Análisis de impacto de la Ingeniería Social sobre los resultados y el desempeño en el marco de la gestión de la Seguridad de la Información para el Departamento Administrativo Nacional de Estadística (DANE).

Carlos Alberto Ortíz Aux

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería

Especialización en Seguridad Informática

Popayán, 2020

Análisis de impacto de la Ingeniería Social sobre los resultados y el desempeño en el marco de la gestión de la Seguridad de la Información para el Departamento Administrativo Nacional de Estadística (DANE).

Carlos Alberto Ortíz Aux

Monografía presentada para optar al título de Especialista en Seguridad Informática

director:

Msc. Johnn Eduard Criollo Salamanca

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería

Especialización en Seguridad Informática

Popayán, 2020

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Presidente del jurado

_____

Jurado 1

_____

Jurado 2

Popayán, Agosto de 2020.

Dedicatoria

Así como toda la suma de mis esfuerzos, también este breve espacio de mi vida dedicado a esta especialización, trabajo final y su correspondiente logro está dedicado a mis dos hijas por ser mi más grande y acaparadora motivación en todos y cada uno de los pasos que debo afrontar, y a toda mi familia por ser siempre mi apoyo en los constantes impulsos, tropiezos, alegrías y tristezas de mi existir.

Agradecimientos

A mi padre por su terca constancia, quien, aunque creció en un mundo de contrastantes necesidades, luchó incansablemente porque a su familia no le faltara nada.

A mi madre por su tenaz perseverancia y resiliencia, quien ha entregado su carrera, su independencia, su vida y más para que sus hijos y sus nietas encuentren el camino de la felicidad.

A mis hermanas por su cariño protector que me ofrecieron desde mi más temprana edad.

A mi esposa por ese amor incondicional que persevera en la unión y el entendimiento.

A mis dos adorables, traviesas y maravillosas hijas que lograron implantar en mi mente la terrorífica dependencia de saber de ellas felices.

A mi director de grado quien supo orientarme y estuvo siempre muy pendiente y dedicado al progreso de mi trabajo de grado.

A aquellos amigos que siempre han estado a mi lado y a aquellos que ya partieron, y que juntos han contribuido al entorno que me trae a este tiempo, lugar y forma.

A la incandescente casualidad o error del universo y la existencia, ocupándome en este sitio y lugar lleno de bruma y claridad que nunca habría aprendido a manejar sin lo que me brindaron todas las personas de mis afectos.

Tabla de contenido

Lista de imágenes

Introducción

La gestión de la seguridad de la información es actualmente una labor inherente a cualquier tipo de organización sea gubernamental o privada, de igual manera independiente del core de cualquier negocio. Quizás en algunas perspectivas, la inversión de tiempo y esfuerzo en una adecuada gestión de seguridad de la información sería inviable, esto, teniendo en cuenta la preparación para efectuar la implementación de dicho menester dependiendo del entorno y su correspondiente relación costo-beneficio. Sin embargo, en el caso de las entidades gubernamentales, la aplicación de la gestión de seguridad de la información en sus diferentes planes, programas y cualquier lineamiento que rija su ejecución operativa e incluso administrativa, es algo en lo cual se han venido preparando y mejorando a lo largo de la experiencia que tienen tales entidades, todo bajo el impulso entregado por el Ministerio de las Tecnologías de la Información y las Comunicaciones a través del programa Gobierno en línea, el cual enmarca no solo los lineamientos sino la legalidad de todo el proceso.

No obstante lo anterior, hay un sinnúmero de agentes externos e internos que pueden incidir en cualquier ejecución de estos planes, programas y proyectos, tales como las vulnerabilidades causadas por malas prácticas, en ejemplos tan simples como descuidar impresiones con datos sensibles, o por el ambiente externo la continua e incansable lucha contra los piratas informáticos que siempre verán en la información una fuente para actividades criminales. En el caso de entidades gubernamentales, estos son ya bastante conocidos, algunos obviados, otros aceptados (a pesar de ser incorrectamente aplicables) y otros combatidos formal o activamente.

El esfuerzo encaminado a llevar a buen término todos y cada uno de los objetivos planteados en todos los proyectos que componen un plan de acción de cualquier entidad gubernamental, son en sí la aplicación de técnicas globalmente conocidas articuladas con estrictos lineamientos que suelen ser precedidos por aspectos legales, operativos, administrativos, y dentro de estos últimos, deben aplicarse todos aquellos requerimientos en seguridad de la información que dictan las normas locales, nacionales e incluso internacionales. El ejemplo más relevante de ello es el Plan de Gobierno en Línea, el cual marca la pauta para la estandarización de la seguridad de la información que garanticen el buen funcionar en este aspecto y con ellos la correcta ejecución de los rubros del erario público nacional a través de las muchas entidades componentes del estado colombiano y sus correspondientes planes de acción.

Ha sido muy importante el avance en la evaluación de la gestión de la seguridad de la información de dichas entidades, iniciando con la presentación de planes de acción con su correspondiente apartado exclusivo en la parte administrativa para este tópico, llegando a estas alturas a mediciones de impacto que una vez fueran implementadas correspondieron a una prometedora estrategia para revelar el efecto real de la labor de las entidades a favor de la plena conservación de integridad, disponibilidad y privacidad de la información que todos los ciudadanos tienen depositada en dichas organizaciones.

Lo anterior viene siendo algo independiente del core del negocio de cada una de las entidades. En este escrito singularmente hablando del Departamento Administrativo Nacional de Estadística – DANE, dicho énfasis viene orientado a la reserva estadística principalmente, tal como existen otras entidades con el mismo objetivo a lo largo del territorio nacional. Esto es, nada más que la sinergia atribuida al aprovechamiento de la recopilación de datos en todo el territorio nacional y de diversas temáticas con la correcta aplicación de estándares analíticos y

estadísticos que permita proveer de las herramientas para la correcta toma de decisiones gubernamentales.

Se espera con esta monografía analizar de manera pragmática cuáles son los factores de la Ingeniería Social aplicada por agentes externos y que inciden en el éxito o fracaso de los proyectos ejecutados en esta entidad para así contribuir al mejoramiento de la gestión de resultados en cualquier otra entidad gubernamental.

Resumen analítico del escrito

La presente monografía pretende hacer un análisis constructivo de las causas que generan dificultades en el entorno de la Gestión de la Seguridad de la Información en el Departamento Administrativo Nacional de Estadística – DANE, entidad del orden Nacional con misión estadística para la toma de decisiones en pro del desarrollo sostenible y el correcto direccionamiento de políticas en el país y a partir de ello, definir la incidencia de impacto en el cumplimiento de dicha misión.

Como entidad pública del orden ejecutivo, cuenta con un presupuesto basado únicamente en el tesoro nacional, y realiza su deber misional financiándose por rubros de Funcionamiento y de Inversión, siendo este último el referente a los proyectos internos y externos recibidos. Estos proyectos se administran en el Banco de Proyectos, a través de la metodología Marco lógico y abarcan objetivos misionales y corporativos que en últimas siempre apuntan a la misión de la entidad. Uno de los objetivos de apoyo es el de brindar adecuada seguridad a la información que se procesa en la entidad, máxime cuando se trata de una entidad de estadística que debe constantemente garantizar su reserva.

En varias ocasiones se han percibido ocasionales pero notorias brechas entre los resultados esperados y los obtenidos al final de la jornada, por lo cual se crea la indagación acerca de cuáles son las principales dificultades relacionadas con la gestión de seguridad de la información y que afectan el entorno de la gestión de estos proyectos para posteriormente analizarlas y documentarlas de una manera críticamente constructiva, todo enfocado hacia la ingeniería social,

práctica que ha venido evolucionando a lo largo de los años y que no discrimina por tipo de víctima.

Palabras Clave: Gestión de la Seguridad de la Información, Riesgos, Vulnerabilidades, Ingeniería Social, Entidades Públicas.

Abstract

This monography aims to create a constructive analysis of all those causes that generate any kind of difficulties within the environment of Information Security Management in the National Administrative Bureau of Statistics of Colombia (DANE), countrywide organization with an Statistical mission leading to the accurate make of decisions in order to a sustainable development and the proper addressing of policies in the country, and, starting from there, defining the impact regarding the accomplishment of that mission.

As a public organization part of the executive order, has a budget based only in the National treasury, and executes its missional duty by financing its activities from operational and investment entries, this last one becoming the one in regards to the internal projects and those received from the outside of the organization. These projects are managed within the Projects Bank, through the Logic Frame methodology and include a wide variety of missional and corporate objectives, that nevertheless aim to the organization mission. One of those support goals is to provide with an adequate protection and security to the data being process in all those projects, even more when it comes to a statistical organization that must permanently guarantee information reserve.

Several times, fortuitous but evident gaps between the expected results and the ones achieved have been noticed, hence comes inquiry about what are the main issues Information Security related that truly affect the environment for the management of those project, so they can be further analyzed and documented in a critically constructive way, all the time focused

towards Social Engineering, practice that has been evolving throughout the years in such a manner that does not discriminate for type of victim.

Keywords: Information Security Management, Risks, Vulnerabilities, Social Engineering, Public Organizations.

Definición del problema

Existen a nivel nacional políticas gubernamentales que marcan la pauta y dictan los lineamientos generales para la gestión de la seguridad de la información al interior de entidades públicas con distintos niveles de administración, orden, régimen y autonomía. Adicionalmente, es notorio que en la realidad, la aplicación estas políticas llevadas a la práctica no alcanzan un grado satisfactorio de efectividad frente al accionar administrativo y tecnológico que tienen estas entidades, sobre todo en lo que concierne a la satisfacción del estado colombiano. Si bien no existe particularmente un estudio acerca de la favorabilidad de la entidad objeto de este escrito, precisamente es la entidad oficial encargada de delimitar este aspecto para todas las entidades, demostrando por ejemplo en los resultados de la "Encuesta sobre Ambiente y Desempeño Institucional Nacional EDI" la falta de motivación de la ciudadanía a acceder a servicios a través de canales digitales, siendo que suelen ser más sencillos prefieren los canales presenciales:

Ilustración 1, Resultados factor "Servicio al Ciudadano"

En 2019, los servidores afirmaron que el canal de atención preferido por la ciudadanía que acude a sus entidades, para realizar un trámite o solicitar un servicio, son las *oficinas o puntos de atención presencial* (40,5%), seguido del *sitio web de las entidades* (31,7%).

Gráfico 14. Porcentaje de servidores según el canal de atención que consideran es el preferido por la ciudadanía al momento de realizar un trámite o solicitar un servicio en su entidad.
Total nacional
2019

Canal de atención preferido por la ciudadanía al momento de realizar un trámite o solicitar un servicio en su entidad.*	Porcentaje %	IC (+-)	Diferencia puntos porcentuales 2018-2019
Oficinas o puntos de atención presencial.	40,5	0,6	-1,8
Sitio web de la entidad (Internet).	31,7	0,6	-0,2 **
Correo electrónico.	14,3	0,4	3,1
Línea telefónica de atención.	9,0	0,3	-0,7
Correo postal-cartas.	2,5	0,2	-0,3
Aplicación móvil (App)	1,9	0,2	-0,9

Fuente: DANE, EDI 2019.
* Opción de respuesta única.
** Variación estadísticamente no significativa.

Tomada de: https://www.dane.gov.co/files/EDI_nal/2019/Boletin-tecnico-edi-nacional-2019.pdf, P. 14

De las diferentes causas que pueden generar estas dificultades, se pueden referenciar varias, incluyendo la falta de recursos para la ejecución de actividades que mejoren la seguridad de la información, la falta de recurso humano calificado para la orientación de dichas tareas, las dificultades políticas y organizacionales que afectan la planeación y control de los distintos proyectos tecnológicos, entre otras, sin embargo parece común, redundante y prominente la existencia constante de alguna justificación que ampare a los ejecutores frente a las críticas externas por la ineficiencia e ineficacia de acciones en la labor orientada a la seguridad de la información que emplea recursos públicos para cualquiera que sea la misión institucional de la entidad oficial.

