ANALISIS DE RIEGOS DE SEGURIDAD DE LA INFORMACIÓN DETECTADOS EN EL SERVICIO DE GESTIÓN DE CREDITOS DEL PORTAL WEB DE LA ENTIDAD PÚBLICA ICETEX.

TRABAJO DE GRADO

ANA MARIA BETANCOURT ARANGO

CÓDIGO 1622010029

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

2017

ANALISIS DE RIEGOS DE SEGURIDAD DE LA INFORMACIÓN DETECTADOS EN EL SERVICIO DE GESTIÓN DE CREDITOS DEL PORTAL WEB DE LA ENTIDAD PÚBLICA ICETEX.

TRABAJO DE GRADO

ANA MARIA BETANCOURT ARANGO

CÓDIGO 1622010029

ASESOR: ALEJANDRO CASTIBLANCO CARO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Bogotá, Septiembre 2017

TABLA DE CONTENIDO

ANALISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DETECTADAS EN EL SERVICIO DE GESTIÓN DE CREDITOS DEL PORTAL WEB DE LA ENTIDAD PÚBLICA ICETEX.

1. RESUMEN EJECUTIVO

Las empresas que se desarrollan en el ámbito del gobierno Colombiano, están creadas y diseñadas para cumplir funciones claves para la buena administración, control y gestión de toda la información de las personas que conforman nuestro país. Estos procesos se ejecutan y se llevan a cabo por diferentes medios, uno de ellos son los servicios que se prestan a través de la web por servidores especializados para estas tareas. El problema surge cuando dichos servidores mencionados anteriormente, se encuentran vinculados a las bases de datos de la organización o a diferentes procesos fundamentales para la compañía. Un ataque exitoso que ingrese por medio del servicio web, podría generar pérdidas significativas y ocasionar problemas internos y externos de todo tipo.

Este proyecto toma como referencia al Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior – Icetex. Dicha entidad, perteneciente al gobierno Colombiano, enfoca sus esfuerzos como ente regulador y prestador de servicios de apoyo económico para la otorgación de créditos estudiantiles. Actualmente, cuentan con un portal web bajo el dominio de: www.icetex.gov.co [1], a través del mismo, prestan a sus miles de usuarios, servicios de gestión de créditos en línea.

Este proyecto, se basa en el estudio del entorno en el que se desarrolla el servicio de Gestión de Créditos del portal web del Icetex, lo anterior, está vinculado a la detección y análisis de los activos de tecnologías de la información y las comunicaciones que apoyan al servicio para su buen funcionamiento, una vez se analizan y estudian estos activos, se procede a generar una detección de posibles riesgos que puedan materializarse por medio de este servicio web y que logren afectar la confidencialidad, disponibilidad e integridad de la información.

Tiene como fase inicial, la comprensión y análisis del entorno en el que se desarrolla la entidad Icetex, sus partes interesadas y los actores o entidades que ejercen control sobre esta empresa. Se identifica el servicio de Gestión de Créditos y el contexto en el que este proceso se desarrolla.

Como segunda fase, se busca la detección de los activos ligados al proceso de Gestión de Crédito del portal web del Icetex, lo anterior, con el ánimo de realizar una búsqueda de los posibles riesgos que se detectan dentro de este servicio, se procede con la categorización de dichos riesgos bajo una medida de probabilidad por impacto legal, reputacional y operativo.

Como fase final, se plantean los controles que podrían aportar a la disminución de la probabilidad de que un riesgo se materialice dentro del servicio de Gestión de Créditos del portal web de la entidad,

Por último, como resultados esperados, se plantea una guía con los controles que se sugieren para el manejo de los riesgos encontrados dentro de los activos ligados a este proceso.

Con el fin de buscar la protección de la confidencialidad, integridad y disponibilidad de la información en el proceso de Gestión de Créditos del Icetex se toma como punto de partida la norma NTC/ISO 31000 para la gestión del riesgo con el fin de identificar, analizar, y evaluar los riesgos que pueden afectar el cumplimiento de los objetivos de la entidad [2].

Basados en esto, se plantean los procesos y aspectos más relevantes para lograr un adecuado análisis de los riesgos que se detecten dentro del proceso de Gestión de Crédito del portal web del Icetex.

