de campo.

8.2.5.4 Lista de Líderes

Es el registro de los líderes políticos, sindicales, comunales, educadores, etnias, entre otros, es un activo de gran valor debido a que registra la información de quienes aportan los votos que no corresponden a los de opinión sino que vienen representados por el apoyo de una estructura, esta información es muy valiosa para las campañas contrincantes ya que con esta podrían acercarse a los líderes y cambiar su apoyo, este activo se encuentra en el proceso de contacto con los votantes en los subprocesos estratégico y campo; el propietario es el director político y el custodio el director de campaña.

8.2.5.5 Información Estratégica no Documentable

Es toda aquella información relativa a estrategias a aplicar que no se registran en ningún documento físico ni digital pero que es trasmitida por las líneas de comunicación entre los actores más importantes de las campañas que tienen datos o tácticas con objetivos como desprestigiar las campañas de la competencia, acciones estratégicas que se necesitan adoptar rápidamente en campo; normalmente está compuesta por información inmediata para tomar acciones rápidas por lo que su uso más practico es a través de la mensajería instantánea; este tipo de información es fugaz por lo que no tiene ningún propietario pero si tiene custodios que normalmente son el candidato, director de campaña, director político, director financiero, contador y director de comunicación.

8.2.5.6 Imagen en Plataformas Electrónicas

Actualmente uno de los activos de información más críticos es la imagen del candidato a través de las nuevas herramientas de las tecnologías de la información que si bien proveen una facilidad de promoción masiva también tiene asociados riesgos que pueden afectar la reputación del candidato y cambiar la intención de voto de los electores de manera muy rápida por lo que debe ser tenido a consideración en el aseguramiento de la información.

8.2.5.7 Estrategia de Comunicación

Este activo de información hace ahínco en todo lo relativo a los planes, estudios e indicadores documentados en las cuales se basa la campaña para llegar al público

en general a través de medios de comunicación, trabajo de campo, discurso y debates, entre otros, que quedan registrados en estudios de debilidades y fortalezas propios, encuestas privadas de la campaña, discurso del candidato y estrategia publicitaria que de ser conocidos por los contendores pondrían en desventaja a la campaña.

Tabla 8. Activos de Información

Activo	Procesos	Contenedor	Descripción	Propietario	Custodios
Contabilidad	Contabilidad	Computador	Archivo digital alojado en PC de contador	Contador	Contador
		Informes	Archivos digitales o físicos con estados financieros de campaña	Contador	Candidato/Director Campaña/Director Financiero/ Candidato
		Facturas	Soportes físicos ingresos/egresos	Contador	Administración/Contador/Personal
Agenda	Financiación/ Contacto con los votantes	físico	Agenda escrita en cuaderno	Responsable de Agenda	Director financiero, director de comunicación, director de campaña, director político y candidato
		Digital	Agenda Digital		
Registro Votantes	Contacto con los votantes en los subprocesos de comunicación y administración TI	Digital	Archivo digitalizado con la información de los posibles votantes normalmente alojada en Excel en campañas de bajo presupuesto	Coordinador de Campo	Administrador TI
		Formularios Físicos	Formularios donde se recoge datos y firma de votantes		Voluntarios, Coordinador de Voluntarios, Administrador TI
Lista de Lideres	Contacto con los votantes en los subprocesos estratégico y campo	Archivo digital	Archivo digitalizado con la información de los lideres adscritos y sus datos de contacto	Director Político	Director de campaña
Información estratégica no documentable	Todos los procesos	Dispositivo Móvil	Mensajes almacenados en dispositivos	NA	Candidato, director de campaña, director político, director financiero, contador y director de comunicación
		Emails	Mensajes almacenados en Correos electrónicos		

		Llamadas	Mensajes difundidos por voz a través de llamadas		
Imagen en Plataformas Electrónicas	Contacto con los votante	Redes sociales	Redes sociales como Facebook y Twitter para promoción del candidato	Director de Comunicación	Administrador TI, Administradores de redes sociales
Estrategia de Comunicación	Contacto con los votantes en el subproceso de comunicación	Archivos Digitales	Archivos digitales de planes y estudios estratégicos de Comunicación	Director de Comunicación	Candidato y director de campaña
		Archivos Físicos	Archivos impresos de planes y estudios estratégicos de Comunicación		

8.2.6 Alcance

Con el análisis de contexto se define el alcance que abarca el análisis de riesgos el cual para este escenario cobija todos los procesos y subprocesos de la campaña electoral debido a que en su modelo de funcionamiento organizacional cuenta con una estructuración relativamente pequeña y todos están alineados con sus objetivos a diferencia de lo que se puede encontrar en una empresa de tamaño considerable que puede contener muchos procesos de los cuales algunos no se relacionan con su objetivo de negocio; por lo tanto se aplicara la metodología propuesta a los procesos antes mencionados y a sus activos de información críticos dispuestos en la tabla 8.

ANEXO 3

8.3 Registro de Riesgos

Se realiza y se plasma todo el proceso para el análisis y evaluación del riesgo como se plantea en la metodología con el fin de identificar, analizar y valorar los riesgos y finalmente con los resultados elaborar la tabla de registros de riesgos (tabla 12) la cual es uno de los productos del proyecto.

8.3.1 Amenazas y Vulnerabilidades

Para los activos de información resultantes del estudio del contexto se identifican las amenazas y vulnerabilidades teniendo en cuenta sus contenedores, propietarios y usuarios como se dispone en la tabla 8 para poder estructurar los riesgos los cuales se registran en la tabla 9.

Tabla 9. Amenazas, Vulnerabilidades y Riesgos

Activo	Contenedor	Amenazas	Vulnerabilidades	Riesgos
Contabilidad	Computador	1. Interna no Intencional 2. Externa Intencional 3. No cumplimento de regulación 4. Malware	1. No copia de respaldo 2. Archivo accesible 3. PC no seguro	1. Sanción por infringir la ley de transparencia por pérdida de la contabilidad. 2. Pérdida de confianza de patrocinadores por filtración de donaciones. 3. Afectación de imagen de candidato por revelación de patrocinadores de mala reputación.
	Informes	1. Externa Intencional	1. Archivo accesible	4. Campaña queda en desventaja estratégica debido a que la competencia conoce su bajo presupuesto.
Agenda	físico	1. Externa Intencional 2. Interna no intencional	1. No copia de respaldo 2. Archivo accesible	1. Afectación de imagen de candidato por filtración de reunión con aliado de mala reputación. 2. Perdida de patrocinio debido a sabotaje a reunión con patrocinadores. 3. Atentado a la integridad Física del candidato. 4. Candidato no asiste a presentación por extravío de agenda.
	Digital			
Registro Votantes	Digital	1. Externa Intencional 2. Interna no intencional 3. No cumplimento de regulación 4. Malware	1. No copia de respaldo 2. Archivo accesible 3. PC no seguro 4. No Cifrado	1. Se detiene operación de estrategia de comunicación de campo por eliminación de archivo de registro. 2. Suspensión de proceso de registro de votantes por infringir ley de protección de datos.
	Formularios Físicos	1. Externa intencional 2. Interna no intencional 3. Ambiental	1. Almacenamiento accesible 2. Almacenamiento no seguro	3. Candidato no puede inscribir su postulación por firmas por perdida de formularios.