Cabe aclarar que existe una gran diferencia entre la gestión de seguridad informática en el ámbito privado y la gestión de seguridad informática en el ámbito público, siendo adicional la dificultad en éste último, esto debido a que como a todo proyecto, el sector privado tiene una ventaja motivacional mayor que en el sector público, lo cual a su vez que genera un desconcierto para los gestores de tales proyectos tecnológicos que han contribuido a esta labor en ambas partes, notándose también un perfil que ha sido moldeado o influenciado dependiendo del ámbito en el que se ha adquirido esta experiencia.

Existe en la contextualización del problema que se pretende definir, segmentados grupos de entidades que comparten ciertas características en cuando a su centralización o descentralización de políticas que orientan su accionar misional, por lo que, es importante también caracterizar estas condiciones ya que los entornos organizacionales pueden influir notoriamente en la manera de gestionar los recursos incluyendo también los proyectos relacionados con la tecnología de la información y la seguridad de la misma, ya sean internos y externos que en el entorno

organizacional y operativo se desarrollan. Esto, a pesar de que existe ya una política nacional establecida para tratar de estandarizar las reglas de juego del entorno.

Para el caso en particular, el Departamento Administrativo Nacional de Estadística, entidad pública del orden Nacional cuya misión se enfoca a obtener, procesar, administrar y proveer datos estadísticos para la correcta toma de decisiones en entornos políticos, educativos, gubernamentales, etc., todo en pro de un desarrollo sostenible, la situación parece aún más crítica, pues su carácter autónomo pareciera disponer de aún más dificultades teniendo en cuenta el contexto político que enmarca su administración, hecho que obviamente se verá también reflejado en la ejecución de los proyectos relacionados con la seguridad de la información al interior de la misma.

Partiendo de una posición crítica y desde un ámbito interno de tal entidad pública colombiana, surge entonces tal planteamiento que origina la motivación del análisis que se pretende realizar, así:

¿Cuál es el nivel de incidencia de la ingeniería social que afecta la seguridad de la información en cuanto al cumplimiento de la misión institucional del DANE?

Teniendo en cuenta la naturaleza de este problema, se considera pertinente abordarlo desde el contexto de la gestión de seguridad de la información en general, para que contribuya al entendimiento de las dificultades que más adelante se detallen.

Justificación

Al interior del Departamento Administrativo Nacional de Estadística, se puede evidenciar como se articulan múltiples proyectos que pretenden abordar directa o indirectamente los diferentes roles de la misión institucional, y de igual manera se perciben las falencias de la ejecución de estos proyectos a lo que se le suman las constantes críticas del público en general. Todo esto conlleva a una consideración del actuar misional con respecto a la eficiencia, eficacia, efectividad e incluso productividad de los proyectos articulados en el Plan Operativo Anual de Inversiones.

Es importante tener en cuenta que las críticas externas surgen a partir de la preocupación del público en general, quienes en veeduría del manejo del erario público manifiestan su insatisfacción constantemente, lo que genera un deterioro de la Imagen Corporativa que es de sobremanera importante para el deber misional ya que como entidad pública depende también del apoyo social que brinda una confianza en todo el actuar y los proyectos que involucran acciones de la comunidad en general para ejercer la actividad estadística en todo el territorio nacional. Esto es ya conocido en varios episodios de la historia reciente colombiana, y se ha visto cómo la percepción de la seguridad en la información con los datos de los ciudadanos puede llegar a afectar el rol de este organismo gubernamental, tal como ocurrió a inicios del año 2018 en medio del operativo del Censo Nacional de Población y Vivienda, para el cual se implementaron herramientas tecnológicas con el fin de agilizar la recolección de datos, hechos

que fueron criticados duramente en base a una posible brecha de seguridad con las credenciales de acceso para acceder a dicho formulario[1].

A un menor nivel, pero aún con gran importancia también se encuentra la preocupación del funcionario interno que no ve sus esfuerzos convertidos en una satisfacción demostrable del público en general y en varias ocasiones tampoco se ve el resultado materializado por la incidencia de múltiples factores internos o externos, tales como la renuencia de la gente en confiar en el principio de confidencialidad que otorga el DANE a sus investigaciones, lo que genera un desconcierto en aquellas ocasiones en las que no se tiene un control de los resultados o inclusive cuando no se conoce el porqué de los mismos, máxime cuando se trata de temas de seguridad de la información por cuanto suelen ser aspectos meramente administrativos y tecnológicos que deberían estar contenidos sin que no solo no afecte la operatividad sino que la facilite y la mantenga íntegra.

Este análisis se realiza para coadyuvar a la identificación y gestión de las principales dificultades que se presentan en el entorno de la gestión de la seguridad de la información en el Departamento Administrativo Nacional de Estadística – DANE, en especial aquellas relacionadas con los constantes e inevitables intentos de ataque a través de la ingeniería social, y de esa manera contribuir a la eficiencia, eficacia, efectividad, productividad y mejoramiento de la imagen corporativa de esta y las demás entidades a las que aplique un objeto similar.

[1] Wradio, 15 de enero de 2018. “La página del eCenso almacena mal tu contraseña, no la uses”. Recuperado de: https://www.wradio.com.co/noticias/actualidad/la-pagina-del-ecenso-almacena-mal-tu-contrasena-no-la-uses-juliana-pena/20180115/nota/3689816.aspx

Objetivos

Objetivo General

Identificar dificultades del entorno de la gestión de seguridad de la información en cuanto a la ingeniería social y cómo esta afecta en el desempeño y los resultados del Departamento Administrativo Nacional de Estadística – DANE.

Objetivos Específicos

- Definir el estado del arte en la gestión de seguridad de la información para el Departamento Administrativo Nacional de Estadística – DANE.
- Recopilar las políticas, planes, programas procedimientos y demás lineamientos que marcan la pauta para la gestión de seguridad de la información en la organización.
- Identificar las dificultades de gestión de seguridad de la información y la incidencia de las amenazas producidas por la ingeniería social.
- Catalogar, clasificar y priorizar los factores y dificultades que rodean la seguridad de la información en la entidad en cuanto a la incidencia de ataques por ingeniería social.
- Realizar una comparación sistemática con otras entidades del estado Colombiano que puedan llegar a presentar la misma vulnerabilidad.

Marco Teórico

Con el fin de abordar la temática conceptual y teórica del análisis que se pretende realizar en esta monografía, se hace necesario enfocar los términos, conceptos y documentación en la gestión de la seguridad de la información y su entorno más general aplicable a la terminología obligatoria para las entidades oficiales del estado colombiano, así como a ciertos parámetros que definen de una manera específica el actuar de este gerenciamiento en el Departamento Administrativo Nacional de Estadística específicamente.

Proyecto.

Un proyecto es un conjunto único y discreto de tareas con un inicio definido (estado del arte), una finalización concebida y un resultado esperado. Esto puede ser tan simple como realizar un informe para un curso, o tan complejo como diseñar, desarrollar y poner a prueba un destructor para la fuerza naval de un País.

Como se mencionó anteriormente, cada proyecto debe tener en cuenta las restricciones en tiempo que están determinadas por un plan de trabajo o cronograma, un alcance que se demarca mediante la justificación y propósito del proyecto en sí y un presupuesto que generalmente es limitado. En este sentido se tienen varios criterios para la valoración de resultados, en términos de eficiencia, eficacia, efectividad y productividad.

Proyecto Tecnológico

Es un planteamiento administrativo de las organizaciones, enfocado al fortalecimiento de la infraestructura física y lógica de TI que debe contribuir a la ejecución operativa del core del negocio.

Cuando un negocio desea controlar sus proyectos tecnológicos colisionan dos paradigmas, el mundo de la administración de portafolios financieros y el mundo de la administración de proyectos de TI. En la implementación de portafolios de proyectos de IT, las organizaciones pueden orientarse más hacia la conservación del recurso financiero, afianzando decisiones ejecutivas o pueden orientarse más hacia el mundo TI afianzando los proyectos. La oportunidad que presenta una correcta administración de los proyectos tecnológicos es cómo combinar ambos alcances para fortalecer una organización en su infraestructura tecnológica[2]. Para el caso de las entidades colombianas, a partir de las cifras oficiales de inversión en actividades de ciencia, tecnología e innovación que reporta el Observatorio Colombiano de Ciencia y Tecnología (OCyT) en el libro de indicadores 2018, evidencian que desde el año 2011 este indicador comienza a incrementarse y el año con mayor inversión es el año 2013 donde la cifra fue 0,75% como porcentaje del PIB debido a la inclusión de recursos de Ciencia y Tecnología en el sistema general de regalías y en los siguientes años la cifras comienzan a disminuir. Es así, como el último dato reportada para el año 2018 de la inversión en actividades de ciencia, tecnología e innovación es del 0,61% como porcentaje del PIB. Los sectores que más aportan a este indicador son las empresas (51,94% de la inversión en ACTI) y el sector público como presupuesto general de la nación y regalías (22,34% de la inversión en actividades de ciencia, tecnología e

[2] Bonham, S. S. (2005). "IT Project Portfolio Management". Artech House, Inc. Pag. 117

innovación)[3]. Lo anterior sugiere un forcejeo entre la decisión de invertir en campos como TI y Seguridad Informática versus la percepción de favorecimiento al hacerlo.

Proyecto en Seguridad de la Información

Estrategias y lineamientos específicos dentro de un plan organizacional enfocado a la preservación de la seguridad de la información. Usualmente es un aparte de los PETIC de cada institución, sin embargo pueden ser tomados como proyectos administrativos independientes, aunque aún conectados a toda la base de proyectos de TI.

Generalmente existen lineamientos globales a nivel nacional y mundial que dictan las medidas básicas a implementar en este aspecto, los cuales deben ser alineados a las políticas internas de cada organización y por su puesto al mismo core del negocio.

Eficiencia

Es la capacidad del gestor de proyecto en virtud del alcance de los mejores resultados posibles con el aprovechamiento máximo de los recursos disponibles, incluyendo los recursos financieros, humanos, logísticos, etc.

[3] Portafolio.co. "El reto de invertir en ciencia, tecnología e innovación en Colombia". Tomado de: https://www.portafolio.co/economia/el-reto-de-invertir-en-ciencia-tecnologia-e-innovacion-en-colombia-529537. 18 de mayo de 2019.

Eficacia

Corresponde al logro de las metas, concebido como la satisfacción de resultados medidos a través de métricas que pueden ser representadas en indicadores.

Efectividad

Resulta de la articulación del logro de metas esperadas o proyectadas con una administración óptima de los recursos disponibles.

Productividad

Se habla de productividad cuando se contrastan los resultados o productos al final de la ejecución de un proyecto con respecto a los recursos empleados. Es una relación que denota un índice de beneficio al final de las tareas del proyecto.

Gestión de Proyectos

La administración y gestión de proyectos es el proceso de planificación, monitoreo, control, evaluación y ajuste de un conjunto único de tareas que tienen un inicio, un final y un resultado. El proceso de gestión de proyectos se lleva a cabo dentro de tres restricciones a saber: tiempo, costos y alcance. La meta de la gestión de proyectos es generar un producto técnicamente aceptable cuya consecución sea oportuna y dentro del presupuesto establecido. Con el fin de lograr esto, la gestión de proyectos intenta reducir los riesgos asociados con el proyecto a la par que intenta maximizar los beneficios, incluyendo la rentabilidad y mercadeo.

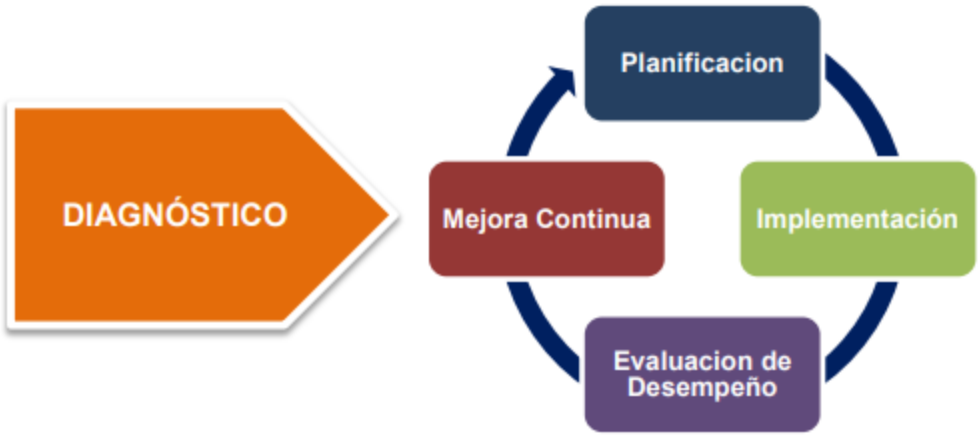
Gestión de Seguridad en la Información

Para el caso de la República de Colombia, además de la constitución política, en materia de gestión de seguridad de la información se define el proceder general a través del Modelo de Seguridad y Privacidad de la Información, el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión. Dicho modelo pretende facilitar la comprensión del proceso de construcción de una política de privacidad por parte de las entidades estatales, que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información[4].