- Establecimiento del contexto: Se enfoca en conocer el mapa de procesos y el funcionamiento interno que tienen la entidad orientado en el área de las tecnologías de la información y las comunicaciones, se establecen los principales roles y funciones de las personas encargadas de los procesos y tareas que apoyan al proceso de seguridad de la información.

- Identificación de activos: Se establecen los activos que están ligados al servicio de Gestión de Créditos del portal web del Icetex, se define el líder del activo, los custodios que pueden tener dominio del mismo, el contenedor que encapsula la información del activo, etc.

- Identificación del riesgo: Teniendo en cuenta los activos detectados, se realiza una identificación de las posibles amenazas que pueden materializarse y convertirse en un riesgo para el activo de la información.

- Análisis del riesgo: Se definen dos características para poder continuar con la valoración del riesgo. La probabilidad de que el riesgo se materialice basado en medida de tiempo y el impacto legal, reputacional u operacional que pueda tener el riesgo basado en medida monetaria.

- Evaluación del riesgo: Se plantean los posibles controles y la efectividad que los mismos puedan tener para la reducción de la probabilidad de que un riesgo se materialice.

- Tratamiento del riesgo: Se plantean con el ánimo de generar un plan de seguimiento a los controles definidos para los riesgos detectados, lo anterior para facilitar la administración de los riesgos que fueron detectados dentro del proceso de análisis del sistema de Gestión de Crédito del portal web del Icetex.

Este proyecto de grado, tienen como resultado 6 entregables que encapsulan todo el desarrollo de la aplicación de la norma NTC/ISO 31000, en ellos, se detalla todo el contexto en el que se desarrolla el sistema de Gestión de Crédito del portal web del Icetex. Se tiene

como resultado, los riesgos detectados dentro del proceso y los controles que se sugieren para la disminución de la afectación de la confidencialidad, integridad y disponibilidad de la información.

En este trabajo se estudia el servicio de gestión de créditos que se maneja por cada uno de los usuarios del Icetex a través de su portal web, se detectaran los activos de seguridad de la información asociados a dicho servicio, con el fin de plantear posibles riesgos y brechas de seguridad de la información. Basados en la norma NTC/ISO 31000 para la gestión del riesgo se identificaran, analizaran, y evaluaran los riesgos que pueden afectar al servicio de gestión de créditos del Icetex. Se creara un plan de tratamiento de riesgos basado en controles de seguridad informática que logren disminuir la probabilidad de que un riesgo se materialice.

2. JUSTIFICACIÓN

Los servidores web son un objetivo atractivo para los hackers y ciber delincuentes que por diferentes razones buscan afectar la disponibilidad, integridad y confidencialidad de la información de estos servicios, si se habla del sector gobierno los ataques por parte de estos delincuentes se incrementan de manera notoria, ya sea por cuestiones políticas, éticas o económicas, son mayores las razones que se encuentran por parte de externos para atacar este tipo de servicios. Estos ataques se presentan a diario y es por eso que cobra importancia realizar evaluaciones oportunas de las posibles vulnerabilidades con el ánimo de disminuir el impacto y afectación que pueda generar la explotación de una de ellas por parte de ciber delincuentes.

El Icetex cuenta con 409.000 beneficiarios [3], estos usuarios pueden ingresar sin restricciones a la página de la entidad y realizar consultas de sus créditos por medio de su portal web, dichos servicios, están enlazados a las bases de datos que contienen la información de los usuarios de la entidad. Por otra parte, cabe resaltar que son muchos los beneficiarios insatisfechos por el manejo de la entidad con sus créditos, lo que podría motivar a un externo a buscar la afectación de la compañía a través de su sitio público.

El desarrollo de este trabajo, está orientado a la detección de las vulnerabilidades dentro del proceso de gestión de créditos de la página web del Icetex, teniendo en cuenta las falencias que se presenten, se plantean controles que puedan aportar a la disminución de la probabilidad de que un riesgo se materialice.

3. MARCO TEORICO Y REFERENTES

Tomando como referencia la ISO/IEC 27000 e ISO/IEC 21001 - Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Se plantean a continuación los principales conceptos y definiciones que ponen en contexto el desarrollo de este trabajo:

Activo: "Cualquier cosa que tenga valor para la organización" [4].

Confidencialidad: "Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados" [4].

Disponibilidad: "Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada". [4]

Integridad: "Propiedad de salvaguardar la exactitud y estado completo de los activos" [4].