Lista de Lideres	Archivo digital	1. Externa intencional 2. Malware	1. Almacenado sin seguridad	1. Pérdida de votos debido a que campaña opositora se roba los lideres porque tuvo acceso a la lista. 2. Imagen desfavorable por filtración de alianzas con líderes de mala reputación.
Información estratégica no documentable	Dispositivo Móvil	1. Externa intencional 2. Malware	1. Dispositivos sin seguridad de acceso 2. Dispositivos no seguros 3. Visible a personas alrededor	1. Afectación de imagen de candidato por filtración de mensajes privados por robo de dispositivo. 2. Afectación de imagen de candidato por filtración de información por hackeo de dispositivo. 3. Afectación de imagen de candidato por filtración de mensajes por técnica de shoulder surfing.
	Emails		1. Contraseñas no seguras 2. Equipo vulnerable a malware 3. Phishing	4. Afectación de imagen de candidato por filtración de información por cuenta de correo hackeada.
	Llamadas		1. No cifradas 2. Susceptible a chuzadas	5. Afectación de imagen de candidato por filtración de grabaciones de llamadas.
Imagen en Plataformas Electrónicas	Redes sociales	1. Externa intencional	1. Contraseñas no seguras 2. Phishing 3. Redes no seguras 4. Dispositivo no seguro 5. Noticias falsas 6. Personal responsable temporal	1. Afectación de imagen de candidato por publicaciones falsas a través de su cuenta original. 2. Disminución de popularidad por circulación de noticias falsas. 3. Se detiene operación de promoción en redes por perdida de credenciales de acceso por renuncia de administrador de la plataforma.
Estrategia de Comunicación	Archivos Digitales	1. Interna no Intencional 2. Externa Intencional	1. No copia de respaldo 2. Archivo accesible	1. Pérdida de productividad por eliminación de documentos estratégicos. 2. Campaña queda en desventaja ante sus competidores por filtración de información estratégica almacenada en medios digitales
	Archivos Físicos	1. Externa intencional	1. Documento accesible	3. Campaña queda en desventaja ante sus competidores por filtración de información estratégica almacenada en medios físicos

En la tabla se puede observar que la estructuración de los riesgos se formula alineando la afectación hacia los objetivos estratégicos del entorno objeto de análisis con la finalidad de que para los candidatos, líderes y directivos de las campañas sea justificable la implementación de medidas para mitigarlo; cabe anotar que todos los riesgos que pueden afectar la imagen del candidato por ende impactan la imagen de la campaña y el partido al que este afiliado de darse el caso, lo que no solo genera disminución en la votación favorable al candidato actual sino que también perjudicara las aspiraciones futuras del partido por lo que estos deben ser conscientes de las consecuencias que puedan ser causadas por el no aseguramiento de la información y por lo tanto deberían promover su implementación entre sus candidatos afiliados.

8.3.2 Impacto y Probabilidad

Aplicando la metodología descrita en el apartado (4.4.2.1) se valoran los activos identificados usando las tablas 3 y 4 y el resultado se dispone en la tabla 10 la cual es la referencia para calcular el impacto.

Tabla 10. Valoración de Activos

Activo de Información	Confidencialidad						Integridad						Disponibilidad					
	R	ES	PD	LT	S	F	R	ES	PD	LT	S	F	R	ES	PD	LT	S	F
Contabilidad	A	M	B	B	B	A	B	B	B	A	B	B	M	B	B	A	B	B
Agenda	M	M	B	B	A	M	B	M	B	B	B	B	B	M	B	B	B	M
Registro de Votantes	B	M	A	B	B	B	B	M	M	B	B	B	B	A	M	B	B	B
Lista de Lideres	A	A	B	B	B	M	B	B	B	B	B	B	B	M	B	B	B	B
Información estratégica no documentable	A	A	B	B	B	A	B	B	B	B	B	B	B	A	B	B	B	B
Imagen en Plataformas Electrónicas	B	B	B	B	B	B	A	A	B	B	B	A	B	A	B	B	B	B
Estrategia de Comunicación	B	M	B	B	B	B	B	M	B	B	B	B	B	M	B	B	B	B

Para la estimación de la probabilidad se aplican las tablas 5 y 6 a cada riesgo de la manera dispuesta en el numeral (4.4.2.2) y con los valores resultantes se construye la tabla 11.

Tabla 11. Probabilidad

Riesgo	Motivación	Capacidad	Facilidad	Conocimiento	Promedio	Probabilidad
Sanción por infringir la ley de transparencia por pérdida de la contabilidad.	1	6	5	2	4	M
Pérdida de confianza de patrocinadores por filtración de donaciones.	2	6	5	6	5	M
Afectación de imagen de candidato por revelación de patrocinadores de mala reputación.	9	6	5	6	7	A
Campaña queda en desventaja estratégica debido a que la competencia conoce su bajo presupuesto.	4	6	5	6	5	M
Afectación de imagen de candidato por filtración de reunión con aliado de mala reputación.	9	8	7	5	7	A
Perdida de patrocinio debido a sabotaje a reunión con patrocinadores.	9	8	7	1	6	M

Atentado a la integridad Física del candidato.	3	1	7	5	4	M
Candidato no asiste a presentación por extravío de agenda.	1	8	7	1	4	M
Se detiene operación de estrategia de comunicación de campo por eliminación de archivo de registro.	5	5	5	3	5	M
Suspensión de proceso de registro de votantes por infringir ley de protección de datos.	6	5	5	1	4	M
Candidato no puede inscribir su postulación por firmas por perdida de formularios.	9	6	5	6	7	A
Pérdida de votos debido a que campaña opositora se roba los lideres porque tuvo acceso a la lista.	9	6	6	8	7	A
Imagen desfavorable por filtración de alianzas con líderes de mala reputación.	4	6	6	8	6	M
Afectación de imagen de candidato por filtración de mensajes privados por robo de dispositivo.	6	3	7	7	6	M
Afectación de imagen de candidato por filtración de información por hackeo de dispositivo.	6	1	2	7	4	B
Afectación de imagen de candidato por filtración de mensajes por técnica de shoulder surfing.	6	9	7	3	6	M
Afectación de imagen de candidato por filtración de información por cuenta de correo hackeada.	6	6	6	7	6	M
Afectación de imagen de candidato por filtración de grabaciones de llamadas.	9	1	1	7	5	M
Afectación de imagen de candidato por publicaciones falsas a través de su cuenta original.	9	6	6	7	7	A
Disminución de popularidad por circulación de noticias falsas.	9	9	9	9	9	A
Se detiene operación de promoción en redes por perdida de credenciales de acceso por renuncia de administrador de la plataforma.	3	6	9	1	5	M
Pérdida de productividad por eliminación de documentos estratégicos.	3	6	5	6	5	M

Campaña queda en desventaja ante sus competidores por filtración de información estratégica almacenada en medios digitales	9	6	5	9	7	A
Campaña queda en desventaja ante sus competidores por filtración de información estratégica almacenada en medios físicos.	9	6	7	9	8	A

8.3.3 Evaluación del Riesgo

Para calcular los niveles de riesgo primero se finaliza la valoración del impacto con la selección del criterio de seguridad afectado por cada riesgo con lo que se ubica el valor más alto en la tabla 10 para dicho criterio con lo que se obtiene el valor final del impacto, los valores de probabilidad e impacto se ubican en el mapa de riesgos de la tabla 13 para obtener el nivel de riesgo el cual se registra en la tabla 12.