En dicho modelo se establece un ciclo para la ejecución y monitoreo de las actividades para el logro de esta imperante meta con respecto a la protección de los datos, así:

Ilustración 2, "Ciclo de operación del Modelo de Seguridad y Privacidad de la Información"

[4] Ministerio de Tecnologías de la Información y las Comunicaciones. "Seguridad y Privacidad de la Información", 2016, Pág. 9.



Tomado de: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

También se conceptualiza en este modelo de manera detallada para las entidades gubernamentales, la fase de diagnóstico con sus correspondientes metas, resultados y lo que es bastante adecuado, los instrumentos MSPI que Mintic ha puesto a disposición para que sirvan como apoyo y hoja de ruta en estos procesos. De igual manera los lineamientos específicos vienen supeditados a cada fase a evaluar, continuando con la planificación, implementación, evaluación de desempeño y mejora continua.

Gestión de Seguridad de la Información para el Departamento Administrativo Nacional de Estadística

El Departamento Administrativo Nacional de Estadística, mediante Resolución No. 0447 del 22 de marzo de 2019, por la cual "adopta y las Políticas de Gobierno Digital y Seguridad Digital,

se designa al Líder de Gobierno y Seguridad Digital y se dictan otras disposiciones", complementada posteriormente a través de la Resolución 1024 de 28 de junio de 2019, a través de la cual "se adopta el Registro de Activos de Información".

A través de la primera, se crea además un Comité Operativo de Tecnologías de Información, el cual cumple las funciones de ser enlace operativo y de comunicación entre las dependencias y la Oficina de Sistemas para los temas concernientes al Gobierno Digital y la Seguridad Digital, así como Liderar y ser multiplicadores de las actividades de sensibilización, comunicación y apropiación que organice la Oficina de Sistemas[5].

Metodología de Gestión de Seguridad de la Información

Existen varios métodos para ayudar al gestor o director de proyectos en la planificación, organización y administración de tareas en concordancia con las restricciones existentes, y de esa manera lograr el objetivo final del proyecto. No obstante, la metodología relevante para el presente escrito es la ISO 27001:2013, considerada como el estándar principal internacional que apunta a "especificar los requerimientos para establecer, implementar, mantener y mejorar continuamente un sistema de administración de seguridad de la información"[6], y se integra a las organizaciones a nivel mundial con el propósito de ayudar a asegurar los recursos de información. Sus aplicaciones permiten a la organización a determinar y evaluar los riesgos de seguridad de la información y a implementar procedimientos y mecanismos que preservan su integridad, confidencialidad y disponibilidad. Con esto, las organizaciones públicas pueden

[5] Departamento Administrativo Nacional de Estadística. "Resolución 0447, Gobierno Digital". 2019, página 4.
[6] IPQ - Instituto Português da Qualidade, I.P., «NP ISO/IEC 27001:2013 - Tecnologia de informação -- Técnicas de segurança -- Sistemas de gestão de segurança da informação - Requisitos». IPQ - Instituto Português da Qualidade, I.P., 2013.

evaluar todas las estrategias de manera cíclica para mejorarlas y mantenerlas[7].

En este estándar también se contempla la administración de incidentes. La estructura del estándar indica que esta operación sigue el ciclo de mejora PHVA, también presente en el estándar ISO 9001, el cual apunta a hacer que los procesos de administración sean más ágiles, claros y objetivos.

Planificar: La norma nos dice que se debe:

- Establecer los objetivos del sistema y sus procesos.
- Establecer los recursos necesarios para generar y proporcionar resultados de acuerdo con los requisitos del cliente y las políticas de la organización.
- Identificar y abordar los riesgos y las oportunidades.

Hacer: Implementar lo planificado. La norma ISO 9001 se relaciona esta fase con los capítulos 7 y 8. La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la calidad. La organización debe considerar:

- Las capacidades y limitaciones de los recursos internos existentes;
- Qué se necesita obtener de los proveedores externos

Verificar: Realizar el seguimiento y (cuando sea aplicable) la medición de los procesos y los productos y servicios resultantes respecto a las políticas, los objetivos, los requisitos y las actividades planificadas, e informar sobre los resultados. Se encuentra en el Capítulo 9. La

[7] CARVALHO, Carla. "Adapting ISO 27001 to a Public Institution". 2019, Pág. 1. Tomado de: http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=1&sid=449e1b8b-727b-462a-9755-0529ff5f6587%40sessionmgr4006

organización debe determinar:

- Qué necesita seguimiento y medición.
- Los métodos de seguimiento, medición, análisis y evaluación necesarios para asegurar resultados válidos.
- Cuándo se deben llevar a cabo el seguimiento y la medición.
- Cuándo se deben analizar y evaluar los resultados del seguimiento y la medición.

Actuar: Es necesario tomar acciones para mejorar el desempeño, cuando sea necesario. El capítulo 10 Mejora, indica que la empresa tiene que determinar y seleccionar las oportunidades de mejora e implantar cualquier acción que sea necesaria para cumplir con los requisitos del cliente. Deben incluir:

- Mejorar los productos y servicios para cumplir los requisitos, así como considerar las necesidades y expectativas futuras.
- Corregir, prevenir o reducir los efectos no deseados.
- Mejorar el desempeño y la eficacia del sistema de gestión de la calidad.[8]

Herramientas para la Gestión de Seguridad de la Información

En general, las herramientas para la Gestión de la Seguridad de la Información son principalmente documentales, procedimientos, procesos y lineamientos que otorgan las medidas, línea base y proceder para cada una de las actividades concernientes a este tema. No obstante, lo anterior, se pueden enlistar de la siguiente manera:

[8] "ISO 9001 y el ciclo PHVA". Tomado de: https://www.nueva-iso-9001-2015.com/2019/05/ciclo-phva-en-iso-9001/

Seguridad Física

Consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales, incendios accidentales tormentas e inundaciones.
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos deliberados.

De igual manera se pueden tener acciones hostiles que pongan en riesgo la infraestructura física que soporta los servicios tecnológicos en donde se alojan los activos de información del DANE, tales como:

- Robo.
- Fraude.
- Sabotaje.

En este nivel, se deben establecer controles de acceso a las áreas vulnerables y sensibles, usando guardias, detectores de metales, sistemas biométricos, verificación automática de firmas, seguridad con animales o protección electrónica.

Seguridad Lógica

Consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Para lograr lo anterior, se requieren controles como restringir el acceso a los programas y archivos, asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan, asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto, que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro, que la información recibida sea la misma que ha sido transmitida, que existan sistemas alternativos secundarios de transmisión entre diferentes puntos y que se disponga de pasos alternativos de emergencia para la transmisión de información.

De manera similar a la seguridad física se deben implementar mecanismos de control de acceso como Identificación y Autentificación, Roles, transacciones, Limitaciones a los Servicios, modalidad de acceso, ubicación y horario, controles de acceso interno y externo y administración.

Como una mezcla de los anteriores dos temas, se deben establecer controles de acceso a copias de seguridad de equipos y acceso a copias de seguridad de servidores.

Políticas de Seguridad

Es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema."

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero... ante todo, "(...) una política de seguridad es una forma de comunicarse con los usuarios... Siempre hay que tener en cuenta que la seguridad comienza y termina con personas." y debe:

- Ser holística (cubrir todos los aspectos relacionados con la misma). No tiene sentido proteger el acceso con una puerta blindada si a esta no se la ha cerrado con llave.
- Adecuarse a las necesidades y recursos. No tiene sentido adquirir una caja fuerte para proteger un lápiz.
- Ser atemporal. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.[9]

Niveles de Acceso a la Información

En este punto, teniendo que ser definido específicamente para los roles y procesos del objeto de estudio, se deben al menos considerar la gestión de:

- Programas de Control
- Administración de Contraseñas
- Niveles de acceso
    - Consulta de la información no restringida o reservada.
    - Mantenimiento de la información no restringida o reservada.
    - Consulta de la información incluyendo la restringida o reservada.

[9] Instituto de Financiamiento, Promoción y Desarrollo de Tuluá. “Políticas de Seguridad Informática”. 2017, página 7.

- Mantenimiento de la información incluyendo la restringida.

Marco de Gestión COBIT

Las mejores prácticas en auditoria recomiendan Cobit, como la herramienta estándar para tecnologías de información más utilizada en la ejecución de auditorías; a continuación se explica detalladamente algunos conceptos manejados por ésta y los dominios, procesos y actividades que lo conforman[10]:

- Efectividad: se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- Eficiencia: se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
- Confidencialidad: se refiere a la protección de información sensible contra divulgación no autorizada.
- Integridad: se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
- Disponibilidad: se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- Cumplimiento: se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de

[10] IT Governance Institute. redyseguridad. 4 de Diceimbre de 2013. Tomado de: http://redyseguridad.fip.unam.mx/proyectos/cobit/seccion_informativa/pdfscobit/resumen_ejecutivo.pdf

negocio impuestos externamente.

- Confiabilidad de la información: se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.
- Datos: los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, entre otros.
- Aplicaciones: se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.
- Tecnología: la tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, entren otros.
- Instalaciones: recursos para alojar y dar soporte a los sistemas de información.
- Personal: habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

Se fundamenta en 5 principios que permiten a la empresa construir un efectivo marco de gobierno y administración de TI y se basa en un conjunto holístico de 7 habilitadores, considerando las tendencias actuales de gobierno y administración alineado con otros marcos de referencia.

Los cinco principios de COBIT 5:

1. Satisfacer las necesidades de los interesados.
2. Cubrir la empresa de extremo a extremo.
3. Aplicar un solo marco integrado.

4. Habilitar un enfoque holístico.
5. Separar Gobierno de Administración.

Cobit 5 cuenta con una guía genérica de procesos que divide en cinco categorías:

- Evaluar, Orientar y Supervisar (EDM).
- Alinear, Planificar y Organizar (APO).
- Construir, adquirir e implementar (BAI).
- Entrega, Servicio y Soporte (DSS).
- Supervisar, Evaluar y Valorar (MEA).

Para el desarrollo del marco de buenas prácticas, se utilizarán de los procesos APO las métricas representadas en indicadores claves de desempeño y los factores críticos de éxito, para monitorear y controlar los avances o entregables que se desarrollan en la etapa contractual y se desarrollarán las fórmulas para el cálculo del porcentaje de cumplimiento con base en la metodología SMART, definida así por el acrónimo de específico (Specific), medible (Measurable), alcanzable (Achievable), orientado a resultados (Result-oriented) y a tiempo (Timely).[11]

ITIL

ITIL es considerada una de las mejores prácticas para la administración de servicios de tecnología, fue desarrollada por el gobierno del Reino Unido y globalmente es adoptada por

[11] PARRA ALVARADO, José Francisco. "Marco de Buenas Prácticas para la Planeación de la Adquisición de Servicios de TI en las Entidades Públicas Colombianas". Pág 72. Universidad Nacional De Colombia, 2019.

muchas organizaciones en el sector tanto público como privado.

Se puede afirmar que no es un estándar prescriptivo que es debe ser seguido al pie de la letra, no dice lo que debe hacerse en una organización proveedora de cualquier tipo de servicios y no hay un certificado para adoptar exitosamente este marco, por el contrario, es un marco de trabajo que las organizaciones pueden adoptar y adaptar para mejorar la manera en que entregan sus servicios de tecnología. Es ampliamente conocida como una fuente para las buenas prácticas. Soporta organizaciones a la par que estás entregan servicios de tecnología a sus usuarios[12].