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. [5]

Evaluación del riesgo: "proceso de comprar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo" [4]

Tratamiento del riesgo: "Proceso de selección e implementación de medidas para modificar el riesgo" [4]

Valoración del riesgo: "Proceso global de análisis y evaluación del riesgo" [4]

Riesgo residual: "nivel restante de riesgo después del tratamiento del riesgo" [4].

Seguridad de la información: "Preservación de la confidencialidad, integridad y disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad" [4].

Sistema de gestión de seguridad de la información SGSI: "Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información" [4].

Por otra parte, cabe resaltar algunos casos de estudio que resaltan la problemática y evidencian la necesidad de evaluar las entidades del estado y sus servicios web. En Colombia, son objeto de estudio, diferentes empresas del sector susceptibles de ataques enfocados en tecnologías de la información y las comunicaciones, en el año en curso, Calderon [4] realiza una revisión sobre la seguridad de las entidades públicas para las que aplica gobierno en línea, dado que Colombia se encuentra en un nivel muy bajo en cuanto a los avances tecnológicos. Baron [5] propone una metodología para el análisis de vulnerabilidades de la Policía Nacional en su dirección de telemática, la intención de ataques por parte de terceros era cada vez mayor, tiene como resultado las recomendaciones para minimizar el impacto de

las vulnerabilidades detectadas. En el 2016, días antes de la votación del plebiscito se presentó un ataque a la Registraduria General de la Nación que se generó por medio de su servidor web y que afectaba la consulta del lugar de votación de cientos de Colombianos, dado que según el servicio, el documento que se ingresaba resultaba “Cancelado por muerte”. El ministro de defensa, Luis Carlos Villegas, con referencia al presunto hacker encargado de efectuar el ataque afirmó: “Se pudo comprobar que ha perpetrado 3.196 incursiones y atacado a 134 dominios web asociados con entidades del gobierno como la Presidencia de la República, ministerios, la propia Policia Nacional y la Registraduria” [6]. Por otra parte el registrador Galindo aseguro: “La web de la Registraduria es sometida diariamente a más de 320 mil ataques por parte de piratas informáticos” [7].

El Icetex, tiene como entes de control a La Contraloría General de la República, Contaduría General de la Nación, Superintendencia Bancaria de Colombia, Ministerio de Hacienda y Crédito Público, Departamento Nacional de Planeación, Departamento Administrativo de la Función Pública, Procuraduría General de la Nación y el Ministerio de Educación Nacional. Los procesos que al interior de la entidad se desarrollan, son auditados de manera anual para evaluar el cumplimiento de las normativas y leyes por las que se debe regir la entidad.

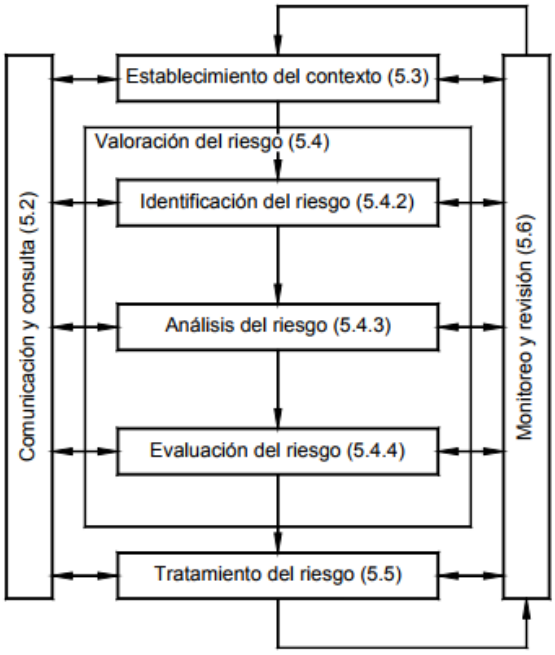
Tomando como referencia los informes de auditoría realizados en el mes de Mayo del año en curso, se encontraron reportes de falencias encontradas en las bases de datos de la entidad “Aplicativos. El ICETEX en la vigencia 2016 operaba sus bases de datos con los aplicativos C&CETEX (Cartera y Crédito), APOTEOSYS (Contabilidad) y ORION (Contratación) de los cuales se evidenciaron diversas debilidades y falencias.” [8]