Tabla 12. Registro de Riesgos

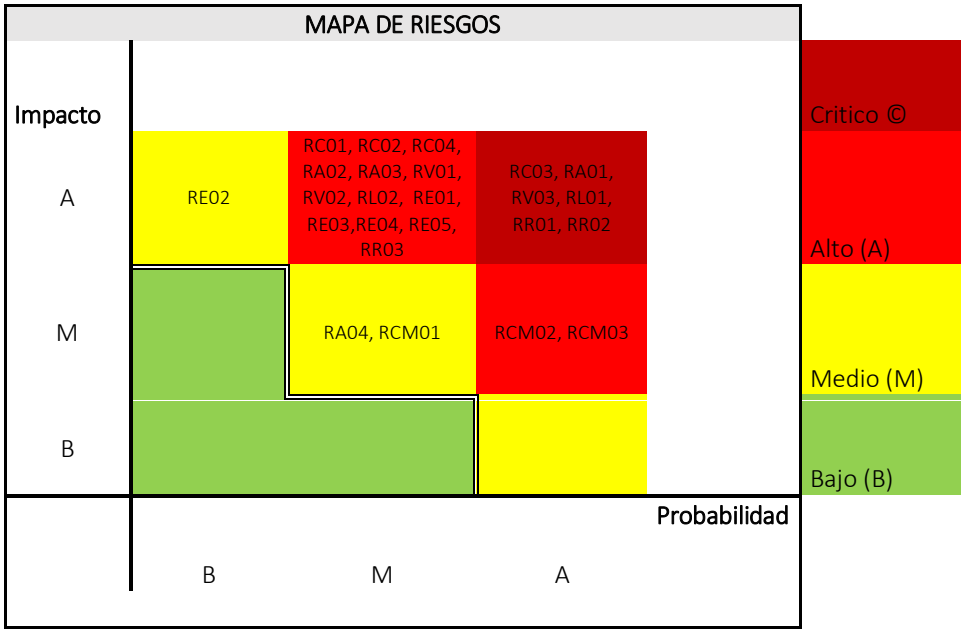
ID Riesgo	Activo	Descripción Riesgo	Criterio	Impacto	Probabilidad	Nivel Riesgo	Propietario
RC01	Contabilidad	Sanción por infringir la ley de transparencia por pérdida de la contabilidad.	Disponibilidad	A	M	A	Contador
RC02		Pérdida de confianza de patrocinadores por filtración de donaciones.	Confidencialidad	A	M	A	
RC03		Afectación de imagen de candidato por revelación de patrocinadores de mala reputación.	Confidencialidad	A	A	C	
RC04		Campaña queda en desventaja estratégica debido a que la competencia conoce su bajo presupuesto.	Confidencialidad	A	M	A	
RA01	Agenda	Afectación de imagen de candidato por filtración de reunión con aliado de mala reputación.	Confidencialidad	A	A	C	Responsable de Agenda
RA02		Perdida de patrocinio debido a sabotaje a reunión con patrocinadores.	Confidencialidad	A	M	A	
RA03		Atentado a la integridad Física del candidato.	Confidencialidad	A	M	A	
RA04		Candidato no asiste a presentación por extravío de agenda.	Disponibilidad	M	M	M	
RV01	Registro Votantes	Se detiene operación de estrategia de comunicación de campo por eliminación de archivo de registro.	Disponibilidad	A	M	A	Coordinador de Campo
RV02		Suspensión de proceso de registro de votantes por infringir ley de protección de datos.	Confidencialidad	A	M	A	

RV03		Candidato no puede inscribir su postulación por firmas por perdida de formularios.	Disponibilidad	A	A	C	
RL01	Lista Lideres	Pérdida de votos debido a que campaña opositora se roba los lideres porque tuvo acceso a la lista.	Confidencialidad	A	A	C	Director Político
RL02		Imagen desfavorable por filtración de alianzas con líderes de mala reputación.	Confidencialidad	A	M	A	
RE01	Información estratégica no documentable	Afectación de imagen de candidato por filtración de mensajes privados por robo de dispositivo.	Confidencialidad	A	M	A	Niveles Altos
RE02		Afectación de imagen de candidato por filtración de información por hackeo de dispositivo.	Confidencialidad	A	B	M	
RE03		Afectación de imagen de candidato por filtración de mensajes por técnica de shoulder surfing.	Confidencialidad	A	M	A	
RE04		Afectación de imagen de candidato por filtración de información por cuenta de correo hackeada.	Confidencialidad	A	M	A	
RE05		Afectación de imagen de candidato por filtración de grabaciones de llamadas.	Confidencialidad	A	M	A	
RR01	Imagen en Plataformas Electrónicas	Afectación de imagen de candidato por publicaciones falsas a través de su cuenta original.	Integridad	A	A	C	Director de Comunicación
RR02		Disminución de popularidad por circulación de noticias falsas.	Integridad	A	A	C	
RR03		Se detiene operación de promoción en redes por perdida de credenciales de acceso por renuncia de administrador de la plataforma.	Disponibilidad	A	M	A	
RCM01	Estrategia de Comunicación	Pérdida de productividad por eliminación de documentos estratégicos.	Disponibilidad	M	M	M	Director de Comunicación
RCM02		Campaña queda en desventaja ante sus competidores por filtración de información estratégica almacenada en medios digitales	Confidencialidad	M	A	A	
RCM03		Campaña queda en desventaja ante sus competidores por filtración de información estratégica almacenada en medios físicos.	Confidencialidad	M	A	A	

El resultado del nivel para la mayoría de los riesgos es alto, esto es debido a que los activos identificados para el caso son muy críticos para las campañas y normalmente no se tienen asegurados inclusive algunos de estos se manejan con imprudencia por lo que la probabilidad de que sean vulnerados también tiende a niveles altos; entre los resultados también se identifican seis riesgos críticos, tres de estos por afectaciones a la confidencialidad algo lógico debido al hermetismo

con el que se debe manejar la información en este entorno y las ventajas que daría a los competidores acceder a esta, estos casos se basan en la posible filtración de información de patrocinadores, líderes y agendas que pueden relacionar la campaña con aliados con una posible reputación negativa o intereses particulares que serían vistos por los electores como falta de integridad ocasionando un descenso en su imagen; otro riesgo crítico es para un caso particular que se puede presentar previamente a las elecciones para un candidato independiente que se desea inscribir por firmas y pierda los formularios donde están registrados lo que causaría su no registro para las elecciones, los últimos dos riesgos de esta categoría son relacionados con la integridad debido al uso de las redes sociales y son el caso en que un atacante tome el control de la cuenta del candidato difundiendo información falsa o privada que pueda afectar la campaña y el de las noticias falsas difundidas por cuentas ajenas que como se ha evidenciado a lo largo del documento tiene un efecto muy negativo.

Tabla 13. Mapa de Riesgos



ANEXO 4

8.4 Plan de Tratamiento de Riesgos

Teniendo en cuenta los resultados del registro de riesgos de la tabla 12 se da paso a la elaboración del producto final el cual corresponde al plan de tratamiento de riesgos para lo cual se proponen primero las contramedidas responsables de mitigar los riesgos identificados y finalmente de elaboradas la propuesta de controles se define el plan de implementación de estos.

8.4.1 Controles

Al analizar los resultados de la evaluación del riesgo se encuentra que todos deben ser tratados ya que superan el nivel de riesgo aceptable definido ubicado en bajo, por lo tanto siguiendo las condiciones establecidas por el estudio previo del proyecto para usar medidas con un enfoque administrativo y siguiendo las sugerencias del anexo A de la norma ISO 27001 se presentan las salvaguardas seleccionadas en la tabla 14 anexándolas al registro de riesgos del numeral anterior.

Tabla 14. Registro de Riesgos con Controles

ID Riesgo	Activo	Descripción Riesgo	Impacto	Probabilidad	Nivel Riesgo	Propietario	Controles
RC01	Contabilidad	Sanción por infringir la ley de transparencia por pérdida de la contabilidad.	A	M	A	Contador	1. Política de Confidencialidad 2. Política BYOD 3. Cifrado 4. Política de Backup
RC02		Pérdida de confianza de patrocinadores por filtración de donaciones.	A	M	A		1. Política de Confidencialidad 2. Política BYOD 3. Cifrado
RC03		Afectación de imagen de candidato por revelación de patrocinadores de mala reputación.	A	A	C		1. Política de Confidencialidad 2. Política BYOD 3. Cifrado
RC04		Campaña queda en desventaja estratégica debido a que la competencia conoce su bajo presupuesto.	A	M	A		1. Política de Confidencialidad 2. Política BYOD 3. Cifrado
RA01	Agenda	Afectación de imagen de candidato por filtración de reunión con aliado de mala reputación.	A	A	C	Responsable de Agenda	1. Política de Confidencialidad 2. Política BYOD
RA02		Perdida de patrocinio debido a sabotaje a reunión con patrocinadores.	A	M	A		1. Política de Confidencialidad 2. Política BYOD
RA03		Atentado a la integridad Física del candidato.	A	M	A		1. Política de Confidencialidad 2. Política BYOD
RA04		Candidato no asiste a presentación por extravío de agenda.	M	M	M		1. Software de agenda