Actualmente, ITIL recoge la gestión de los servicios TI como uno de sus apartados, habiéndose ampliado el conjunto de estas buenas prácticas a la gestión de la seguridad de la información, gestión de niveles de servicio, perspectiva de negocio, gestión de activos software y gestión de aplicaciones. Estas buenas prácticas provienen de las mejores soluciones posibles que diversos expertos han puesto en marcha en sus empresas en el momento de ofrecer servicios de TI. (Great Britain Office of Government, 2007).

La versión denominada como ITIL v3, fue divulgada en el año 2007, en la cual se agrupan los elementos principales de ITIL en 5 volúmenes: Estrategia del Servicio (ES), Diseño del Servicio (DS) Transición del Servicio (TS), Operación del Servicio (OS) y Mejora Continua del Servicio (MCS).

- Gestión de Servicios de TI

ITIL define el servicio como un medio para entregar valor a los clientes facilitándoles un resultado deseado sin la necesidad de que estos asuman los costes y riesgos específicos

[12] Agutter, C. (2013). ITIL Lifecycle Essentials : Your essential guide for the ITIL Foundation exam and beyond. ITGP. P. 33.

asociados.

Una correcta gestión de este servicio requerirá:

- Conocer las necesidades del cliente.
- Estimar la capacidad y recursos necesarios para la prestación del servicio.
- Establecer los niveles de calidad del servicio.
- Supervisar la prestación del servicio.
- Establecer mecanismos de mejora y evolución del servicio.

La metodología ITIL define la Gestión de Servicios como un conjunto de capacidades organizativas especializadas para la generación de valor a los clientes expresado en forma de servicios.

- El ciclo de vida de los servicios TI.

ITIL estructura la gestión de los servicios TI sobre el concepto de Ciclo de Vida de los Servicios. Este enfoque tiene como objetivo ofrecer una visión global de la vida de un servicio desde su diseño hasta su eventual abandono sin por ello ignorar los detalles de todos los procesos y funciones involucrados en la eficiente prestación del mismo.

El Ciclo de Vida del Servicio consta de cinco fases:

a. Estrategia del Servicio: Propone tratar la gestión de servicios no sólo como una capacidad sino como un activo estratégico (Great Britain Office of Government, 2013a).
b. Diseño del Servicio: Cubre los principios y métodos necesarios para transformar los objetivos estratégicos en portafolios de servicios y activos (Great Britain Office of Government, 2013b).

c. Transición del Servicio: Cubre el proceso de transición para la implementación de nuevos servicios su mejora (Great Britain Office of Government, 2013c).
d. Operación del Servicio: Abarca las mejores prácticas para la gestión del día a día en la operación del servicio (Great Britain Office of Government, 2013d).
e. Mejora Continua del Servicio: Proporciona una guía para la creación y mantenimiento del valor ofrecido a los clientes a través de un diseño, transición y operación del servicio optimizado (Great Britain Office of Government, 2013e)[13].

ISO 27001

Es la norma principal de la serie 27000 y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los Sistemas de Gestión de Seguridad de la Información de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO[14].

La norma ISO 27000 es certificable. Esto significa que una empresa puede solicitar una auditoría a una entidad certificadora acreditada y si la supera, obtener la certificación. Antes de solicitar la auditoría las empresas necesitan contar con un Sistema de Gestión de Seguridad de la Información (SGSI). El SGSI debe estar implementado en la empresa como mínimo con tres

[13] PARRA ALVARADO, José Francisco. "Marco de Buenas Prácticas para la Planeación de la Adquisición de Servicios de TI en las Entidades Públicas Colombianas". Pág 64. Universidad Nacional De Colombia, 2019
[14] AEC. AEC. [En línea] 2012. Tomado de: http://www.aec.es/web/guest/centro-conocimiento/norma-une-isoiec-27001.

meses de antelación.

Cada uno de los puntos exigidos en la norma pertenece a una etapa de un proceso: Plan – Do – Check – Act (Planificar-Hacer-Verificar-Actuar), que se aplica para estructurar todos los procesos del SGSI. El SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estas expectativas.

Sin embargo, al momento de realizar la auditoría, a algunos puntos se les da más relevancia que a otros:

- Política de seguridad: debe incluir los objetivos de seguridad de la información de la organización, tener en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, estar alineada con la gestión de riesgo general, establecer criterios de evaluación de riesgo y ser aprobada por la Dirección.
- Asignación de responsabilidades de seguridad: En toda actividad debe existir un responsable. Durante el proceso de certificación cada tarea debe estar definida para que una o unas personas de la organización la realicen.
- Formación y capacitación para la seguridad: debe realizarse una concienciación de todo el personal en lo relativo a la seguridad de la información.
- Registro de incidencias de seguridad: durante el proceso, debe realizarse un registro de los eventos casuales (incidencias), y determinar su impacto y frecuencia. Determinar controles de detección y respuesta a dichos incidentes.
- Gestión de continuidad del negocio: el SGSI definido, debe estar enfocado en mantener la continuidad del negocio, por lo tanto este objetivo no puede perderse en el camino de

implementación del sistema de seguridad.

- Salvaguarda de registros de la organización: la información hace parte de los activos de la organización, por lo tanto ésta debe preservarse y cuidarse como tal. Los registros de la organización ya sea del negocio o relacionados con el sistema de seguridad deben cumplir con las propiedades fundamentales: confidencialidad, integridad y disponibilidad.
- Protección de datos personales: hacen parte de la información de la organización y por ello deben ser protegidos.
- Derechos de propiedad intelectual: contar con las licencias y/o permisos para el uso de software en la organización.

Después que se ha implantado el SGSI en la organización, ésta solicita la auditoría a la empresa certificadora, la cual se realiza en varias fases:

- Pre-auditoría: es opcional, ayuda a recoger información sobre el estado de la organización antes de la auditoría real.
- Fase 1 de la auditoría: análisis de la documentación por parte del Auditor Jefe y la preparación del informe de la documentación básica del SGSI del cliente, destacando los posibles incumplimientos de la norma que se verificarán en la Fase 2. Este informe se envía junto al plan de auditoría al cliente. El periodo máximo entre la Fase 1 y Fase 2 es de 6 meses.
- Fase 2 de la auditoría: es la fase de detalle de la auditoría, en la que se revisan las políticas, la implantación de los controles de seguridad y la eficacia del sistema en su conjunto. Se realiza una revisión de las exclusiones según la Declaración de Aplicabilidad (documento SOA), de los hallazgos de la Fase 1, de la implantación de

políticas, procedimientos y controles y de todos aquellos puntos que el auditor considere de interés. El resultado es el informe de auditoría.

- Certificación: en el caso de que se descubran durante la auditoría no conformidades graves, la organización deberá implantar acciones correctivas; una vez verificada dicha implantación o en el caso de no haberse presentado inconformidades, el auditor podrá emitir un informe favorable y el SGSI de organización será certificado según ISO 27001.

Después de obtener la certificación debe hacerse un seguimiento, y realizar auditorías semestrales o anuales para verificar que el SGSI si se usa en la organización. La certificación debe renovarse cada tres años realizando nuevamente todo el proceso de auditoría.

El auditor es la persona que comprueba que el SGSI de una organización se ha diseñado, implementado, verificado y mejorado conforme a lo detallado en la norma. En general, hay tres clases de auditores: auditor interno (de primera parte), pertenece a la organización, realiza auditorías como mantenimiento del sistema de gestión y como preparación a la auditoría de certificación. Auditor de cliente (de segunda parte), audita una organización en nombre de un cliente de ésta. Finalmente está el auditor independiente (de tercera parte), que audita una organización como tercera parte imparcial; normalmente, porque la organización tiene la intención de lograr la certificación. El auditor, sobre todo si actúa como de tercera parte, ha de disponer también de una certificación personal. Esto quiere decir que, nuevamente un tercero, certifica que posee las competencias profesionales y personales necesarias para desempeñar la labor de auditoría de la materia para la que está certificado.

El proceso de certificación es largo, complejo y costoso, por lo que algunas empresas no pueden realizarlo. Sin embargo pueden aplicar algunos puntos claves para lograr un buen nivel de seguridad. Aunque el término buen nivel es subjetivo, sobre todo por el desconocimiento del

impacto negativo que pueda traer un riesgo que se materializa.

Algunas recomendaciones que deben tenerse en cuenta al momento de implementar un sistema de seguridad en la organización son las siguientes:

- La primera de ellas y tal vez la más importante, es el conocimiento de los altos directivos de lo que puede suceder si no se implementa el sistema de gestión de seguridad de la información. A la alta dirección debe hablársele en términos del negocio, es decir, demostrar las pérdidas económicas, que pueden tenerse en caso de no contar con un SGSI. De esta tarea puede encargarse el jefe del área de sistemas de la organización.
- Se debe realizar una identificación de los activos relacionados con la información, desde los equipos que la soportan hasta las aplicaciones para su uso y la información misma. Después identificar los más críticos para la compañía y con base en estos empezar la tarea de diseño e implementación del SGSI.
- Cuando las directivas de la organización tienen claro la necesidad de implantar un SGSI y han identificado los componentes críticos entre los activos, debe fomentarse una cultura de seguridad con todos los miembros de la organización para minimizar los riesgos por desconocimiento. Se debe tener en cuenta que plasmar en un papel algunas normas de seguridad no crean una cultura, es un proceso que debe realizarse de manera constante, ya que para generar cultura es necesario crear conciencia del cambio.
- Los expertos en el área de seguridad (jefe de área y otros trabajadores) deben ser los encargados de identificar las amenazas y debilidades que afectan a cada uno de los activos críticos. De esta forma se pueden definir los riesgos que afectan el proceso normal de la organización, incluyendo el impacto y la frecuencia con la que puedan ocurrir.

- Cuando se definen los riesgos, debe tenerse en cuenta que es imposible evitar o controlarlos todos, por eso en la organización debe definirse un nivel aceptable de riesgo, es decir, definir cuáles son los riesgos que se pueden asumir ya que no generarán un impacto muy negativo para el funcionamiento correcto de las actividades de la organización. La definición del nivel aceptable de riesgo debe estar bajo la responsabilidad directa de la alta gerencia de la organización y estar enfocado en el negocio y el cliente.
- Con los riesgos, el impacto, la frecuencia y el nivel aceptable se definen entonces, los controles que deben seguirse para evitar o minimizar los riesgos. Estos controles se enfocan en reducir el impacto, la frecuencia o evitar que el riesgo se materialice y cause un daño al correcto funcionamiento del negocio, que finalmente se verá reflejado en una pérdida o gasto económico.

Todo esto hace parte del Sistema de Gestión de Seguridad de la Información (SGSI), pero como ya se indicó anteriormente, es algo que no debe quedar sólo escrito. Hasta ahora se tiene únicamente el diseño.

- Después de tener el diseño del sistema de seguridad, debe empezar a aplicarse en la organización, para esto es necesario promover la capacitación de las personas que laboran en la organización, comprar e implantar los equipos y aplicaciones necesarios.
- Para que la implementación sea efectiva, debe hacerse un seguimiento a los controles y, para lograr este seguimiento es necesario la documentación de los procesos y de los hallazgos. Con esta información se realiza una retroalimentación para corregir errores que aún se mantienen y mejorar el SGSI incluyendo nuevos riesgos posibles o restándole importancia a aquellos que se han logrado minimizar.

Aunque estas recomendaciones parezcan demasiado complicadas, son más fáciles, y económicas, de implementar que la norma completa para lograr la certificación (especialmente si se trata de empresas pequeñas y medianas) ya que, para esta segunda es necesario, generalmente, la intervención de un tercero que ayude en el proceso como asesor[15].

SGSI

El sistema de gestión de la seguridad de la información (SGSI) es un conjunto de normas y controles, el cual busca ser un proceso sistemático, documentado, conocido y adoptado por toda la organización con el fin de garantizar que la organización realice una correcta gestión de la información, buscando dentro del mismo asegurar la disponibilidad, integridad y disponibilidad de los activos.

Un Sistema de Gestión de Seguridad de la Información es una herramienta que le permite a las organizaciones establecer políticas, procedimientos, medidas y controles de seguridad los cuales siempre tienen que estar alineados a los objetivos del negocio, y provee los elementos adecuados para la debida gestión del riesgo con el fin de poder mantener el mismo por debajo del nivel definido por la organización.[16]

Como parte de la documentación del Sistema de Gestión de Seguridad de la Información se tienen entre otros los siguientes documentos considerados:

- Procedimientos de seguridad.