Icetex define planes de mejoramiento donde detectan sus falencias y las acciones a interponer para lograr un progreso en los procesos que puedan verse afectados, el último plan de mejoramiento (2016), define: “Sistema de Gestión de Seguridad de la Información (SGSI). El ICETEX no cuenta con un área o un grupo de seguridad de la información plenamente definido y liderado o encabezado por un rol como el de "Oficial de Seguridad", que lleve a cabo las funciones que están establecidas en el Manual de Seguridad de la Información, razón por la cual se presentan diversas debilidades en el proceso” [8]

4. METODOLOGÍA

Con el fin de buscar la protección de la confidencialidad, integridad y disponibilidad de la información en el proceso de Gestión de Créditos del Icetex se toma como punto de partida la norma NTC/ISO 31000 para la gestión del riesgo con el fin de identificar, analizar, y evaluar los riesgos que pueden afectar el cumplimiento de los objetivos de la entidad.

La norma NTC/ISO 31000 propone:



NTC/ISO 31000 – Gestión del riesgo – Procesos para la gestión del riesgo [2].

FASE 1: Establecimiento del contexto:

OBJETIVO: Analizar el contexto, el entorno y los demás factores que generan impacto sobre la confidencialidad, integridad y disponibilidad del proceso de gestión de créditos del portal web del Icetex

Con el ánimo de poder desarrollar el proceso de análisis y gestión de riesgos asociados al servicio de gestión de créditos del portal web del Icetex, primero se debe tener el contexto en el que el proceso se desarrolla y demás factores que afecten lo afecten o que sean afectados por la falla del mismo.

Cronograma					
Establecimiento del contexto	**Descripción**	**Semana**			
		1	**2**	**3**	**4**
Identificar el contexto	En esta actividad se analiza la empresa, el núcleo de su negocio y los factores externos o internos que puedan afectar el funcionamiento adecuado de la compañía.	**X**			
Actores relevantes internos	Se debe entender la importancia del problema desde su perspectiva.	**X**			
Actores relevantes externos	Se debe entender la importancia del problema desde su perspectiva.	**X**			
Identificación de la estructura	Esta actividad se basa en el conocimiento que se tiene sobre el funcionamiento del servidor web de la empresa y los demás componentes ligados a él.	**X**			
Identificación de políticas	Esta actividad está ligada a las políticas, permisos y demás fundamentos que tiene la empresa en cuanto al servicio de gestión de créditos del portal web	**X**			
Identificación del procesos	Entendimiento de los procesos que se desarrollan o que dependen del servicio web para su funcionamiento		**X**		
Definición de técnica	Se basa en la definición de la metodología que se va a aplicar para el análisis y la detección de los riesgos		**X**		
Antecedentes	Antecedentes: Se basa en el estudio de los problemas o casos relacionados con el planteado	**X**			
Definición de metodología de medición	Definición de la metodología para la medición del impacto y la probabilidad de los riegos	**X**	**X**		
Definición de metodología de evaluación	Definición de la metodología de evaluación de los controles	**X**	**X**		

Actualmente, el proceso está custodiado por el director de tecnología y trabaja de la mano con procedimientos de: emergencias de software, soporte en infraestructura, desarrollo de software, asignación de accesos a sistemas de información, catalogación y control de versiones, revisión logs bases de datos, inventario de software y hardware y control de software legal, gestión de backups, pruebas de vulnerabilidad y control de cambios [1].

FASE 2: Identificación del riesgo:

OBJETIVO: Identificar los riesgos de la seguridad de la información ligados a los principales activos asociados al proceso de gestión de créditos del portal web del Icetex.

Como fase inicial se plantea la identificación de los activos de información ligados al contexto del servicio de Gestión de Créditos del portal web del Icetex, se identificara el responsable, los custodios, el contenedor y la valoración que ese activo de la información tiene.

Posteriormente, se realizara la identificación de riesgos determinando las causas, con base en factores internos y/o externos que pueden afectar la seguridad de la información de los activos; presentando una descripción de cada uno y definiendo posibles consecuencias.