RV01	Registro Votantes	Se detiene operación de estrategia de comunicación de campo por eliminación de archivo de registro.	A	M	A	Coordinador de Campo	1. Política de Confidencialidad 2. Política BYOD 3. Cifrado 4. Política de Backup
RV02		Suspensión de proceso de registro de votantes por infringir ley de protección de datos.	A	M	A		1.Política de tratamiento de datos personales 2. Política de Confidencialidad 3. Política BYOD
RV03		Candidato no puede inscribir su postulación por firmas por perdida de formularios.	A	A	C		1. Política de Confidencialidad
RL01	Lista Lideres	Pérdida de votos debido a que campaña opositora se roba los lideres porque tuvo acceso a la lista.	A	A	C	Director Político	1. Política de Confidencialidad 2. Política BYOD 3. Cifrado
RL02		Imagen desfavorable por filtración de alianzas con líderes de mala reputación.	A	M	A		1. Política de Confidencialidad 2. Política BYOD 3. Cifrado
RE01	Información estratégica no documentable	Afectación de imagen de candidato por filtración de mensajes privados por robo de dispositivo.	A	M	A	Niveles Altos	1. Protocolo comunicación estratégica no documentable 2. Política BYOD
RE02		Afectación de imagen de candidato por filtración de información por hackeo de dispositivo.	A	B	M		1. Protocolo comunicación estratégica no documentable 2. Política BYOD
RE03		Afectación de imagen de candidato por filtración de mensajes por técnica de Shoulder surfing.	A	M	A		1. Protocolo comunicación estratégica no documentable 2. Política BYOD
RE04		Afectación de imagen de candidato por filtración de información por cuenta de correo hackeada.	A	M	A		1. Protocolo comunicación estratégica no documentable 2. Política de confidencialidad 3. Política de email 4. Política de contraseñas 5. Política BYOD
RE05		Afectación de imagen de candidato por filtración de grabaciones de llamadas.	A	M	A		1. Protocolo comunicación estratégica no documentable
RR01	Imagen en Plataformas Electrónicas	Afectación de imagen de candidato por publicaciones falsas a través de su cuenta original.	A	A	C	Director de Comunicación	1. Política de redes sociales 2. Política de contraseñas 3. Política BYOD
RR02		Disminución de popularidad por circulación de noticias falsas.	A	A	C		1. Protocolo noticias falsas
RR03		Se detiene operación de promoción en redes por perdida de credenciales de acceso por renuncia de administrador de la plataforma.	A	M	A		1. Política de redes sociales
RCM01	Estrategia de Comunicación	Pérdida de productividad por eliminación de documentos estratégicos.	M	M	M	Director de Comunicación	1. Política de Backup
RCM02		Campaña queda en desventaja ante sus competidores por filtración de información estratégica	M	A	A		1. Política de Confidencialidad 2. Política BYOD

		almacenada en medios digitales					
RCM03		Campaña queda en desventaja ante sus competidores por filtración de información estratégica almacenada en medios físicos.	M	A	A		1. Política de Confidencialidad

Como se puede observar en la tabla un mismo control se puede aplicar a varios riesgos debido a que al ser de base administrativo como políticas tienen una cobertura más transversal; en el apartado siguiente se presentan los controles elegidos, la persona designada como propietario del riesgo debe velar por que se cumplan las disposiciones de las medidas a implementar en el activo de información del cual se destinó como propietario.

8.4.1.1 Política de Confidencialidad

Por la que se dispone la clasificación y manejo de información categorizada como crítica y que no debe ser conocida por agentes externos a la campaña electoral.

Este documento solo debe ser conocido por las personas autorizadas para manipular información categorizada como confidencial; la información que debe cumplir con este lineamiento es la contabilidad, la agenda, el registro de votantes, la lista de líderes y la estrategia de comunicación.

Los autorizados a acceder a cada activo son:

Contabilidad: Contador, candidato, director de campaña y director Financiero.

Agenda: Candidato, director financiero, director de comunicación, director de campaña y director político.

Registro Votantes (Digital): Coordinador de Campo y Administrador TI, se comparte esta información con otros directores de necesitarse para estrategias de comunicación siguiendo los lineamientos aquí dispuestos y con autorización del director de campaña o el candidato.

Lista de Lideres: Director Político, Director de Campaña y Candidato.

Estrategia de Comunicación: Director de Comunicación, Director de Campaña y Candidato se comparte esta información de necesitarse para estrategias de comunicación siguiendo los lineamientos aquí dispuestos y con autorización del director de campaña o el candidato.

8.4.1.1.1 La clasificación de la información confidencial se divide en dos niveles N1 y N2 donde N1 es la información que debe estar en estado cifrado, como se dispone en el protocolo de cifrado, y N2 la información confidencial que puede permanecer en texto plano pero siguiendo las condiciones aquí dispuestas; hacen parte de N1

la contabilidad, el registro de votantes y la lista de líderes; N2 cobija a la agenda y estrategias de comunicación.

8.4.1.1.2 Información clasificada solo puede transmitirse a las personas autorizadas para su acceso en formato digital en estado cifrado o plano de acuerdo a su nivel de clasificación a través del email oficial de la campaña como lo dispone la política de email; en el caso del registro de votantes el cual es necesario para varias dependencias de estrategias de promoción, publicidad e información entre otras, el propietario de este activo a solicitud de las otras partes y con la debida autorización del candidato o director de campaña podrá enviar la información a las partes solo fragmentada, es decir, si se requiere para comunicaciones vía línea telefónica solo se enviara los datos del número del teléfono, si otra parte necesita informar vía correo electrónico el propietario solo enviara los campos referentes al email.

8.4.1.1.3 Solo deben ser impresos en casos necesarios autorizados por el director de campaña o el candidato y cuando ya no sea de utilidad en ningún caso debe usarse como papel de reciclaje y se debe destruir de manera tal que quede ilegible.

8.4.1.1.4 Información en estado físico como los formularios de registro de votantes deben estar en un contenedor seguro protegido con llave como por ejemplo un archivador metálico, la llave la cual debe tener un duplicado la debe administrar el propietario del riesgo como se define en la tabla 14 y todos los duplicados los debe almacenar de manera segura el director de campaña; si el lugar de almacenamiento es un local de la campaña el contenedor debe estar ubicado en un recinto al interior de este que no posea ventanas hacia al exterior y que tenga una puerta segura que permanezca con llave la cual debe manejar el administrador del local y el director de campaña, el recinto debe estar aislado de filtraciones de agua y debe tener un elemento de extinción de incendios.

El no cumplimiento de los lineamientos aquí dispuestos resultara en expulsión de la campaña electoral y terminación inmediata de la relación contractual que se posea, si es el caso, además de la respectiva denuncia a la autoridad competente de presentarse alguna consecuencia negativa causada por su no adecuada aplicación.

8.4.1.2 Política BYOD (Bring Your Own Divice)

Por medio de la cual se definen los requerimientos y configuraciones de los dispositivos electrónicos de comunicación y procesamiento de información como tabletas, teléfonos inteligentes y computadores personales que son de propiedad de las personas involucradas con la campaña; fundamentándose en que las campañas políticas tienen un modo de funcionamiento distribuido, es decir, que el trabajo se hace en campo y por sus características únicas de movilidad, tiempo y presupuesto las tecnologías de información usadas son aportadas por cada individuo, o sea que las campañas de presupuesto ajustado no adquieren equipos

para sus integrantes, por lo que se hace necesario reglamentar su uso para prevenir incidentes adversos hacia la seguridad de la información.

Los lineamientos generales aquí dispuestos deben ser conocidos y cumplidos por todo el personal adscrito a la campaña que procese, transmita y almacene información relacionada a esta, desde el candidato y cargos directivos hasta voluntarios; el administrador TI será el responsable de verificar las condiciones aquí formuladas.

8.4.1.2.1 Lineamientos Generales

Regulaciones generales que deben aplicar todos los individuos cobijados por la presente política; todas las tareas sobre la información relativa a la campaña deben hacerse a través de los equipos aquí dispuestos y en ningún caso utilizar equipos de terceros.

