MANUAL DE BUENAS PRACTICAS SOBRE LA SEGURIDAD DE LA INFORMACIÓN SENSIBLE DE LA ENTIDAD DEL DANE

ANGEL YESID DUCUARA CRUZ
JAIME ADRIAN MOYA MOLANO

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

MANUAL DE BUENAS PRACTICAS SOBRE LA SEGURIDAD DE LA INFORMACIÓN SENSIBLE DE LA ENTIDAD DEL DANE

ANGEL YESID DUCUARA CRUZ
JAIME ADRIAN MOYA MOLANO

Trabajo de grado para optar al título de
Especialista en Seguridad de la Información

Asesor
ALEJANDRO CASTIBLANCO CARO

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

Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Institución Universitaria Politécnico Grancolombiano para optar al título de Especialista en Seguridad de la Información.

_____

Jurado

_____

Jurado

Bogotá, Mayo de 2017

CONTENIDO

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información (ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos).

BRECHA DE SEGURIDAD: secuencia de datos, o de comandos que se aprovecha de un error, de una falla o de una vulnerabilidad para producir un comportamiento involuntario o inesperado en un programa informático.

CONFIDENCIALIDAD: es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

CONTROL CORRECTIVO: control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

CONTROL DETECTIVO: control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

CONTROLES: son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

DISPONIBILIDAD: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

EVALUACIÓN DE RIESGO: es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir.

IDENTIFICACIÓN DE AMENAZAS: una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

INFORMACIÓN SENSIBLE: es el nombre que recibe la información personal privada de un individuo, por ejemplo, ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos.

INTEGRIDAD: propiedad de la información relativa a su exactitud y completitud.

ISO/IEC 27002:2013: guía de buenas prácticas en seguridad de la información que describe de forma detallada las acciones que se deben tener en cuenta para el establecimiento e implementación de los objetivos de control y controles descritos de una forma general en el Anexo A de la norma ISO 27001.

MATRIZ DE NIVEL DE RIESGO: la determinación final del nivel de riesgo es el resultado de multiplicar los valores asignados a la probabilidad de una amenaza por los valores asignados a la magnitud del impacto.

MITIGACIÓN DE RIESGOS: la mitigación de riesgos, es el segundo proceso de la administración de riesgos, comprende la priorización, evaluación e implementación de controles que reduzcan los riesgos de acuerdo con las recomendaciones emanadas del proceso de valoración de riesgos.

NIVELES DE SERVICIO: buscar un compromiso realista entre las necesidades y Expectativas del cliente y los costes de los servicios asociados, de forma que estos sean asumibles tanto por el cliente como por la organización TI.

RECOMENDACIONES DE CONTROL: la meta de las recomendaciones de control es reducir el nivel de riesgo del sistema de TI y de los datos a un nivel aceptable.

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.

VULNERABILIDAD: defecto o debilidad en los procedimientos de seguridad, diseño, implementación o en los controles internos del sistema que podrían ser explotadas y que resulta en una brecha de seguridad o violación de las políticas de seguridad.

1. RESUMEN EJECUTIVO

El proyecto de grado consiste específicamente en concientizar al personal de la entidad del DANE, sobre la suma importancia que en la actualidad tiene la protección de la información, dado que especialmente la Entidad reconoce que la información y en especial los datos son utilizados para producir estadísticas y estos se entienden como los activos más importantes para la continuidad del negocio. Para poder proteger dicha información se pretende el diseño de un manual de buenas prácticas acompañado de políticas y procedimientos de seguridad de la información, con el cual nos ayuda y nos da pautas para poder proteger la privacidad, seguridad, gestión del ciclo de vida de la información, cumpliendo con los mandatos de la constitución y la ley de reserva estadística; promoviendo la confianza y cooperación de los ciudadanos colombianos.

Es importante que la seguridad de la información sea un requisito inherente a las actividades y procesos de la entidad, y nunca deberá ser una función adicional o no prioritaria.

Mediante el manual de buenas prácticas se busca establecer políticas y lineamientos sobre los cuales se debe direccionar el desarrollo de la seguridad de la información del DANE y los principios de actuación del personal que tenga acceso o responsabilidades sobre la información sensible en la Entidad.