[15] LADINO A., Martha Isabel, VILLA S., Paula Andrea, LÓPEZ E., Ana María. "FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS". Pág. 35. Universidad Tecnológia de Pereira. 2011.
[16] HURTADO PÉREZ, Andrés, ROBAYO GONZÁLEZ, Omar. "DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI- PARA LOS PROCESOS CRÍTICOS DE LA COOPERATIVA FEBOR BASADO EN LA NORMA ISO 27001:2013" 2019, Página 33.

- Procedimientos de Auditorías Internas.
- Gestión de Indicadores.
- Procedimiento de Revisión por la Dirección.
- Gestión de Roles y Responsabilidades.
- Metodología de Análisis de Riesgos.

Procedimiento de seguridad

es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los Procedimientos de Seguridad permiten aplicar e implantar las Políticas de Seguridad que han sido aprobadas por la organización. Se describe cómo se implementan, en las áreas a proteger, las políticas generales que han sido definidas para toda la entidad, en correspondencia con las necesidades de protección en cada una de ellas, atendiendo a sus formas de ejecución, periodicidad, personal participante y medios.

Para cada uno de estos documentos se tiene la misma estructura con el fin de conservar una consistencia en toda la documentación, la estructura del documento contendrá además de un encabezado en donde se registrará título del procedimiento, código establecido por manual de calidad y administración documental, un subtítulo, un responsable, un numero de edición, un campo de aprobación, una fecha, total de páginas y anexos si contiene, además de un control de cambios del documento.

Procedimientos de Auditorías Internas:

Verificar si el sistema de gestión de seguridad de la información opera de acuerdo con los planes, procedimientos, registros y controles establecidos y es conforme con los requisitos de la norma ISO 27001:2013 y es eficaz para satisfacer los requisitos relacionados con seguridad de la información

Gestión de Indicadores:

Es donde se implementan indicadores de gestión para mantener monitorizado y actualizado del SGSI, los cuales permiten controlar el funcionamiento de las medidas de seguridad implementadas, eficacia y eficiencia.

Procedimiento de Revisión por la Dirección:

El Sistema de Gestión de Seguridad de la Información contempla una evaluación periódica, sistemática y estructurada a cargo de la Alta Dirección que permite asegurar una adecuada planeación y la corrección de las desviaciones en el cumplimiento de los objetivos y como tal, incluye la toma de decisiones sobre acciones necesarias, que dentro de un marco de conveniencia razonable para la organización, promueva el mejoramiento de productos, procesos y capacidades organizacionales que permitan alcanzar resultados de eficiencia, eficacia y efectividad.

Gestión de Roles y Responsabilidades:

El Sistema de Gestión de Seguridad de la Información define los diferentes roles y

funciones. Entre estas definiciones de roles y responsabilidades se podrán identificar alguno de los siguientes ítems:

- Quien es el responsable de la ejecución de cada hito.
- Quien toma las decisiones, solo o conjuntamente con otros.
- Quien gestiona los recursos y controla el progreso del trabajo.
- Quien debe ser informado.
- Quien debe ser consultado.
- Quien debe participar.
- Quien debe dar apoyo o dotar de infraestructura al equipo.
- Quien asegura la calidad de los resultados.

Metodología de Análisis de Riesgos

La realización del análisis de riesgos tiene como fin identificar de manera clara los riesgos a los cuales está expuesta la organización, y basados en esta identificación de los riesgos determinar cuáles medidas de seguridad serán las adecuadas para los diferentes activos de seguridad de la información, de igual manera permite establecer los planes de contingencia, para este caso realizaremos un análisis de riesgo residual, que es un tipo de análisis que se realiza teniendo en cuentas las medidas de seguridad que la organización ya tiene planteadas, como resultado de este tipo de análisis se obtiene el riesgo real al cual están expuestos los diferentes activos de la información que tiene la organización.

MAGERIT como metodología de Análisis de Riesgos.

MAGERIT es un instrumento para facilitar la implantación y aplicación del Esquema Nacional de Seguridad proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información.

MAGERIT permite:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. El análisis de riesgos considera los siguientes elementos:
    1. Activos: Son los recursos del sistema de información o relacionados con este, necesarios para que funcione correctamente y alcance los objeticos propuestos por la dirección.
    2. Amenazas: Son las situaciones o hechos que pueden producir daño y que les pueden pasar a los activos causando un perjuicio a la organización.
    3. Vulnerabilidades: Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre un activo de la información.
    4. Impacto: Daño causado sobre el activo de la información una vez se materializa una

de las vulnerabilidades, conociendo el valor de los activos es más sencillo estimar el valor del impacto.

5. Riesgo: Es la probabilidad de que una amenaza se materialice y afecte a los activos de la información.
6. Salvaguardas: Mecanismo de protección frente a las amenazas.

Al análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de que perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar que salvaguardas hay dispuestas y cuan eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Declaración de aplicabilidad:

Es una relación con todos los controles de la norma en donde se observa si existen controles, y la razón de la selección de cada uno de ellos, resaltando si el control surge de un requerimiento legal, de una obligación contractual, de un requerimiento de negocio o de las mejores prácticas, o si el control surge como resultado del análisis de riesgos realizado a los activo de información de

la organización[17].

SGSI DANE

El DANE reconoce la información y en especial a los datos utilizados para producir estadísticas, como los activos más importantes de la Entidad; por lo tanto, se compromete a proteger la privacidad y seguridad de la misma, cumpliendo con los mandatos de la constitución y la ley de reserva estadística, promoviendo la confianza y cooperación de los ciudadanos.

De acuerdo con las facultades otorgadas al Ministerio de las TIC, para generar estrategias de implementación y evaluación del modelo de seguridad y privacidad de la información en las entidades del Estado, y al Decreto 2573, "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea". El DANE a través de la Oficina de Sistemas adelanta el desarrollo de los requerimientos de la norma ISO 27001 / 2013, a través de un plan estructurado, buscando el debido cumplimiento de los tiempos estimados por la ley, sin dejar de alinear el SGSI1 al Sistema Integrado de Gestión Institucional SIGI.

El DANE en su Misión de Producir y difundir información estadística de calidad para la toma de decisiones y la investigación en Colombia, así como desarrollar el Sistema Estadístico Nacional está obligado a proteger la información a través del cumplimiento de disposiciones nacionales. Alineándose a las directrices de MINTIC y apoyándose en la norma ISO 27001[18]

[17] MAYA A., Paula Andrea. "Plan de implementación del SGSI basado en la Norma ISO 27001:2013". Pág. 63. Universitat Oberta de Catalunya, 2016.
[18] Departamento Administrativo Nacional de Estadística. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI). 2019.

Ilustración 3, Cumplimiento para Entidades del Orden Nacional en Colombia

Sujetos Obligados del Orden Nacional

Componente/Año	2015	2016	2017	2018	2019	2020
TIC para ser servicios	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para Gobierno abierto	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	25%	50%	80%	100%	Mantener 100%	Mantener 100%
Seguridad y Privacidad de la Información	40%	60%	80%	100%	Mantener 100%	Mantener 100%

Ilustración 7 – Cumplimiento para Entidades del Orden Nacional

Tomado de: https://www.funcionpublica.gov.co/web/eva/preguntas-frecuentes/-/asset_publisher/7EbdP9CIenBf/content/estructura-organizacional/418537?_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_7EbdP9CIenBf_redirect=https%3A%2F%2Fwww.funcionpublica.gov.co%2Fweb%2Feva%2Fpreguntas-frecuentes%3Fp_p_id%3Dcom_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_7EbdP9CIenBf%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_7EbdP9CIenBf_cur%3D0%26p_r_p_resetCur%3Dtrue%26_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_7EbdP9CIenBf_assetEntryId%3D28746986

En cuanto a los Beneficios documentados para el DANE, el SGSI establece un plan de

acciones que ayuda a la entidad a identificar, controlar, mitigar o asumir los problemas de seguridad técnicos, de estructura organizacional y normativa, mediante el análisis de riesgos, mejorando y manteniendo los pilares de la seguridad de la información y contribuyendo con la continuidad de las operaciones estadísticas de la entidad. La implementación, operación y mantenimiento del SGSI aporta los siguientes beneficios:

- Minimizar daños.
- Retorno de la inversión.
- Continuidad del negocio.
- Cultura ética.
- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o daño de la información.
- Acceso de los usuarios a la información, con consistentes medidas de seguridad.
- Revisión permanente de los riesgos y los controles.
- Generación de confianza entre los usuarios debido a la garantía de calidad y confidencialidad de la información.
- Auditorías externas que ayudan a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión, como el Sistema de Gestión de la Calidad (ISO 9001), el Sistema de Gestión Ambiental (ISO 14001).
- Conformidad con la legislación vigente. Decreto 2573 de 2014 “Lineamiento de la estrategia de gobierno en línea”.
- Solidez de la imagen de la entidad.
- Confianza y reglas claras para las personas de la organización.

- Reducción de costos y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.[19]

Ataque Informático

Un ataque informático consiste en que un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático, ya sea el caso de un host, una red privada o un servidor, lo cual tendrá como consecuencia perdida de información y/o pérdidas económicas en alguna organización. Por ello la seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar enfocada a proteger la propiedad intelectual y la información relevante de las organizaciones y personas. Por ejemplo, las redes inalámbricas 802.11 que están en constante crecimiento actualmente, tienen la ventaja de ser flexibles y adaptarse a la infraestructura de las organizaciones, pero la desventaja que conlleva es que es vulnerable a cualquier tipo de ataque informático.[20]

Ingeniería Social

Es uno de los elementos principales y más actuales para los ataques informáticos, el cual ha ido en creciente progreso a la par con el despliegue y utilización de las tecnologías de la información en la población mundial.

[19] Departamento Administrativo Nacional de Estadística. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI). 2019.
[20] Medina Rojas, Jhonatan Deyvi; Rivas Montalvo, Yonathan Yajanovic. "Evaluación del Rendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos" 2020.

La Ingeniería Social se sustenta en un sencillo principio: “el usuario es el eslabón más débil”. Dado que no hay un solo sistema en el mundo que no dependa de un ser humano, la Ingeniería Social es una vulnerabilidad universal e independiente de la plataforma tecnológica. A menudo, se escucha entre los expertos de seguridad que la única computadora segura es la que esté desenchufada, a lo que, los amantes de la Ingeniería Social suelen responder que siempre habrá oportunidad de convencer a alguien de enchufarla[21].

El aumento de múltiples opciones en internet para tener una red social como Facebook, Instagram, Twitter, entre otras, es directamente proporcional a la necesidad del ser humano de consumir servicios como estos, compartir información personal y hacerla pública es la que aprovechan los ciberdelincuentes para vulnerar las personas y conseguir sus objetivos, que por lo general no son nada buenos. Los ataques de ingeniería social han ido en aumento día tras día y la estrategia que utilizan los ciberdelincuentes supone un gran trabajo de investigación para ellos, lo que los lleva también a ser cada vez más eficientes y obtener mejores resultados, la eficiencia de esta modalidad es por lo siguiente:

1. Primero recolectan toda la información posible extrayéndola de las redes sociales, para ello se registran en las plataformas creando perfiles falsos ya sea en Facebook, Twitter, LinkedIn, etc.
2. Consolidan un plan de ataque para transmitir fiabilidad.
3. Recolectan información particular, entienden su comportamiento (temas de interés, amigos, gustos, etc.), y ganan su confianza.

[21] M. Mercè. (2002, Dic 26). “Ingeniería Social: Mentiras en la Red”. Tomado de: http://ww2.grn.es/merce/2002/is.html

4. El atacante hace su primer acercamiento (con un falso perfil) teniendo ya definida la táctica de engaño que va a utilizar.
5. Cuando la víctima lo considera "su amigo," el delincuente se muestra cercano y siempre intentará sonsacarle aún más información a través de mentiras.
6. Una vez siendo "amigos," el ciberdelincuente pedirá datos más personales (correo electrónico, dirección, número de teléfono, etc.).
7. En este punto, la identidad podría suplantar de una manera más rápida y eficiente, o se le enviaría a través de correo electrónico un enlace llamativo que al abrirlo ejecutase un troyano que infecta el computador y diera acceso a las cuentas bancarias de la víctima.
8. Después de obtener lo que buscaba el atacante borra todo rastro, abandona perfiles y no vuelve a hablar con la víctima[22].