8.4.1.2.1.1 Los dispositivos móviles como tabletas y teléfonos no pueden tener modificación de su sistema operativo original por lo que para el caso de Android el sistema no puede estar rooteado y en Apple no puede tener jailbreak.

8.4.1.2.1.2 Los dispositivos móviles deben solicitar pin de acceso para desbloquearlo y se deben bloquear automáticamente por inactividad de un (1) minuto.

8.4.1.2.1.3 Los computadores personales deben tener el sistema operativo original licenciado y solo se permite versiones que cuenten con soporte a la fecha de realización de este documento como para el caso de Windows se permite desde la 7 hasta la más actual; no se puede incluir equipos con sistemas operativos Windows Xp y Vista.

8.4.1.2.1.4 Los computadores personales deben habilitar usuario y clave de inicio de sesión del sistema operativo.

8.4.1.2.1.5 Las operaciones que deban realizarse a través de internet que sean relativas a las actividades de campaña deben hacerse a través de redes seguras ya sea la red de datos personal, la del hogar o la dispuesta por la campaña en su local central, de darse el caso; en ningún motivo se podrá realizar este tipo de actividades a través de redes abiertas como las de centros comerciales, aeropuerto, restaurantes, entre otras.

8.4.1.2.1.6 No descuidar los equipos móviles y computadores personales en lugares públicos para evitar su acceso no autorizado o robo.

8.4.1.2.1.7 Todas las contraseñas que sean usadas en las regulaciones de esta política que así lo requieran deben cumplir con la política de contraseñas.

8.4.1.2.1.8 Todos los equipos de cómputo deben ser protegidos con programa antivirus del cual se recomienda el uso en sistemas operativos Windows de su antivirus propio (Security Essentials) ya que es gratuito y no consume muchos recursos en versiones del sistema 8 y 10 viene por defecto; en ningún caso se debe ejecutar más de una solución de antivirus al mismo tiempo y el programa a instalar debe ser original licenciado.

8.4.1.2.1.9 No se permite el uso de dispositivos de almacenamiento USB, la trasferencia de archivos relativos a la campaña entre partes autorizadas debe realizarse a través de las cuentas de correo asignadas para tal fin.

8.4.1.2.1.10 Equipos móviles y computadores deben tener activo actualizaciones de sistema automático con una periodicidad de revisión diaria con el fin de proteger las fallas de seguridad que se van generando.

8.4.1.2.1.11 Los computadores personales deben entrar en estado de suspensión por inactividad pasados cinco (5) minutos y deben solicitar las credenciales de inicio de sesión al reanudarse.

8.4.1.2.2 Lineamientos Información Clasificada

Regulaciones que deben ser aplicadas adicionalmente a las presentadas en los lineamientos generales a los dispositivos del personal que almacena y procesa información clasificada como confidencial de los niveles N1 y N2 como se dispone en la política de confidencialidad (8.3.1.1); estos lineamientos específicos solo deben ser socializados con el personal que tiene acceso a esta categoría de información y el administrador TI que brindara apoyo en las tareas de verificación, configuración, instalación y capacitación.

8.3.1.2.2.1 Los computadores personales deben tener bloqueo de arranque con contraseña de BIOS.

8.3.1.2.2.2 Los dispositivos móviles deben tener instalado un protector de pantalla anti espía el cual es una capa de cristal que solo permite la visibilidad desde una ubicación al frente del equipo con el fin de evitar técnicas de shoulder surfing, es decir, filtración de información por acceso visual al equipo al ser operado por su propietario.

8.3.1.2.2.3 No usar dispositivos móviles con sistemas operativos desatendidos, es decir que para la fecha de realización de este documento solo se permite el uso de dispositivos iPhone con modelo 5s o posteriores y para Android desde 2.4 o superiores.

8.3.1.2.2.4 Los dispositivos móviles y equipos de cómputo solo deben tener instaladas las aplicaciones y programas necesarios para el desarrollo de las actividades propias de la campaña y deben provenir de las fuentes originales.

8.3.1.2.2.5 En equipos móviles Android se debe activar el cifrado de dispositivo para proteger la información contenida, esta tarea no es necesaria en iPhone ya que viene activa por defecto al bloquear su acceso con pin.

8.3.1.2.2.6 Desactivar o no aceptar recordar contraseñas al acceder a las cuentas de aplicaciones que el usuario utilice para el desempeño de sus actividades de campaña.

El no cumplimiento de los lineamientos aquí dispuestos resultara en expulsión de la campaña electoral y terminación inmediata de la relación contractual que se posea, si es el caso, además de la respectiva denuncia a la autoridad competente de presentarse alguna consecuencia negativa causada por su no adecuada aplicación.

8.4.1.3 Política de Email

Por la cual se propone y reglamenta la administración y uso de cuentas de correo electrónico para el personal de campaña que por su interacción con la información de campaña así lo requiera.

Los lineamientos aquí dispuestos deben ser conocidos y cumplidos por todo el personal adscrito a la campaña que procese, transmita y almacene información relacionada y que para tal fin necesite una cuenta de correo de la campaña, a excepción de los que estén dirigidos a personal con acceso a información confidencial; el administrador TI será el responsable de apoyar y verificar las condiciones aquí formuladas.

8.3.1.3.1 Todos los usuarios que requieran transmitir información de campaña se les deben crear una cuenta de correo en el mismo proveedor con un formato general que indique que pertenece a la campaña. Ej. nombre.campaña@gmail.com con método de recuperación a través del número de teléfono móvil.

8.3.1.3.2 Al momento de crear las cuentas por facilidad el administrador TI debe generar una clave estándar relacionada con la cedula del usuario el cual debe cambiar la contraseña al primer inicio de sesión cumpliendo con las políticas de contraseñas.

8.3.1.3.3 Se debe acceder a las cuentas de correo de campaña solo desde los dispositivos personales propios abarcados en la política BYOD (8.3.1.2) y no de terceros y siempre ingresar digitando la dirección de internet del proveedor de servicios en la barra de direcciones del navegador y no desde enlaces externos.

8.3.1.3.4 Las cuentas solo deben ser usadas para actividades relativas a la campaña electoral.

8.3.1.3.5 No se debe proporcionar la cuenta de correo para registrarse en otras plataformas o solicitudes de información que no estén relacionadas con la campaña.

8.3.1.3.6 No se debe abrir correos de remitentes desconocidos con asuntos sospechosos y que no tengan relación con la campaña y se prohíbe acceder a los vínculos, enlaces o archivos adjuntos que estos contengan; este lineamiento se debe atender para todas las cuentas de correo que maneje el usuario desde sus dispositivos personales ya que cualquier incidente por su mal uso puede afectar la información de campaña almacenada en el equipo.

8.3.1.3.7 No se debe habilitar o acceder a que se recuerde la contraseña en un ningún dispositivo, es decir, se debe ingresar usuario y contraseña cada vez que se inicie sesión.

8.3.1.3.8 Cuentas de usuarios que están en la categoría de autorizados a acceso a información confidencial (8.3.1.1) deben tener activa la verificación de dos pasos para acceder a la cuenta de correo a través del uso de la contraseña y el envío de un código a su teléfono móvil personal.

8.3.1.3.9 Cerrar sesión cada vez que se deje inactiva la cuenta.

8.3.1.3.10 Se debe ingresar directamente a las cuentas de correo desde la barra de direcciones del navegador digitando la dirección web exacta; en ningún caso se debe proporcionar usuario y contraseña ingresando desde un enlace externo por ejemplo de un correo electrónico o cualquier otro sitio.

Se recomienda G-Suite de Google si se requiere una administración más controlada por un costo anual aproximado de $150.000 para poder gestionar de manera centralizada creación de cuentas, definición de políticas de contraseñas, accesos, cifrado, forzar cambio de contraseña, entre otros; con el objetivo de que las políticas acá dispuestas tengan un mayor grado de cumplimiento por los usuarios.

El no cumplimiento de los lineamientos aquí dispuestos resultara en expulsión de la campaña electoral y terminación inmediata de la relación contractual que se posea, si es el caso, además de la respectiva denuncia a la autoridad competente de presentarse alguna consecuencia negativa causada por su no adecuada aplicación.