Adicionalmente contaremos con el apoyo de la elaboración de documentos de políticas y procedimientos sobre la seguridad de la información, donde se garantice el correcto uso y cuidado de la información en la Entidad, emitida por el área de tecnología y sistemas de información, acompañado de un manual de procedimientos relacionado con la realización correcta de Backus de la información sensible que está alojada en los equipos de cómputo y servidores del DANE.

Las políticas y procedimientos sobre la seguridad de la información aplican para el personal que hace parte del área de la Dirección de Metodología y Producción Estadística (Dimpe), que eta ubicado en la sede principal (Dane Central) en la cuidad de Bogotá, esta área hace parte de un proceso misional de la Entidad y específicamente una de las funciones principales es proponer a la Subdirección del Departamento las políticas que deban seguirse para el diseño, desarrollo e implementación de las investigaciones estadísticas, teniendo en cuenta la normatividad vigente y según requerimientos técnicos. Un proceso sumamente importante que depende directamente del área de Dimpe es el cálculo del IPC, el cual significa el indicador estadístico que permite establecer la variación porcentual promedio de los precios de un conjunto de bienes y servicios de consumo final que

demandan o usan los hogares, este indicador se genera el 5 de cada mes y su publicación de primera mano debe ir directamente a la presidencia de la república, posterior a ello se publica en los diferentes medios de comunicación, como: prensa, televisión, radio y demás.

Mediante el diseño del manual de bunas prácticas y los documentos de políticas y procedimientos sobre la seguridad de la información, se espera que los funcionarios de la Entidad y especialmente del área de Dimpe se concienticen de la importancia y sumo cuidado de la protección de la información, de igual manera se busca proteger al máximo los activos de información contra una amplia gama de amenazas para asegurar la continuidad de las operaciones, maximizar la eficiencia y la eficacia en pro del alcance de los objetivos estratégicos y misionales de la Entidad. Así mismo, se pretende definir y ejecutar campañas de entrenamiento y socialización de la seguridad de la información, para mantener actualizada la documentación que fundamenta el Sistema de Gestión de Seguridad de la Información. Finalmente se busca proteger la imagen, los intereses y el buen nombre del DANE.

El tiempo que se tiene establecido para llevar a cabo el desarrollo del proyecto de grado, para el diseño del manual de buenas prácticas de sobre la seguridad de la información en la entidad del DANE, esta detallado en el plan de trabajo y se estima aproximadamente de seis (6) meses, de acuerdo a los objetivos planteados, las actividades y los entregables del proyecto.

Los costos que se tienen estimados para llevar a cabo con el éxito del presente proyecto en la Entidad, es por valor de $63.840.000, dicho valor equivale al recurso humano por la asesoría de dos (2) especialistas en seguridad de la información y por el tiempo que dure el proyecto que es de seis (6) meses.

2. JUSTIFICACIÓN

El Gobierno Nacional ha demostrado un serio compromiso para que las entidades estatales estandaricen las acciones de implementación y uso de las tecnologías de la información y la comunicación, propendan por la seguridad de la información y desarrollen medidas para proteger la información y los servicios frente a las amenazas informáticas.

En este sentido el Ministerio de las Tecnologías de la Información y las Comunicaciones dentro de sus responsabilidades ha sido encomendado para diseñar y formular políticas y planes para la coordinación y estandarización de acciones tendientes a implementar el uso de las TIC y proteger los bienes, activos, servicios, derechos y libertades dependientes del Estado a través de la definición de una estrategia de seguridad y privacidad de la información desde la perspectiva de la tecnología.

Debido a lo anterior, el DANE considera que la seguridad es indispensable para proteger los activos de la información de las amenazas, por ende, propenderá por la continuidad de la operación, minimizando el riesgo de daño o pérdida de la información.

Para apoyar el cumplimiento de los objetivos estratégicos, la Entidad contempla la seguridad de la información como uno de los factores críticos de éxito; debido a esto, la información debe disponer de la debida protección, con el fin de mantener la confianza de los usuarios internos y externos, en los procesos, en los trámites y en los servicios. Por consiguiente, se diseñará el manual de buenas prácticas con políticas y procedimientos para la gestión correcta de la seguridad de la información.