Phishing

El phishing es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

El escenario de Phishing generalmente está asociado con la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en el sitio web original, en lugar del falso. El engaño suele llevarse a cabo a través de correo electrónico y, a menudo estos correos contienen enlaces a un sitio web falso con una apariencia casi idéntica a un sitio legítimo. Una vez en el sitio falso, los usuarios incautos son engañados para que ingresen sus datos confidenciales, lo que les

[22] ROMERO, Diego. "EL ARTE DE LA INGENIERÍA SOCIAL". Pág. 3. Universidad Piloto de Colombia, 2016.

proporciona a los delincuentes un amplio margen para realizar estafas y fraudes con la información obtenida.

La principal manera de llevar adelante el engaño es a través del envío de spam (correo no deseado) e invitando al usuario a acceder a la página señuelo. El objetivo del engaño es adquirir información confidencial del usuario como contraseñas, tarjetas de crédito o datos financieros y bancarios. A menudo, estos correos llegan a la bandeja de entrada disfrazados como procedentes de departamentos de recursos humanos o tecnología o de áreas comerciales relacionadas a transacciones financieras[23].

Baiting

Consiste en dejar dispositivos de almacenamiento extraíble (CD, DVD, USB) infectados con algún software infectado en algún lugar a la vista (por ejemplo, baños públicos, ascensores, aceras, etc.), esperando a que alguien los recoja y conecte a su dispositivo. Al hacerlo, aquél afortunado que encontró un USB misterioso el cual el software malicioso se instalara y permitirá que el hacker obtenga los datos personales del usuario[24].

Hacker.

Persona apasionada por la seguridad de la información con avanzados conocimientos en el área de la informática tiene un desempeño extraordinario en el tema y es capaz de realizar muchas actividades desafiantes en plenitud tiene la capacidad de dominar en un buen porcentaje varios

[23] Cortés Hernández, Andrés Mauricio. "INGENIERÍA SOCIAL: PHISHING Y BAITING", Página 3.
[24] IBID, Pág. 3

aspectos como: lenguajes de programación, manipulación de hardware y software, telecomunicaciones; estas habilidades las utiliza con un buen fin, apoyando a empresas en el área de seguridad informática y de la información para solventar las brechas de seguridad y apoyar al área del SOC (Security Operation Center)[25].

Cracker

Es considerado un vandálico virtual. Este utiliza sus conocimientos para invadir sistemas, descifrar claves y contraseñas de programas y algoritmos de encriptación, ya sea para poder correr juegos sin un CD-ROM, o generar una clave de registro falsa para un determinado programa, robar datos personales, o cometer otros ilícitos informáticos. Algunos intentan ganar dinero vendiendo la información robada, otros sólo lo hacen por fama o diversión. Es por ello por lo que se debe tener diferentes capas de seguridad en cada compañía como en cada ordenador personal con el fin de ser precavidos con el manejo de la información[26].

Protección de datos en Colombia

La protección de datos personales en Colombia es uno de los fundamentos en que se basa la estrategia de Gobierno en Línea, abarcando un apartado para los Derechos de los Usuarios en relación a sus datos personales, según los cuales en cumplimiento de lo dispuesto en la normativa aplicable se informa de la existencia de un fichero automatizado de datos personales. Al usuario se le reconocen los derechos de acceso, rectificación, cancelación y oposición al tratamiento de

[25] IBID, Pág. 4
[26] IBID. Pág. 5

datos personales y podrá ejercitarlos mediante un formulario de actualización de datos disponible en el sitio de MINTIC[27].

[27] Ministerio de Tecnologías de la Información y las Telecomunicaciones. “Políticas de Privacidad”. Tomado de: https://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7935.html

Aspectos Metodológicos

Consideraciones Legales

El marco legal para la administración y gestión de la seguridad de la información en Colombia, parte de principios básicos generalizados en todo el mundo, fundamentados en las premisas que ya se conocen: confidencialidad, integridad y disponibilidad.

Es importante recalcar el hecho de que todos los aspectos de seguridad de la información deben estar en pleno cumplimiento de las normas y legislación vigente, sobre todo en lo que concierne a los derechos informáticos de los usuarios. Esto debe ir perfectamente armonizado con los dominios que presentan los estándares usados y exigidos a las entidades de orden Nacional, tales como los dominios de la norma ISO 27001:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos.
4. Seguridad de Recursos Humanos.
5. Seguridad Física y del Entorno.
6. Gestión de Comunicaciones y Operaciones.
7. Control de Acceso.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes de la Seguridad de la Información.
10. Cumplimiento.

Entre estos, resalta singularmente el dominio de Seguridad de Recursos Humanos que se

refiere al manejo y administración del personal con respecto a sus permisos, accesos, plazos y responsabilidades, situación que se aborda desde dos perspectivas:

- Análisis del acceso a la información misional de la entidad y sus correspondientes restricciones y permisos, con el fin de analizar cuál es la frontera real del acceso a la información, además de la rigurosidad con que se aplican los controles requeridos.
- Análisis del acceso a la información de seguridad de la información, la cual para efectos de análisis de esta monografía, está soportada en el documento "Acuerdo de Confidencialidad entre Carlos Alberto Ortíz Aux y el Departamento Administrativo Nacional de Estadística", el cual contempla entre otros apartes obligaciones como parte receptora de la información:
    - Mantener la información confidencial segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.
    - Proteger la información confidencial, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma del Departamento Administrativo Nacional de Estadística DANE, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.
    - Abstenerse de publicar la información confidencial que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.
    - Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

- Mantener la información confidencial en reserva hasta tanto adquiera el carácter de pública.
- Responder por el mal uso que le den sus representantes a la información confidencial.
- Guardar la reserva de la información confidencial como mínimo, con el mismo cuidado con la que protege la información confidencial.
- La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial sin el previo consentimiento por escrito por parte del Departamento Administrativo Nacional de Estadística DANE.
- La parte receptora se compromete a establecer que los datos a utilizar son: Planes y Programas, Publicaciones en la Intranet y en el Portal Corporativo, registro de incidentes. Se tendrá en cuenta que si existe información como nombre, apellido, cédula, teléfono estas deben ser amparadas por la ley 1581 de 2012 y no puede ser revelada en el documento final del proyecto.
- La información capturada por la parte receptora se observará como cifras para estudio estadístico, comparativo, información cualitativa, cuantitativa, análisis de casos de uso, no existirá ningún tipo de ganancia económica, es netamente educativo.
- La identidad de todo el personal del Departamento Administrativo Nacional de Estadística DANE no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

- Las pruebas realizadas por la parte receptora nunca pondrán en peligro los activos tecnológicos del Departamento Administrativo Nacional de Estadística DANE, ni violentará la ley de delitos informáticos Colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.
- El estudiante CARLOS ALBERTO ORTÍZ AUX se compromete a difuminar, bloquear y ocultar toda información que revele la identidad del Departamento Administrativo Nacional de Estadística DANE para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el repositorio institucional y de acceso público.
- El título del proyecto no podrá contener el nombre de la empresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

A pesar de que los elementos descritos en el segundo punto de abordaje son similares para otras investigaciones, es singularmente particular en este caso dado que el acceso a los datos de seguridad de la información es parte tanto de los requerimientos del trabajo de grado como parte funcional de la misma investigación.

Ahora bien, bajo esta perspectiva se encuentra viabilidad por parte de la entidad para remembrar y analizar datos relacionados con ataques informáticos tendientes a obtener o aprovechar indebidamente datos que son protegidos por ley, enfocándose en aquellos que usan la ingeniería social como medio predilecto en su actuar delictivo.

En el ámbito institucional, el Departamento Administrativo Nacional de Estadística debe garantizar la Protección de Datos Personales, dado que es la organización gubernamental que más datos de este tipo recopila.

La norma ISO 27001 señala en el dominio A.15.1.4., referido a la protección de datos, como control el siguiente: "Se debe garantizar la protección de los datos personales y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica con las cláusulas del contrato".

Para el cumplimiento de este control, quizás el referente internacional más representativo en materia de Protección de Datos Personales es la Directiva 95/46/CE, la cual establece el marco de regulación para los países miembros de la Unión Europea; norma que ha sido desarrollada en cada uno de esos países, producto de la conciencia de los ciudadanos sobre el destino de sus datos y el compromiso del Estado de garantizar las libertades públicas vinculadas al derecho fundamental a la intimidad.

Para el caso de Colombia, se refiere la ley 1266 de 2008, “Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”, a través de la cual se encuentra el rigor que debe tenerse en el cumplimiento de este derecho legal, haciendo que de esta manera se pueda garantizar, que en la recolección, tratamiento y circulación de datos, se respetarán los demás derechos consagrados en la ley[28].

Por parte del operador de bancos de datos, en este caso el Departamento Administrativo Nacional de Estadística se debe contemplar el Régimen General de Protección de Datos Personales. Ley 1581 del 2012 y los decretos 1377 de 2013 y 886 de 2014 que aplican sobre la ley 1581. Esta ley estatutaria fija los principios para el tratamiento de estos datos sensibles, así:

[28] Ley Estatutaria 1266 De 2008. Congreso de la República de Colombia, 2008.

a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;
b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;
c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;
d) Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;
e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;
f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley; Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para

brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

h) Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.[29]

De esta manera se destacan los principios de Seguridad y de Confidencialidad, que a través de esta ley denotan singular requerimiento de protección contra ataques cyber criminales, como en el caso de la ingeniería social como es en este caso de estudio.

En este orden de ideas, para ilustrar la problemática de la intimidad y el habeas data ha de entenderse el concepto de dato de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables", los cuales pueden ser generales, como nombre, domicilio y documento de identidad; hasta información sensible como ideología política, estado

[29] Ley Estatutaria 1581 de 2012, Congreso de la República. 2012.

de salud, tendencias sexuales, credo religioso, grupo étnico, entre otros.

En la economía actual, los datos de carácter personal están sometidos a tratamientos o procedimientos técnicos que permitan recabarlos, modificarlos, bloquearlos, cancelarlos, cederlos o transferirlos a terceros, así como definir perfiles de distinta naturaleza según la información que se desee obtener, acudiendo para ello a programas de minería de datos, que terminan entregando información valiosa sobre los hábitos de consumo de un individuo.

Esta posibilidad de que terceros puedan acceder sin control a la información personal de un individuo es lo que busca proteger el habeas data, en el sentido de que la información personal que sea confiada a una organización por su titular, esté amparada y protegida de usos ilegítimos que desconozca esa tutela constitucional que cada individuo tiene sobre su información, así como sobre los perfiles diseñados a partir de sus hábitos, comportamientos y tendencias.

En consecuencia, en materia de seguridad de la información y en desarrollo de este Derecho Fundamental, consignado en el dominio de la norma ISO 27 001 antes citado, debe procurarse por la organización que toda base de datos, tenga connotación comercial o no, cuente con las medidas jurídicas, tecnológicas y físicas que aseguren su protección.

La ausencia de una norma como la europea antes mencionada, en un determinado país, conduce a que gran parte de las bases de datos en poder de entidades públicas como privadas sean explotadas de manera ilegítima, a partir del abuso, ignorancia o desconocimiento de los derechos que tienen los individuos sobre la información confiada.

En materia de seguridad de la información, tratándose de datos personales, ha de recordarse que la protección a brindar se predica tanto de personas naturales como de personas jurídicas. En cumplimiento del postulado del dominio de la norma ISO 27 001, las organizaciones en la

ejecución de proyectos contratados con terceros no pueden dejar al margen la regulación contractual de las obligaciones que éstos deben acatar para asegurar que las medidas de seguridad de la información personal adoptadas por ella sean realmente eficaces.

Los deberes, cargas, obligaciones, riesgos y sanciones que puedan pesar sobre los titulares de las bases de datos personales no desaparecen por encargar a terceros el tratamiento de tales datos, por el contrario, pueden incrementar el valor de estas por no haber tomado las medidas adecuadas. Igualmente, los terceros a los cuales se encomiende el tratamiento de bases de datos con información personal son responsables por el uso ilegítimo que hagan de los mismos, y en consecuencia serán responsables de los perjuicios que irroguen a los individuos titulares de los datos personales.