8.4.1.4 Política de Tratamiento de Datos Personales

Por la cual se definen los lineamientos en cuanto a la recolección, administración y manejo de datos personales de los cuales hacen parte los registros de votantes en sus formatos físicos y digitales ya que la información reunida en estos hace parte de esta categoría y de darse un uso inapropiado podría infringir la ley de protección de datos pudiendo ocasionar la suspensión de dicha actividad la cual es esencial

para planes de comunicación y promoción del candidato, siendo también una tarea fundamental para la inscripción de un candidato independiente por firmas.

Los lineamientos aquí dispuestos deben ser conocidos y cumplidos por todo el personal adscrito a procesos de registro de votantes, digitalización, almacenamiento y su administración y por todos los usuarios quienes por las funciones asignadas deban acceder a dicha información.

8.3.1.4.1 Todos los formularios físicos de registro de votantes deben contener un parágrafo en un lugar visible donde se especifique que el propietario de los datos al firmar el registro acepta el uso y la política de tratamiento de datos personales de la campaña política.

8.3.1.4.2 Se debe formular **l**a política de tratamiento de datos la cual debe ser publicada en algún recurso en línea como red social, blog, página web o aquel que la campaña disponga y que sea accesible a los titulares de los datos; la dirección e indicaciones de ingreso deben estar presentes en el parágrafo del numeral anterior (8.3.1.4.1).

8.3.1.4.3 El propósito de la recolección de datos debe ser plasmado en la política enunciando que la función del tratamiento de datos es para fines estadísticos, informativos y de promoción de la campaña política.

8.3.1.4.4 La política debe indicar el canal de comunicación para que el titular pueda conocer, actualizar o hacer alguna reclamación sobre sus datos con previa identificación para lo cual se recomienda que sea a través del email de campaña del administrador TI ya que este es el responsable de administrar dichos registros en su estado digital, el titular para la solicitud debe adjuntar fotocopia de su cedula de ciudadanía para verificar que sea el propietario, se debe tener en cuenta que el plazo para responder las solicitudes no puede superar los 15 días hábiles; cabe anotar que el titular de los datos puede solicitar su eliminación en cualquier momento siguiendo el canal descrito.

8.3.1.4.5 La información del registro de votantes digital debe cumplir con la política de confidencialidad N1 (8.3.1.1) y el protocolo de cifrado, en su estado físico debe cumplir con el lineamiento también contenido en la política de confidencialidad específicamente del numeral (8.3.1.1.4); esto con el fin de proporcionar seguridad en cuanto a los aspectos de confidencialidad, integridad y disponibilidad.

8.3.1.4.6 Los equipos de campo responsables de registrar los votantes deben llevar unas pocas copias impresas de la política de tratamiento de datos en caso tal de que alguna persona la solicite.

El no cumplimiento de los lineamientos aquí dispuestos resultara en expulsión de la campaña electoral y terminación inmediata de la relación contractual que se posea, si es el caso, además de la respectiva denuncia a la autoridad competente de presentarse alguna consecuencia negativa causada por su no adecuada aplicación.

8.4.1.5 Política de Contraseñas

Por la cual se definen los lineamientos en cuanto a la creación y administración de contraseñas de usuarios para acceso a las cuentas de las plataformas electrónicas dispuestas para realizar sus funciones asignadas por la campaña política.

Los lineamientos generales aquí dispuestos deben ser conocidos y cumplidos por todo el personal adscrito a la campaña que procese, transmita y almacene información a través de las plataformas electrónicas como correo electrónico y redes sociales asignadas por la campaña.

8.3.1.5.1 La contraseña debe tener una longitud mínima de 10 caracteres, debe contener una combinación de números, letras en minúscula y mayúscula, números y caracteres especiales.

8.3.1.5.2 La metodología para su formulación se debe hacer a través de la aplicación de una frase de contraseña en la cual no se puede relacionar información personal del usuario como fechas de cumpleaños y nombres propios o de familiares, no puede llevar espacios, cada palabra inicia con mayúscula y se deben cambiar las letras que apliquen a números y caracteres especiales, para dar aclaración se muestra un ejemplo usando el nombre de una película, que sea recordable por el usuario, como frase de contraseña, el nombre original es “La Delgada Línea Roja” la contraseña resultante es “L@D3lg@d@L¡n3@R0j@”, nótese que la longitud es de 18 caracteres, se eliminan los espacios entre palabras, la “a” se cambia por “@”, la “e” por “3”, la “i” por “¡” (signo de admiración) y la “o” por “0” y cada palabra inicia con mayúscula.

8.3.1.5.3 La contraseña se debe cambiar si algún incidente de seguridad ocurre que pueda vulnerar las cuentas o a los 6 meses de su uso lo que quiere decir que para un periodo de una campaña se cambiaría solo una vez, el administrador TI debe enviar un mensaje por las cuentas de correo oficiales de la campaña solicitando el cambio; de usarse una plataforma de administración de cuentas se forzara su cambio en las condiciones descritas.

8.3.1.5.4 No se deben escribir las contraseñas en algún papel o archivo digital para su recordación.

8.3.1.5.5 En ningún caso se permite comunicar la contraseña a otro usuario para que un tercero ingrese a la cuenta asignada.

8.3.1.5.6 Se debe usar una contraseña diferente para cada servicio o cuenta necesaria para el desarrollo de las funciones de cada usuario.

El no cumplimiento de los lineamientos aquí dispuestos resultara en expulsión de la campaña electoral y terminación inmediata de la relación contractual que se posea, si es el caso, además de la respectiva denuncia a la autoridad competente de presentarse alguna consecuencia negativa causada por su no adecuada aplicación.

8.4.1.6 Política de Backup

Por la cual se definen los lineamientos en cuanto a la creación y administración de las copias de seguridad de los archivos que sean cobijados por esta medida.

Esta política cobija los activos de información de contabilidad, registró votantes y documentos de la estrategia de comunicación y debe ser socializada para los propietarios de dichos activos solamente; se contara con el apoyo en capacitación de los usuarios del administrador TI.

8.3.1.5.1 Para las copias de seguridad se utiliza herramientas de almacenamiento en la nube como Dropbox, Onedrive o Google Drive, entre otras.

8.3.1.5.2 La condición para escoger el servicio de alojamiento en la nube radica en la cuenta elegida para la creación de los correos electrónicos oficiales, en ningún caso las cuentas de correo y de alojamiento serán de la misma organización con el fin de que en el caso de verse comprometida una cuenta no se pueda acceder a la otra.

8.3.1.5.3 Se debe subir al servicio de alojamiento una copia de seguridad cada semana o cuando haya un cambio o modificación representativa en el archivo.

8.3.1.5.4 Se deben mantener dos copias de seguridad de los activos, la última subida y la de la semana inmediatamente anterior, los registros anteriores a esos se deben eliminar en aras de no sobrepasar los límites de los servicios de alojamiento gratuito; en caso de requerir más capacidad de almacenamiento se debe cancelar una suma económica.

8.3.1.5.5 No se debe habilitar la función de sincronización automática de las copias de seguridad directamente con las carpetas alojadas en el equipo del propietario debido a que si se elimina en esta también se elimina en la nube.

8.3.1.5.6 Cuentas de usuarios que están en la categoría de autorizados a acceso a información confidencial (8.3.1.1) deben tener activa la verificación de dos pasos para acceder a través del uso de la contraseña y el envío de un código a su teléfono móvil personal.

8.3.1.5.7 La información catalogada como confidencial N1 debe ser alojada en estado cifrado como lo dispone la política de confidencialidad (8.3.1.1) y siguiendo los lineamientos del protocolo de cifrado.

8.3.1.5.8 Se debe ingresar directamente a las cuentas de backup desde la barra de direcciones del navegador digitando la dirección web exacta; en ningún caso se debe proporcionar usuario y contraseña ingresando desde un enlace externo por ejemplo de un correo electrónico o cualquier otro sitio.