Una de las necesidades a satisfacer es la protección máxima de los activos de información del DANE, de acuerdo con lo establecido en los procesos institucionales y la regulación existente.

De igual manera los beneficios esperados al diseñar el manual de buenas prácticas acompañado con políticas y procedimientos sobre la seguridad de la información, es garantizar la confidencialidad, integridad y disponibilidad de los activos de información e información sensible de la Entidad. Otro de los beneficios que se lograría es las responsabilidades frente a la seguridad de la información, serán definidas, socializadas, difundidas y deberán ser aceptadas por cada uno de los funcionarios del área involucrada.

3. MARCO TEORICO Y REFERENTES

3.1 MARCO TEORICO

Debido a la evolución permanente de las tecnologías de la información y las comunicaciones que demandan un mayor esfuerzo para garantizar la seguridad, a las constantes amenazas que hoy en día atentan contra la seguridad de la información que cada vez son más especializadas, complejas y avanzadas, y a la normatividad vigente que regula y exige una mayor protección y privacidad de los datos sensibles, personales, comerciales y financieros de las personas, las entidades del gobierno deben contar con manuales de buenas prácticas sobre seguridad de la información basado en estándares de seguridad, con el propósito de poder establecer y mantener un gobierno de seguridad alineado a las necesidades y objetivos estratégicos del negocio, compuesto por una estructura organizacional con roles y responsabilidades y un conjunto coherente de políticas, procesos y procedimientos, que le permiten gestionar de manera adecuada los riesgos que puedan atentar contra la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y no repudio de la seguridad de la información.

Para lograr una adecuada gestión de la información es indispensable que las organizaciones establezcan una metodología estructurada, clara y rigurosa para la valoración y tratamiento de los riesgos de seguridad, con el objetivo de (i) conocer el estado real de la seguridad de los activos de información a través de los cuales se gestiona la información del negocio, (ii) identificar y valorar las amenazas que puedan comprometer la seguridad de la información y (iii) determinar los mecanismos y medidas de seguridad a implementar para minimizar el impacto en caso de las posibles pérdidas de confiabilidad, integridad y disponibilidad de la información.

Así mismo, para tener claro los diferentes conceptos que se enuncian en este marco teórico, en el capítulo “5.1. MARCO CONCEPTUAL (GLOSARIO DE TERMINOS)” se encuentran el glosario de los términos con sus respectivas definiciones, los cuales son utilizados a lo largo del presente trabajo de grado.

Seguridad de la Información: [1]

Consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Fundamentos:

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

Gestión de Seguridad de la Información: [2]

La gestión de la seguridad de la información es un proceso continuo que consiste en garantizar que los riesgos de la seguridad de la información sean identificados, valorados, gestionados y tratados por todos los miembros de la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