El no dotar a las bases de datos personales de la seguridad y medidas de protección adecuadas por parte de las organizaciones que las poseen, en primer lugar implica un desconocimiento de lo dispuesto en la norma ISO 27 001; segundo, la violación a un derecho constitucional, el cual puede ser garantizado a través de acciones de tutela, con el riesgo de indemnizar los perjuicios causados; tercero, es una limitante en el comercio internacional, pues los países europeos y algunos latinoamericanos impiden la transferencia internacional de datos con países o empresas que no garanticen un nivel adecuado de protección de datos (no debe olvidarse el origen europeo de esta norma ISO), y por último, las sanciones que tienden a imponerse por violación a este derecho fundamental de la protección de datos personales y habeas data son muy cuantiosas en términos económicos.[30]

Como herramienta para sobrellevar esta delicada situación y responsabilidad se aprueba el

[30] VELASCO M., Arean Hernando. "el derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001", Pág. 344. 2008.

“Convenio sobre la ciberdelincuencia”, adoptado el 23 de noviembre de 2001 en Budapest, a través del cual el Congreso de la República adhiere esfuerzos en todos las partes responsables y beneficiarias del tema de la seguridad de la información a través de ciertas medidas internas que deben tomarse a nivel nacional, así:

Artículo 2. Acceso ilícito: Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Artículo 3. Interceptación ilícita: Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 4. Interferencia en los datos:

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

2. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves.

Artículo 5. Interferencia en el sistema: Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6. Abuso de los dispositivos:

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

i) Un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5;

ii) Una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático,

con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y

b) la posesión de alguno de los elementos contemplados en los anteriores apartados a.i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a

5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo[31].

Aunque prácticamente todos los apartados de esta sección influyen directa o indirectamente en el objeto de estudio de este documento, es conveniente focalizar hacia el acceso ilícito y hacia el abuso que puede presentarse a la hora de cometer un ciber crimen que se favorezca de las brechas de seguridad causadas por el factor humano.

Hacia la parte externa, es decir, frente a los usuarios, el DANE tiene soportes para requerir información sustancial para las operaciones estadísticas, tanto a nivel de persona como empresa, ya que se manipulan distintos tipos de investigaciones orientadas a distintos focos de información, hogares, índices de precios al consumidor, estadísticas vitales, encuestas económicas, entre otras.

Para ello la entidad exhorta al público en el evento de encontrar rechazos para contestar encuestas, en cuyo caso el doliente puede ser sujeto de requerimientos pre jurídicos que establecen sanciones según el artículo 6° de la Ley 0079 del 20 de octubre de 1993, que

[31] "Convention on Cybercrime", Budapest, 23 de Noviembre de 2001

determina: “El Departamento Administrativo Nacional de Estadística-DANE, podrá imponer multas por una cuantía entre uno (1) y cincuenta (50) salarios mínimos mensuales, como sanción a las personas naturales o jurídicas de que trata el artículo 5° de la presente Ley y que incumplan lo dispuesto en ésta u obstaculicen la realización del censo o de las encuestas, previa investigación administrativa”.

Resulta importante precisar, que de acuerdo con la ley 079 del 20 de octubre de 1993, los datos que el DANE solicita en estos formularios son estrictamente confidenciales y en ningún caso tienen fines fiscales ni pueden ser utilizados como prueba judicial.

No obstante lo anterior y a pesar de contar con el soporte legal para el levantamiento de esta información estadística, existe mucha renuencia basada en creencias populares las cuales pueden incrementarse en fuerza al exponerse vulnerabilidades de seguridad que posea la entidad, por lo cual en este aspecto, es fundamental la incidencia de estos ataques y sus correspondientes consecuencias y el impacto de la Ingeniería Social sobre los resultados y el desempeño en el marco de la Gestión de la Seguridad de la Información para el Departamento Administrativo Nacional de Estadística (DANE), premisa inicial de esta monografía.

Entrevista

Otro de los aspectos metodológicos para la recopilación de información para este documento será el contacto directo con actores de primera línea frente a la administración y ejecución de proyectos en la entidad.

Esta entrevista tiende a ser cualitativa a pesar de que no deja a un lado del todo los análisis cuantitativos, por lo cual también debe suponer un fuerte influenciamiento de parte del

entrevistador. La preparación adquirida para tal fin, es la de la misma experiencia en el aparte de la gestión de proyectos administrativos en la misma entidad por parte del Autor.

Así mismo se propone el "enfoque narrativo"[32] para la negociación temática como herramienta para el análisis de la entrevista.

Diseño Entrevista Responsable Apoyo Informático Sede Suroccidente Cali

1. Nombre.
2. Cargo.
3. Perfil.
4. ¿Desde hace cuánto es usted responsable del Apoyo Informático en la Sede Suroccidente Cali?
5. ¿Ha contribuido a la gestión de seguridad de la información en la entidad desde roles diferentes a este?
6. ¿Cuál es el grado de madurez que usted considera tiene la entidad en cuanto a implementación de políticas de gestión de seguridad de la información?
7. ¿Cuál es el grado de madurez que usted considera tiene la entidad en cuanto a implementación de técnicas de gestión de seguridad de la información?
8. ¿Existe alguna brecha entre los objetivos de seguridad de la información planteados en la entidad y los resultados obtenidos?

[32] Merlisnky, G. "La entrevista como forma de conocimiento y como texto negociado: notas para una pedagogía de la investigación". Revista Cinta de Moebio: Revista Electrónica de Epistemología de Ciencias Sociales. Tomado de: http://dialnet.unirioja.es/servlet/listaarticulos?tipo_busqueda=EJEMPLAR&revista_busqueda=2197&clave_busqueda=157274

9. Qué factores considera usted inciden en el logro de los objetivos de la gestión de seguridad de la información en la entidad?
10. ¿Cómo considera usted que las herramientas usadas para la gestión de seguridad de la información en la entidad ayudan a dicha labor?
11. ¿Qué propone usted para mitigar las fallas acaecidas en las posibles deficiencias en gestión de seguridad de la información si es que ocurren?

Diseño Entrevista Responsable Apoyo Administrativo Sede Suroccidente Cali – Subsede Popayán / Entrevista Responsable Operativo Sede Suroccidente - Subsede Popayán

1. Nombre.
2. Cargo.
3. Perfil.
4. ¿Desde hace cuánto es usted Apoyo Administrativo de la Subsede Popayán?
5. ¿Ha contribuido a la gestión de seguridad de la información en la entidad desde roles diferentes a este?
6. ¿Cuál es el grado de madurez que usted considera tiene la entidad en cuanto a implementación de políticas de gestión de seguridad de la información?
7. ¿Cuál es el grado de madurez que usted considera tiene la entidad en cuanto a implementación de técnicas de gestión de seguridad de la información?
8. ¿Existe alguna brecha entre los objetivos de seguridad de la información planteados en la entidad y los resultados obtenidos?
9. Qué factores considera usted inciden en el logro de los objetivos de la gestión de seguridad de la información en la entidad?

10. ¿Ha sufrido usted algún incidente en seguridad de la información?
11. ¿Cómo considera usted que las herramientas usadas para la gestión de seguridad de la información en la entidad ayudan a dicha labor?
12. ¿Qué propone usted para mitigar las fallas acaecidas en las posibles deficiencias en gestión de seguridad de la información si es que ocurren?
13. ¿Cuáles creen que son sus aportes a la seguridad de la información desde el rol que desempeña actualmente?

Resultados

Revisión Documental

La sistematización del Departamento Administrativo Nacional de Estadística ha avanzado desde hace ya tiempo en la intranet corporativa, medio sobre el cual se puede acceder, previa autenticación de usuario, a los distintos documentos que enriquecen hasta el momento el esquema de seguridad de la información disponible.

Con motivo de la emergencia nacional resultado de los preocupantes datos de contagio del COVID SARS 19, se evidenció una mejora en cierta sección de TI de la entidad, haciendo una migración hacia Sharepoint como medio de publicar los contenidos de intranet:

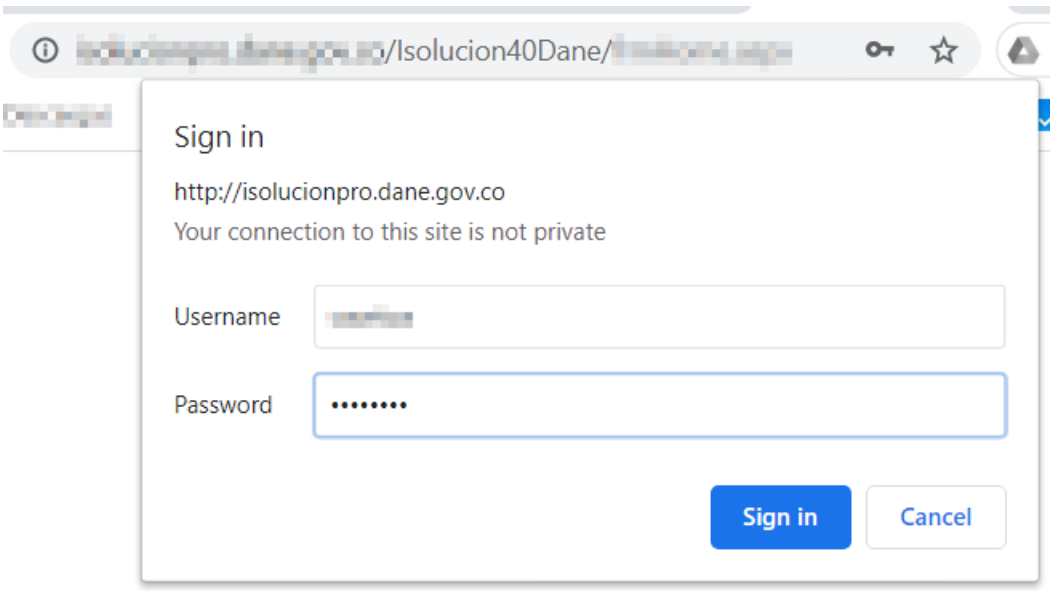
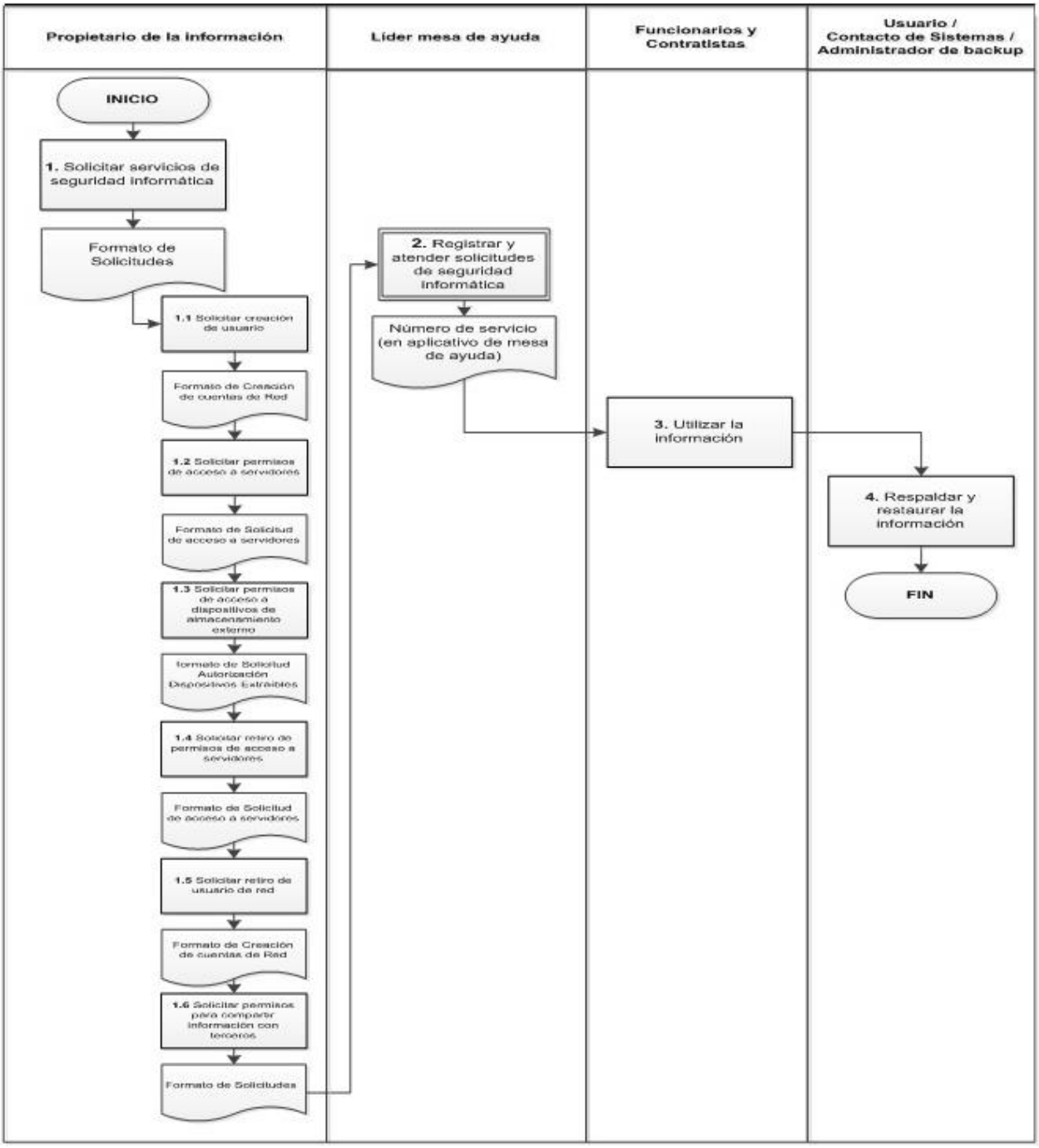


Ilustración 4, Acceso con credenciales a documentación interna DANE.