El no cumplimiento de los lineamientos aquí dispuestos resultara en expulsión de la campaña electoral y terminación inmediata de la relación contractual que se posea, si es el caso, además de la respectiva denuncia a la autoridad competente de presentarse alguna consecuencia negativa causada por su no adecuada aplicación.

8.4.1.7 Política de Redes Sociales

Por la cual se definen los lineamientos en cuanto a la administración de las cuentas de redes sociales usadas para la promoción del candidato y la campaña.

Los lineamientos aquí establecidos deben ser socializados únicamente con el responsable de la administración de las redes sociales, el director de comunicación y el candidato o en su defecto el director de campaña, se contara con el apoyo en capacitación del administrador TI.

8.3.1.7.1 Al momento de crear las cuentas en las redes sociales se debe ingresar como correo de recuperación de contraseña el del candidato, el número telefónico ingresado si debe ser el del administrador de la red social; la contraseña debe cumplir con lo requerido en la política de contraseñas y debe ser solo conocida por el administrador TI y el candidato

8.3.1.7.2 Todas las plataformas de redes sociales deben tener doble factor de autenticación usando contraseña y envío código al teléfono móvil del administrador TI y se deberá solicitar cada vez que se ingrese a la plataforma.

8.3.1.7.3 Se debe acceder a las cuentas de redes sociales oficiales de campaña solo desde los dispositivos personales propios abarcados en la política BYOD (8.3.1.2) y no de terceros y siempre ingresar digitando la dirección de internet del proveedor de servicios en la barra de direcciones del navegador y no desde enlaces externos.

8.3.1.7.4 No se debe habilitar o acceder a que se recuerde la contraseña en un ningún dispositivo, es decir, se debe ingresar usuario y contraseña cada vez que se inicie sesión.

8.3.1.7.5 Cerrar sesión cada vez que se deje inactiva la cuenta.

8.3.1.7.6 No se debe hacer clic en enlaces externos de fuentes desconocidas

8.3.1.7.7 No abrir mensajes de fuentes no fiables o personas desconocidas

8.3.1.7.8 No descargar archivos adjuntos enviados por mensajes a través de las redes sociales.

8.3.1.7.9 No autorizar aplicaciones de terceros en la cuenta de redes sociales a no ser de que sea completamente necesaria para las funciones de promoción del candidato, revisando previamente que sea de una fuente fiable y que los permisos que solicita no invadan la información privada ahí contenida como contactos y fotos.

8.3.1.7.10 De darse el caso en que se retire el administrador de la cuenta de la red social se debe cambiar la contraseña restaurándola con el correo proporcionado el cual es propiedad del candidato y a su vez modificar el número de teléfono al del nuevo responsable.

8.3.1.7.11 Se debe ingresar directamente a las cuentas de redes sociales desde la barra de direcciones del navegador digitando la dirección web exacta; en ningún caso se debe proporcionar usuario y contraseña ingresando desde un enlace externo por ejemplo de un correo electrónico o cualquier otro sitio.

8.3.1.7.12 Se deben publicar y socializar por los medios electrónicos disponibles de la campaña como web, blog, email, mensajería instantánea y por las mismas redes sociales las direcciones de las páginas oficiales de redes sociales asociadas a la campaña.

8.3.1.7.13 Si el candidato ya posee cuenta de redes sociales de uso familiar deshabitarla en el tiempo de la campaña, si de lo contrario su cuenta ya posee un cantidad importante de seguidores y se desea usar como la oficial se debe revisar y eliminar toda información privada o publicaciones que puedan afectar su imagen; cabe anotar que esta cuenta también debe cumplir los lineamientos anteriormente descritos.

El no cumplimiento de los lineamientos aquí dispuestos resultara en expulsión de la campaña electoral y terminación inmediata de la relación contractual que se posea, si es el caso, además de la respectiva denuncia a la autoridad competente de presentarse alguna consecuencia negativa causada por su no adecuada aplicación.

8.4.1.8 Protocolo Cifrado

Se dispone los lineamientos e instrucciones para el manejo de información clasificada como confidencial N1 que debe estar cifrada, para tal fin se hace uso de herramientas incluidas en los paquetes de ofimática de Microsoft ya que están disponibles en la mayoría de computadores personales con la finalidad de que sean apropiadas por cualquier tipo de usuario y no incurrir en gastos adicionales ya que este proyecto considera como base un presupuesto ajustado.

Este protocolo se aplica a los activos información referentes a la contabilidad, el registro de votantes y lista de líderes los cuales están clasificados como N1; estos registros se procesaran usando Excel y los lineamientos aquí contenidos se deben socializar solamente al personal autorizado a acceder a información confidencial N1 y el administrador TI será el responsable de apoyar y verificar las condiciones aquí formuladas.

i. Las versiones aceptadas de Microsoft Office para aplicar este protocolo son la 2007, 2010, 2013 o superiores, en ningún caso se puede proteger los documentos con versiones previas ya que son vulnerables

ii. El cifrado para el documento de Excel en versiones 2007 o superiores se realiza después de abierto el documento seleccionando el menú superior “Archivo” > Información > Proteger Libro > Cifrar con Contraseña, se ingresa la contraseña con las condiciones dadas en la política de contraseñas dispuestas en (8.3.1.5); después de creada la contraseña se guarda el documento.

iii. Para abrir el archivo cifrado se da doble clic sobre este y se ingresa la contraseña asignada en el campo requerido.

iv. El propietario del activo tal como se enuncia en la tabla 8 es el responsable de crear la contraseña y mantenerla secreta, se debe ser cuidadoso con esta ya que si se olvida el documento no podrá recuperarse.

v. Para el registro de votantes en formato digital aunque el propietario es el coordinador de campo normalmente el responsable de administrarlo es el administrador TI, en ese caso el responsable de asignar la contraseña es este último.

vi. Teniendo en cuenta el riesgo de la pérdida de un archivo por olvido de contraseña se establece un procedimiento para tener una alternativa de recuperación escribiendo la contraseña del archivo original en otro documento de Excel y cifrarlo con la contraseña asignada a la cuenta de email; este archivo no se debe almacenar en el equipo del propietario del activo y no se le debe asignar un nombre que lo relacione con su funcionalidad por lo tanto debe reposar en el lugar de almacenamiento que disponga aplicando la política de Backup.

vii. En caso de que alguno de estos activos de información sea requerido por personal de alto nivel el cual tiene privilegios de acceso a toda la información como el candidato o director de campaña se genera una copia del documento con una clave diferente cumpliendo con lo dispuesto en la política de contraseñas y siguiendo los pasos anteriormente descritos para tal fin; se enviara el documento cifrado a través de las cuentas de correo oficiales y la clave será enviada al destinatario mediante el protocolo de comunicación estratégica no documentable la cual debe ser memorizada.

8.4.1.9 Protocolo Comunicación Estratégica no documentable

Este protocolo hace referencia a las herramientas necesarias para comunicar información de necesidad inmediata con fines estratégicos de campaña y que puede ser perjudicial de ser conocida por agentes externos como prensa o competencia con consecuencias como pérdida de ventaja o imagen, hasta afectaciones jurídicas para el candidato y campaña.

Este protocolo solo debe ser conocido por el candidato, director de campaña y quienes están autorizados a acceso a información confidencial y demás personas que el candidato o director cataloguen como fuentes o receptores de la información aquí contenida como por ejemplo asesores externos; el administrador TI brindara soporte para la aplicación de este protocolo.

i. No se debe comunicar este tipo de información a través de llamadas

ii. Se debe instalar la aplicación de mensajería instantánea *Signal* de Open Whisper Systems en cada uno de los dispositivos de los autorizados en este protocolo con el fin de ser el canal oficial para trasmitir este tipo de información; verificar que la fuente de instalación sea la original.

iii. Habilitar la eliminación automática de mensajes para todos los dispositivos, para los cuales los mensajes se eliminaran 1 hora después de ser recibidos por lo que los mensajes recibidos por este medio deben ser prioritarios para su lectura; los pasos para su habilitación y configuración se pueden consultar en la web del creador en la siguiente dirección: https://support.whispersystems.org/hc/en-us/articles/213134237-Does-Signal-have-disappearing-messages-.

iv. Por ningún motivo archivar comunicaciones de esta aplicación.

v. Siempre usar el plan de datos o redes seguras para el uso de esta aplicación.

vi. El administrador TI verificara que los dispositivos tengan la aplicación debidamente instalada y configurada con los términos aquí dispuestos.