[1] http://www.iso27000.es/sgsi.html

[2] http://www.iso27000.es/sgsi.html

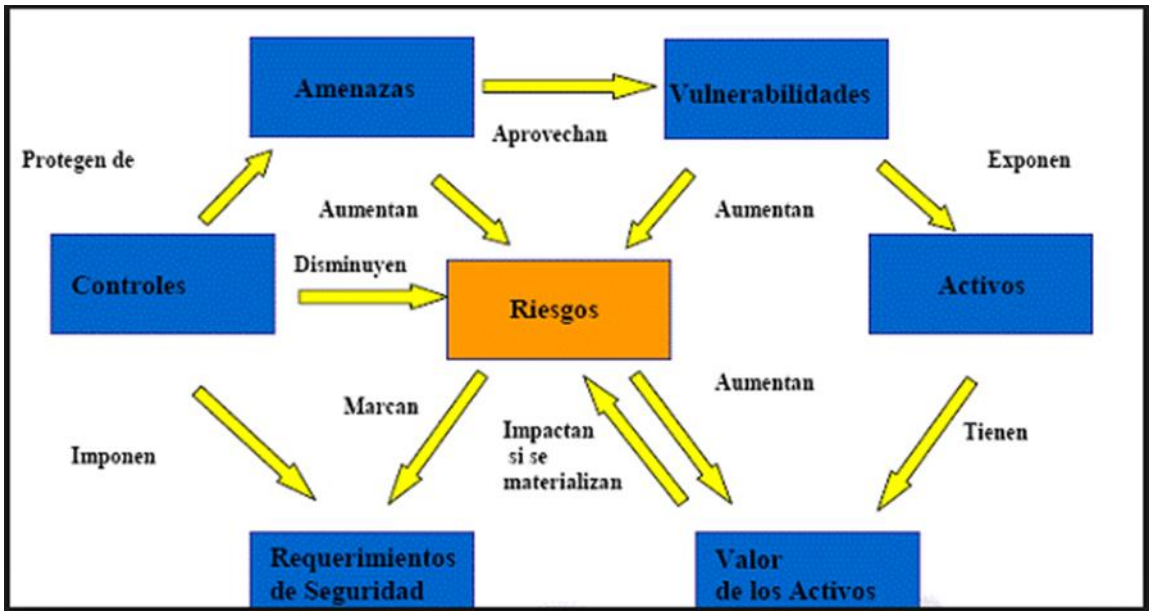

Figura 1. Modelo de gestión de seguridad

Fuente: http://www.iso27000.es

ISO: [3]

Se denomina ISO a la Organización Internacional para la Estandarización, la cual se trata de una federación cuyo alcance es de carácter mundial, ya que está integrada por cuerpos de estandarización de 162 países. Esta organización se estableció en 1947, como un organismo no gubernamental, cuya misión es promover a nivel mundial el desarrollo de las actividades de estandarización.

La familia de las normas ISO/IEC 27000, son un marco de referencia de seguridad a nivel mundial desarrollado por la International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, que proporcionan un marco, lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización. Estas normas especifican los requerimientos que deben cumplir las organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

[3] http://www.implementacionsig.com/index.php/23-noticiac/29-que-es-iso

En Colombia, el Instituto Colombiano de Norma Técnicas y Certificaciones, ICONTEC, es el organismo encargado de normalizar este tipo de normas.

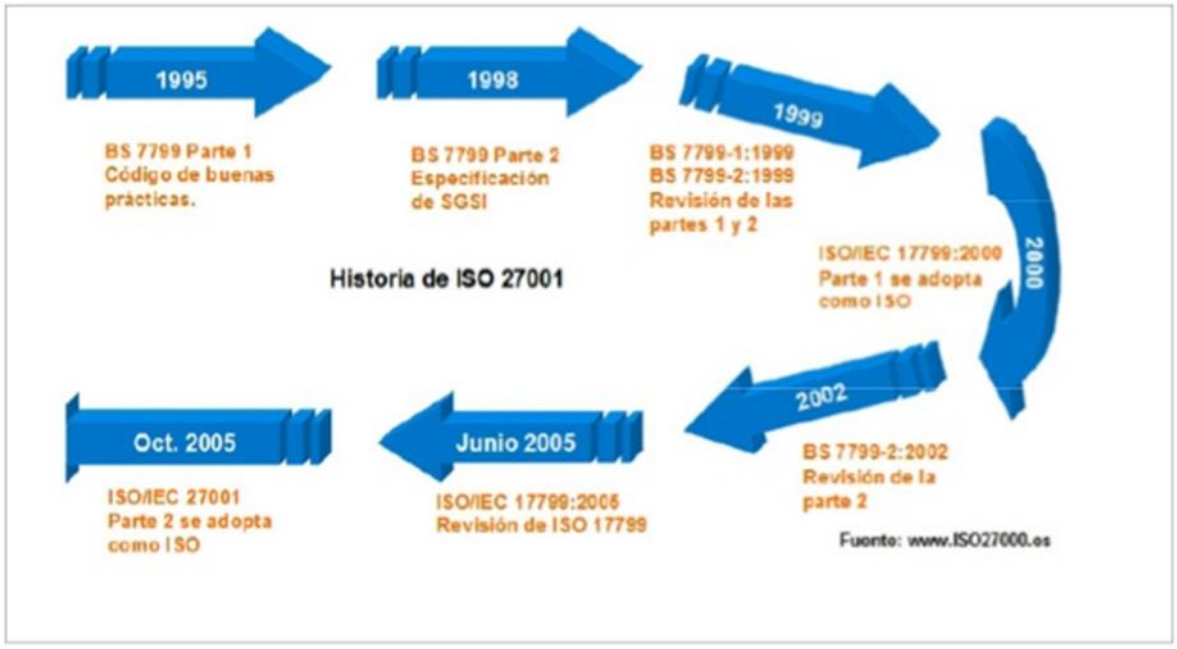

Figura 2. Historia de la ISO

Fuente: http://www.iso27000.es

4. METODOLOGÍA

A continuación, se presenta la metodología creada y desarrollada por el grupo de trabajo, para solucionar el problema en el Departamento Administrativo Nacional de Estadística DANE y construir los entregables propuestos en el proyecto de grado.