Cronograma					
Identificación del riesgo	**Descripción**	**Semana**			
		1	**2**	**3**	**4**
Inventario	Generar un inventario de los activos tangibles e intangibles asociados a la seguridad informática del servicio de gestión de créditos del portal web.		**X**		
Detección de riesgos	Se basa en la detección de los riesgos y posibles brechas de seguridad asociadas al servicio web		**X**		
Detección de causas de los riesgos	Basado en los riesgos, se detectan las posibles causas que puedan materializar el riesgo		**X**		
Detección de consecuencias de los riesgos	Basado en los riesgos, se detectan las posibles consecuencias que puede traer la materialización del riesgo		**X**		

FASE 3: Análisis del riesgo:

OBJETIVO: Valorar los riesgos identificados en el proceso de gestión de créditos del Icetex.

Para el análisis de los riesgos que se identifiquen en el proceso de Gestión de Créditos del portal web del Icetex, se debe analizar las causas y consecuencias, la posibilidad y el impacto de la materialización de un impacto y el criterio con el cual se va a calificar al riesgo.

Cronograma					
Análisis del riesgo	**Descripción**	**Semana**			
		1	**2**	**3**	**4**
Definición de Probabilidades	Generar una escala de probabilidades basados en la frecuencia con la que se puede materializar un riesgo.			**X**	
Definición de Impactos	Generar una escala de impactos legales, de reputación y operacionales basados en el costo que pueda implicar la materialización de un riesgo.			**X**	

Definición de niveles de riesgos	Generar una escala de niveles de riesgo según la calificación de probabilidad x impacto que obtenga el riesgo			**X**	

FASE 4: Evaluación del riesgo:

OBJETIVO: Evaluar los riesgos identificados en el proceso de gestión de créditos del Icetex.

Para la evaluación del riesgo, se tendrá en cuenta la información obtenida en las fases anteriores, se determinaran los riesgos que requieran un tratamiento basados en la definición de niveles de aceptación de riesgo. Se determinaran los controles existentes y la efectividad de los mismos.

Cronograma					
Evaluación del riesgo	**Descripción**	**Semana**			
		1	**2**	**3**	**4**
Detección de controles existentes	Se basa en la detección de los controles que actualmente se aplican para los riesgos detectados dentro del proceso.			**X**	
Evaluación de controles existentes	Se basa en la evaluación de la efectividad de los controles existentes			**X**	
Definición de niveles de aceptación de riesgo	Generar una escala de niveles de aceptación de riesgo, con el ánimo de definir los riesgos que requieren prioridad para su tratamiento, los que pueden manejarse o los que no se deben tratar.			**X**	

FASE 5: Tratamiento del riesgo:

OBJETIVO: Diseñar un plan de tratamiento de los riesgos que permita disminuir la probabilidad o el impacto del riesgo sobre la confidencialidad, integridad y disponibilidad de la información del proceso de gestión de créditos del Icetex.

Esta acción permite determinar los controles a implementar y la posibilidad que tiene de reducir la probabilidad o el impacto del riesgo, con el fin de reducir la criticidad del mismo.

Cronograma					
Tratamiento del riesgo	**Descripción**	**Semana**			
		1	**2**	**3**	**4**

Definición de controles	Se basa en la definición de nuevos controles que apliquen para los riesgos detectados con un nivel de criticidad superior				**X**
Estimación de controles	Se basa en la estimación de la efectividad de los nuevos controles				**X**
Análisis de riesgo residual	Una vez estimados los nuevos controles planteados, definir el nivel de los riesgos resultante después de los controles				**X**

5. RESULTADOS Y DISCUSIÓN

Basados en la metodología planteada, se procede al desarrollo de cada una de las fases. Teniendo en cuenta la NTC/ISO 31000 se define una metodología para el proceso de gestión del riesgo y se plantean diferentes tablas y mecanismos para la identificación, análisis, evaluación y tratamiento de los mismos. Lo anterior, tiene como resultado un entregable por cada una de las fases, donde se detalla dicho proceso y la especificación de la metodología:

FASE 1: Establecimiento del contexto:

- Documentación del proyecto.

FASE 2: Identificación del riesgo:

- Inventario de activos de seguridad de la información asociados al proceso de Gestión de Crédito del portal web del Icetex.
- Inventario de riesgos que afectan la seguridad de la información de los activos asociados al proceso de Gestión de Crédito del portal web del Icetex.

FASE 3: Análisis del riesgo:

- Análisis y valoración de los riesgos detectados dentro de los activos asociados al proceso de Gestión de Crédito del portal web del Icetex.