8.4.1.10 Protocolo Noticias Falsas

Este protocolo hace relación a los pasos a seguir para aplicar técnicas y/o herramientas para contrarrestar los efectos de la publicación de noticias falsas por medios electrónicos principalmente en las redes sociales que puedan afectar la imagen del candidato y campaña.

Los lineamientos aquí establecidos deben ser socializados únicamente con el responsable de la administración de las redes sociales, el director de comunicación y el candidato o en su defecto el director de campaña, se contara con el apoyo en capacitación del administrador TI.

i. El administrador de redes sociales deberá estar atento en cuanto a identificar publicaciones falsas o contenido perjudicial para la campaña.

ii. En caso de detectar una publicación de este tipo deberá reportarla con las herramientas disponibles en cada red social; los pasos de reporte para twitter se disponen en esta dirección https://support.twitter.com/articles/20170486?lang=es y en Facebook https://www.facebook.com/help/181495968648557.

iii. El administrador de las redes debe estar pendiente cuando Facebook y google habiliten las herramientas de reporte de noticias falsas en Colombia para seguir la instrucciones ahí dispuestas ya que son medidas más efectivas que el reporte normal ya que deja marcada la publicación con una nota donde todo el que la vea le comunicara que posiblemente es falsa y le aportara las fuentes fiables para que el usuario lo verifique, mientras tanto se debe utilizar las herramientas anteriores.

iv. Se deben realizar campañas por las redes sociales sobre cómo identificar noticias falsas y como reportarlas con las guías aquí dispuestas, las campañas deben ser realizadas por el administrador pero deben ser apoyadas, enviadas y compartidas también por todos los voluntarios y partidarios de la campaña a través de sus cuentas personales en las redes sociales.

v. Los voluntarios y partidarios deben estar en capacidad para identificar y reportar publicaciones de esta categoría desde sus cuentas de usuario personales.

8.4.1.11 Software de Agenda

Con la finalidad de reducir riesgos en cuanto a acceso no autorizado y perdida a los cuales está expuesta una agenda en estado físico se propone el uso de una herramienta de calendario a través de dispositivos móviles ya que siempre estaría a la mano del candidato o su director de campaña y el responsable de agenda; para tal fin se propone la aplicación y uso de *Google Calendar* la cual es compatible con web, Android e iOS; se debe crear un calendario compartido entre el responsable de agenda y el candidato el cual será administrado por el primero pero visualizado

por los dos en los equipos personales que cumplen con la política de BYOD y deben estar asociados a sus correos oficiales de campaña; cabe anotar que su administración debe cumplir con las políticas relacionadas como la de confidencialidad.

Las instrucciones para el uso compartido de calendario las dispone su fabricante en el enlace https://support.google.com/calendar/answer/37082?hl=es-419.

8.4.2 Plan de Tratamiento de riesgos

Ya con todos los controles formulados se procede a describir el plan de tratamiento de riesgo el cual describe la implementación de los controles y se visualiza en la tabla 15.

Tabla 15. Plan de tratamiento de Riesgos

Control a Implementar	Relacionado a los riesgos	Responsable	Plazo	Recursos
Implementación Política Confidencialidad	RC01, RC02, RC03, RC04, RA01, RA02, RA03, RV01, RV02, RV03, RL01, RL02, RE04, RCM02	Director de Campaña	1 mes	1 hora
Implementación Política BYOD	RC01, RC02, RC03, RC04, RA01, RA02, RA03, RV01, RV02, RL01, RL02, RE01, RE02, RE03, RE04, RR01, RCM02	Administrador TI	1 mes	2 horas
Implementación Política Email	RE04	Administrador TI	1 mes	2 horas
Implementación Política Tratamiento datos personales	RV02	Coordinador de Campo	1 mes	4 horas
Implementación Política Contraseñas	RE04, RR01	Administrador TI	1 mes	1 hora
Implementación Política Backup	RCO1, RV01, RCM01	Administrador TI	1 mes	1 hora
Implementación Política Redes Sociales	RR01, RR03	Administrador TI	1 mes	1 hora
Socialización Protocolo de Cifrado	RC01, RC02, RC03, RC04, RV01, RL01, RL02	Administrador TI	1 mes	1 hora
Socialización Protocolo Comunicación Estratégica no documentable	RE01, RE02, RE03, RE04, RE05	Director de Campaña/ Administrador TI	1 mes	1 hora
Socialización Protocolo de Noticias Falsas	RR02	Administrador TI	1 mes	1 hora
Software de Agenda	RA04	Responsable de Agenda/Administrador TI	1 mes	1 hora

En la tabla se identifica el control a implementar y los riesgos a los que este se asocia; para este caso en particular la implementación de todos los controles

consiste en la socialización y capacitación para la debida aplicación de las políticas, protocolos y herramientas inmersas en estas; no se contempla la creación de estos porque ya están formulados como resultado del proyecto a excepción de la política de tratamiento de datos personales ya que hay que complementar la política que se va a publicar dado que la aquí presentada es la que proporciona los requisitos y recomendaciones a tener en cuenta en su formulación y aplicación.

La socialización y capacitación de estas políticas es función del rol que se designa en la casilla de responsable, para tal fin en el momento de que la campaña defina las personas encargadas de dichos roles se les debe proporcionar la información respecto al control que deben implementar para que puedan estudiarla y apropiarla; cabe aclarar que el responsable de la implementación del control es diferente al responsable del riesgo ya que este último es el que debe velar por que se dé el manejo de la información de acuerdo a los lineamientos de las políticas y protocolos que le aplican al activo de información bajo su cargo.

El plazo presentado para su implementación consiste en el tiempo que tiene el responsable para transmitir la información del control respectivo a los interesados para lo cual se fija un periodo de un mes contando desde el momento de definirse las personas que van a cumplir con los roles que conforman la campaña política en la fase de planeación es decir previo al inicio de la campaña legalmente; esta premura se basa en que cuando inicie la campaña todo lo respectivo a seguridad de la información ya este apropiado porque después de iniciada la etapa de ejecución de campaña el recurso temporal es muy escaso y lo que no se planeó antes de esto normalmente no se lleva acabo.

En lo correspondiente a los recursos, este se mide en el tiempo necesario aproximado para que el o los responsables de la implementación del control lo formalicen socializándolo e instruyendo al personal que esta cobijado por este para que se dé una correcta aplicación en el transcurso de la campaña.

Para llevar a cabo el plan de tratamiento de riesgos como esta propuesto se recomienda realizar dos jornadas de 8 horas cada una cuando ya la campaña tenga definido los roles y cargos más importantes invitando a las personas que están cobijadas, por esto con antelación se debe planear las capacitaciones agrupando controles que sean afines y que estén dirigidos al mismo público para así instruirlo en un mismo ciclo, por ejemplo tener en cuenta que políticas solo van dirigidas a los cargos de más alto nivel y que no debe ser conocida por nadie más, para agruparlos y exponerles la información, con este tema se debe ser muy cuidadoso para aplicar de manera correcta la técnica “Need to Know” que traduce necesidad de conocer y es que solo se le da a conocer este tipo de información a las personas que verdaderamente lo necesitan para desempeñar sus funciones de campaña, porque de lo contrario se estaría generando una debilidad en la protección de la información.

Cuando el control abarque una cantidad de usuarios muy amplia se capacita a los líderes de grupo para que estos a su vez repliquen la información a su equipo de trabajo.

En la capacitación se deben llevar asistencias firmadas por cada sesión de exposición de cada control con el fin de evidenciar que los implicados fueron informados de los lineamientos como de las repercusiones de su no cumplimiento.