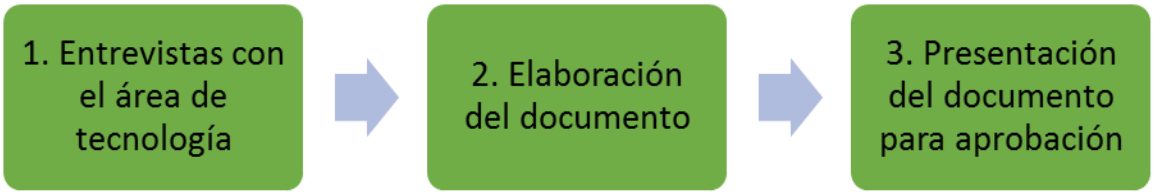

Figura 3. Metodología aplicada

4.1 ENTREVISTAS CON EL ÁREA DE TECNOLOGÍA

Se realizaron entrevistas con el Área de Tecnología y Sistemas de Información del Departamento Administrativo Nacional de Estadística DANE, para conocer las expectativas y la experiencia de los funcionarios para el desarrollo de los manuales de mejores prácticas de seguridad de la información sobre el uso y sumo cuidado de la información, manual de políticas sobre seguridad de la información y manual de procedimientos relacionado con la realización correcta de Backup.

4.2 ELABORACIÓN DEL DOCUMENTO

Para la elaboración de los manuales de mejores prácticas de seguridad de la información sobre el uso y sumo cuidado de la información, manual de políticas sobre seguridad de la información y manual de procedimientos relacionados con la realización correcta de Backup, se alinearon a los objetivos de la entidad y se tuvo en cuenta la norma ISO/IEC 27002:2013.

Para la elaboración del Manual de políticas sobre seguridad de la información se contó con la Guía 2 elaboración de la política general de seguridad y privacidad de la información de MINTIC, la cual es una guía de recomendaciones de políticas de

seguridad de la información como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015. Este conjunto de recomendaciones no es exhaustivo, y aconseja que cada Entidad genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar.

Para la elaboración manual de procedimientos relacionado con la realización correcta de Backup, se contó con la Guía 3 procedimientos de seguridad de la información de MINTIC, la cual es una guía de recomendaciones de procedimientos de seguridad de la información para el Modelo de Seguridad y privacidad de la Información para las Entidades del Estado.

4.3 PRESENTACIÓN DEL DOCUMENTO PARA APROBACIÓN

Se realizaron reuniones con el Director del Área de Tecnología y Sistemas de Información de la entidad para revisar, validar los documentos elaborados en el punto 2, para luego enviarlos a aprobación de la Alta Dirección y posterior publicación en los medios de comunicación establecidos en la entidad y que estos sean de cumplimiento por los funcionarios del Departamento Administrativo Nacional de Estadística DANE.

5. RESULTADOS Y DISCUSIÓN

Los resultados alcanzados en el desarrollo del presente trabajo de grado, se presentan en los siguientes anexos:

Anexo 1. Manual de mejores prácticas de seguridad de la información.

La construcción del manual se realizó con el apoyo del área de sistemas, enfocándose en los temas más importantes y la experiencia del grupo del proyecto y funcionarios del área para trasmitir a los funcionarios de la DIMPE las mejores prácticas en la administración del archivo principal digital, la importancia de las copias de respaldo de información, identificación de personajes de seguridad informática, y la alerta de virus Ransomware - recomendaciones a seguir.

Anexo 2. Manual de políticas de seguridad de la información.