FASE 4: Evaluación del riesgo:

- Inventario de controles existentes sobre los riesgos detectados dentro de los activos asociados al proceso de Gestión de Crédito del portal web del Icetex.
- Análisis y evaluación de los controles existentes detectados dentro de los activos asociados al proceso de Gestión de Crédito del portal web del Icetex.

FASE 5 Tratamiento del riesgo:

- Inventario de controles propuestos para los riesgos detectados dentro de los activos asociados al proceso de Gestión de Crédito del portal web del Icetex.
- Análisis y detección de riesgos residuales detectados en un supuesto de la aplicación de los controles propuestos.
- Políticas para la administración de los riesgos residuales.

Este proyecto tiene como resultado, los riesgos detectados dentro del proceso de gestión de créditos del portal web del Icetex junto con los controles que se plantean con base en la criticidad del riesgo y la necesidad de mitigarlo lo más rápido posible. Los controles planteados dentro de este proceso, son los adecuados para reducir la probabilidad de materialización en menos tiempo una vez que son implementados.

6. CONCLUSIONES

- La metodología planteada por la NTC/ISO 3100 para la gestión del riesgo, sirve como parámetro para el proceso de detección, análisis, tratamiento y evaluación del riesgo del proceso de gestión de créditos del portal web del Icetex.

- El análisis de los riesgos y la postulación de posibles controles sirve como posible tratamiento para la disminución de la afectación de vulnerabilidades que puedan ingresar por medio del servicio web de gestión de créditos del Icetex.

- El cumplimiento de la metodología permitió cumplir con los objetivos planteados para el proyecto.

7. BIBLIOGRAFIA

[1] Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior – ICETEX. Recuperado de: www.icetex.gov.co

[2] NTC/ISO 31000 – Gestión del riesgo. Recuperado de: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

[3] Dinero. Al menos 59.000 usuarios del Icetex están en deuda con el sistema. 2016 Recuperado de: http://www.dinero.com/pais/articulo/jornada-de-normalizacion-de-la-cartera-del-icetex-en-ciudades-de-colombia/232102

[4] ICONTEC (2013). NTC-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Recuperado de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

[5] ISO 27000 (2016). El portal de ISO 27000 en Español. Recuperado de: www.iso27000.es/iso27000.html.

[6] P. Andrea and C. Ramirez "Revisión del nivel de madurez del modelo de seguridad en entidades del orden nacional y territorial de Colombia que aplican gobierno en línea" 2017

[7] C. J. B Duquez "Metodología de análisis de vulnerabilidades para la red de datos en la dirección de telemática de la Policía Nacional" 2010

[8] El Heraldo. Capturado el presunto hacker de la Registraduria (2016). Recuperado de: http://www.elheraldo.co/nacional/capturado-el-presunto-hacker-de-la-registraduria-290148

[9] CMI. El proceso está blindado: Registrador tras ataques de hackers (2016) Recuperado de: http://www.cmi.com.co/politica/pagina-de-la-registraduria-atacada-por-hackers/403784/

[10] ICETEX – Plan de Mejoramiento (2016). Recuperado de: https://portal.icetex.gov.co/Portal/Home/el-icetex/mecanismos-de-control/planes-de-mejoramiento

8. ANEXOS

ANEXO 1:

En este anexo, se definen los activos de la información detectados dentro del proceso de Gestión de Créditos del portal web del Icetex, se definen en él, el impacto legal, reputacional y operacional que puede implicar la falla o perdida de estos activos. Por otra parte se definen también los riesgos detectados dentro del proceso junto con su descripción.

ANEXO 2:

En este anexo, se definen los riesgos detectados dentro del proceso de Gestión de Créditos del portal web del Icetex, junto con sus causas y las consecuencias que puede traer la materialización de los mismos, se califican de acuerdo a su probabilidad e impacto.

ANEXO 3:

En este anexo, se analizan y evalúan los controles existentes detectados para cada uno de los riesgos identificados, junto con la calificación que obtienen.

ANEXO 4:

En este anexo, se plantean los controles para cada uno de los riesgos detectados, junto con la calificación que tiene en diferentes aspectos la implementación de los mismos. Se comparan los impactos y las probabilidades de los riesgos antes y después de la implementación de los controles con el ánimo de evidenciar la efectividad del control. Por último, se establecen las acciones sugeridas para los riesgos residuales resultantes de la evaluación de los controles.