En la construcción del manual se tuvo la experiencia del grupo del proyecto, especialmente de Jaime Moya por su experiencia de más de 15 años en el desarrollo de documentación de sistemas de gestión de calidad y 6 años en el desarrollo de políticas de seguridad de la información en diferentes empresas que ha trabajado. Esta experiencia ayudo a que los tiempos de elaboración del manual se cumplieran al igual que se cumpliera con la calidad esperada por el área de sistemas.

Anexo 3. Manual de procedimientos para la realización correcta de los backup.

El manual de Manual de buenas prácticas sobre la forma correcta de realizar los Backup, fue construido de acuerdo a los problemas más relevantes que se presentan actualmente en la Entidad, como lo son: perdida y/o manipulación de la información sensible de los sistemas de información.

No tuvimos mayores dificultades en la elaboración de dicho manual ya que se había realizado previamente un borrador donde se incluyeron los aspectos más relevantes y detallados sobre la realización de los Backup.

Con este manual aportamos a la construcción del objetivo general porque sugerimos lineamientos y procedimientos sobre las tareas que deben seguir los

funcionarios para la toma de Backup de la forma correcta de la información sensible que está alojada en sus equipos de cómputo y servidores de la Entidad del DANE.

Anexo 4. Artículo IEEE

En la construcción del Articulo IEEE “Manual de buenas Prácticas Seguridad de la Información – DANE”, se tuvo en cuenta los aspectos más relevantes de nuestro proyecto de grado como son: resumen, abstract, objetivos, metodología, estado del arte, resultados y discusión, conclusiones, referencias y autores. En la elaboración de este artículo, no encontramos mayores dificultades, ya que se había realizado previamente un borrador donde se incluyeron los aspectos más importantes y detallados sobre el proyecto de grado.

6. CONCLUSIONES

La seguridad de la información es importante por lo que se deben tomar medidas preventivas en la actualidad, de esta manera para ayudar a la protección de los activos de información en cualquier organización, se deben implementar políticas y procedimientos sobre la seguridad de información que concienticen a los funcionarios sobre la importancia de dichos activos.

Se debe estar en constante investigación con respecto a las vulnerabilidades y amenazas que se hallan en los sistemas, con el fin de que se puedan tomar las medidas respectivas a tiempo. Antes de que sean explotadas por un delincuente.

Los ataques informáticos que se presentan en la actualidad no solo son más frecuentes sino más sofisticados lo que obliga a estar en constante actualización en temas de seguridad, y a estar probando constantemente la efectividad de controles, revisando fallas y corrigiendo.

Con la elaboración del manual de buenas prácticas acompañado de políticas y procedimientos nos dimos cuenta que es una herramienta de gran ayuda que nos permite establecer gobierno de seguridad de la información en la Entidad del DANE. Así mismo con este documento nos garantiza que podemos seguir trabajando y mejorando continuamente en lo que conciernen aspectos de seguridad de la información.

En la fase de implementación de los manuales de buenas prácticas, políticas y procedimientos en la Entidad del DANE especialmente en el área de Dimpe, es importante que la Alta Dirección se comprometa aprobando los manuales indicados y que los usuarios de esta área se concienticen de la importancia y sumo cuidado de la protección de la información.

BIBLIOGRAFÍA

ACEVEDO Juárez, H. (05 de 11 de 2016). Magazcitum, disponible en: http://www.magazcitum.com.mx/.

Guía Nro. 2. Elaboración de la política general de seguridad y privacidad de la información disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Guía Nro. 3. Procedimientos de seguridad de la información disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

http://www.recoverylabs.com/wp-content/uploads/2014/03/ppales-factores-perdida-info-2003.jpg.

http://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_mist_sp.p df

http://www.iso27000.es/sgsi.html

http://www.implementacionsig.com/index.php/23-noticiac/29-que-es-iso

https://www.sophos.com/es-es/security-news-trends/security-trends/data-leakage-prevention.aspx.

https://www.sophos.com/es-es/security-news-trends/security-trends/data-leakage-prevention.aspx.

PAOLI J Antonio, "Comunicación e información", Editorial Trillas, México 1989.

ANEXOS

Anexo 1. Manual de mejores prácticas de seguridad de la información.

Anexo 2. Manual de políticas de seguridad de la información.

Anexo 3. Manual de buenas prácticas sobre Backup.

Anexo 4. Articulo IEEE sobre la seguridad de la información_DANE.