Al revisar el "Procedimiento de Seguridad Informática" se encuentra una serie de actividades con sus respectivos responsables para cada una de ellas enmarcadas dentro del

siguiente esquema:

Ilustración 5, Diagrama de Flujo Procedimiento de Seguridad de Informática.



Tomado de: Departamento Administrativo Nacional de Estadística. "Resolución 0447, Gobierno Digital". 2019.

Esto se ve soportado a través de Planes actualizables en Seguridad y Privacidad de la información, siendo la última emisión en el mes de Enero de 2019 y sobre el cual se rigen las actividades concernientes a este respecto.

Un aparte importante de este plan, en lo que respecta a las herramientas que se usan para penetrar brechas en seguridad informática con ingeniería social, es la asignación de Roles y Responsabilidades, la cual está asociada con la definición de los actores responsables en su actuar y función de la seguridad de la información, cuya asignación no sólo generará las dinámicas propias de un proceso, sino que ampliará la cobertura de la seguridad sobre todos los activos de información en la entidad.

Es destacable es esfuerzo que se hace sobre el factor humano, consagrado en la definición e implementación del Plan de Sensibilización, Comunicación y Capacitación en seguridad de la información y que contempla un programa efectivo de sensibilización, capacitación y comunicación en seguridad de la información debe explicar de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que generalmente están plasmadas en las políticas y procedimientos de seguridad de la información que la Entidad requiere sean cumplidos por parte de todos los usuarios del sistema.

Cualquier incumplimiento a las políticas, debe llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidad.

Esta acción se focaliza sobre el componente humano de la entidad, con el fin de alcanzar no sólo la comunicación del mensaje sino la apropiación y concientización sobre la importancia de asumir la seguridad de la información en la vida personal, profesional y laboral como una

práctica social[33].

Lo anterior evidencia un tratamiento aceptable a través de planteamientos de prevención basados en el control humano, que es en síntesis el origen de la brecha de seguridad en cuanto a ingeniería social.

Entrevistas

Tras haber realizado las tres entrevistas planteadas al contacto de sistemas de la Dirección Territorial Cali, y a los coordinadores Operativo y Administrativo de la Subsede Popayán (Anexos) se logró evidenciar ventajas y situaciones difíciles en cuanto a la administración y gestión de la seguridad de la información.

Coinciden en los relatos las dificultades presentadas a la hora de divulgar la información de los esfuerzos que realiza la Oficina de Sistemas, ya que a pesar de que este tema se incluye en la formación a aspirantes a contratistas, el tiempo no es suficiente. Se divulgan las bases de este tema, pero por cuestiones de tiempo no se entregan a detalle y no se logra hacer un énfasis productivo hacia la manera como deben participar todos los actores en cuanto a la protección de los datos que administra la entidad.

Esto conlleva a otro tema renuente que es la continua renovación de personal contratista, que es en gran parte la fuerza operativa de la entidad. Para cada operación se entiende que se crea anualmente por lo general una convocatoria en la que a veces participan las mismas personas y en menor ocasión ganan el contrato las mismas personas. Esta situación es un manifiesto en

[33] Plan de Seguridad de la Información. Departamento Administrativo Nacional de Estadística, 2019.

común de las entrevistas y de lo cual dan cuenta como uno de los factores negativos para contrarrestar el inconveniente anterior relacionado con la capacitación.

Adicionalmente, en cuanto a la vinculación permanente de los funcionarios, existen algunos que no tienen un entrenamiento consistente en tecnologías de la información, visualizando constantes malas prácticas que acarrean esfuerzos y gastos económicos para contrarrestar las posibles vulnerabilidades y riesgos que esto promueve.

Se denota que la gestión de la información no está completa y es claro que se están teniendo avances recientes que en cierta medida han tenido que ser fortalecidos a través de la emergencia del COVID 19, pero que a su vez no ha tenido divulgaciones oficiales de resultados debido a la carga adicional del trabajo que se ha generado en la pandemia.

Revisión Tecnológica

Este resultado visualizado es producto de la revisión personal realizada a través de los diferentes segmentos de infraestructura física y digital que ha dispuesto la oficina de sistemas para la administración y gestión de seguridad de la información.

Hardware

A nivel de hardware se cuenta con una renovación de equipos de los usuarios que cuentan con una protección de apertura y extracción de elementos internos, por ejemplo el disco duro, lo cual impide que por alguna razón puedan lograr extraer directamente datos al respecto.

Existe también una inversión en servidores modernos de marca reconocida que ofrecen un

mejor procesamiento y a la vez control para los servicios instalados, a saber, servidor de aplicaciones, servidores de bases de datos, servidores de dominio. Existía un equipo dedicado con Sonic Wall el cual fue dado de baja por no contar con las especificaciones técnicas requeridas para una adecuada actualización.

Existe un firewall físico Barracuda NextGen que potencializa enfáticamente con hardware dedicado a la administración de seguridad y que cuenta con una administración basada en Web, número ilimitado de direcciones IP y usuarios protegidos por firewall, sin límite de clientes VPN de conectividad remota, gestión centralizada basada en la nube y opciones de filtro web flexibles.

Software

Además de los componentes de software del firewall físico Barracuda, en consideración a la emergencia nacional decretada por el COVID19, se actualizó la Licencia para el uso de VPN con Fortinet, Forticlient, el cual contiene tres módulos clave: Fabric Agent para la conectividad de Security Fabric, los módulos de seguridad de endpoint y los módulos de acceso remoto seguro. Fabric Agent comparte la telemetría de endpoint con el Security Fabric y ofrece una amplia visibilidad de endpoint, control de cumplimiento y administración de vulnerabilidades. Proporciona protección avanzada de endpoints con antimalware basado en patrones, protección contra vulnerabilidades de seguridad basada en el comportamiento, Web Filtering y un firewall de aplicaciones. FortiClient se integra de forma nativa con FortiSandbox para detectar amenazas de día cero y malware personalizado. FortiClient también proporciona acceso remoto seguro con la VPN incorporada, inicio de sesión único y autenticación de dos factores para mayor

seguridad.[34]

También se evidencia una mejora en la seguridad con la adquisición del servicio de buzón de correo electrónico a través de office 365, cuya administración de seguridad es superior a la versión local de zimbra que estaba en uso. Adicionalmente esta plataforma fue contratada con Sharepoint el cual se usó para mejorar la seguridad de acceso a la intranet corporativa.

La administración de credenciales iniciales de acceso para los usuarios sigue realizándose amarrada al directorio activo en un Windows Server 2012, que también administra las carpetas compartidas y espacios para el backup manual de los funcionarios.

Relación de Incidentes Encontrados

En este menester se realizó consulta principalmente a la oficina central de sistemas, la cual, si bien no tiene un formato exclusivo para la gestión de incidentes en gestión de seguridad de la información, si tiene un repositorio de solicitudes, alertas y requerimientos referentes a este tipo, de los cuales se tienen registro desde la vigencia 2016, año en el cual se empezó a determinar la necesidad de crear estrategias para combatir las amenazas y riesgos en este respecto.

Niveles de Criticidad

Para efectos de análisis de criticidad de los incidentes encontrados, se tomó como base la metodología magerit, simplificando de la siguiente manera:

[34] Forticlient, Protección de endpoint de última generación. Tomado de: https://www.fortinet.com/lat/products/endpoint-security/forticlient

Criticidad Alta: Cuando el incidente genera una vulnerabilidad alta al acceso de los datos.

Criticidad Media: Cuando el incidente representa una vulnerabilidad que a pesar de su riesgo, es poco probable su materialización.

Criticidad Baja: cuando el incidente es notorio pero su materialización tendría un impacto poco significativo a la entidad.

Tabla No. 1. Relación incidentes seguridad informática

Tipo Incidente	Tema	Cantidad	Criticidad
Acceso	Bloqueo credenciales de red	937	Media
Acceso	Bloqueo de credenciales de correo electrónico	628	Media
Fraude	Correos con contenido malicioso	93	Alta
Código Malicioso	Infección a dispositivos	67	Baja
Daños Físicos	Hurto / pérdida en operativo en campo	56	Alta
Daños Físicos	Hurto en Sede	3	Alta
Abuso de Privilegios	Cuentas no inactivas	2	Media
Código Malicioso	Secuestro información	1	Alta

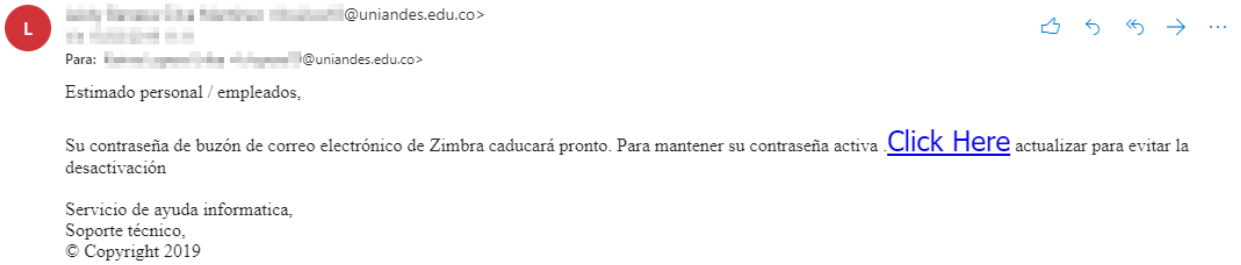
Fuente: DANE 2017-2019

De la revisión anterior se destacan los siguientes tipos de casos asociados con la ingeniería social:

- Correos con contenido Malicioso: al igual que en muchas entidades públicas o privadas, se reciben mensajes de correo con distintas bifurcaciones de la ingeniería social, denotando cierta sofisticación en la metodología, algunos ejemplos son:

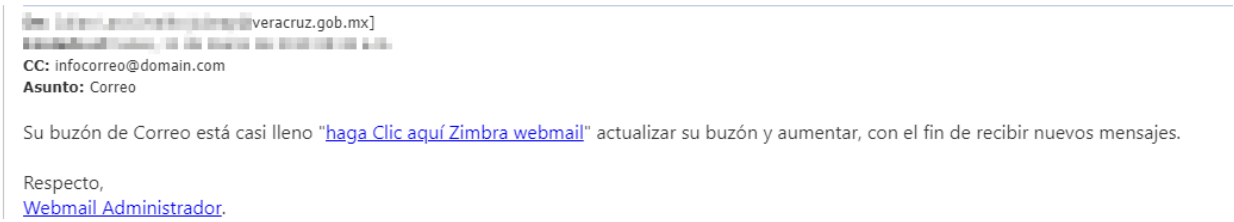
Ilustración 6, Intento de ataque desde dominio iess.gov.ec

Tomado de: Fuente propia.



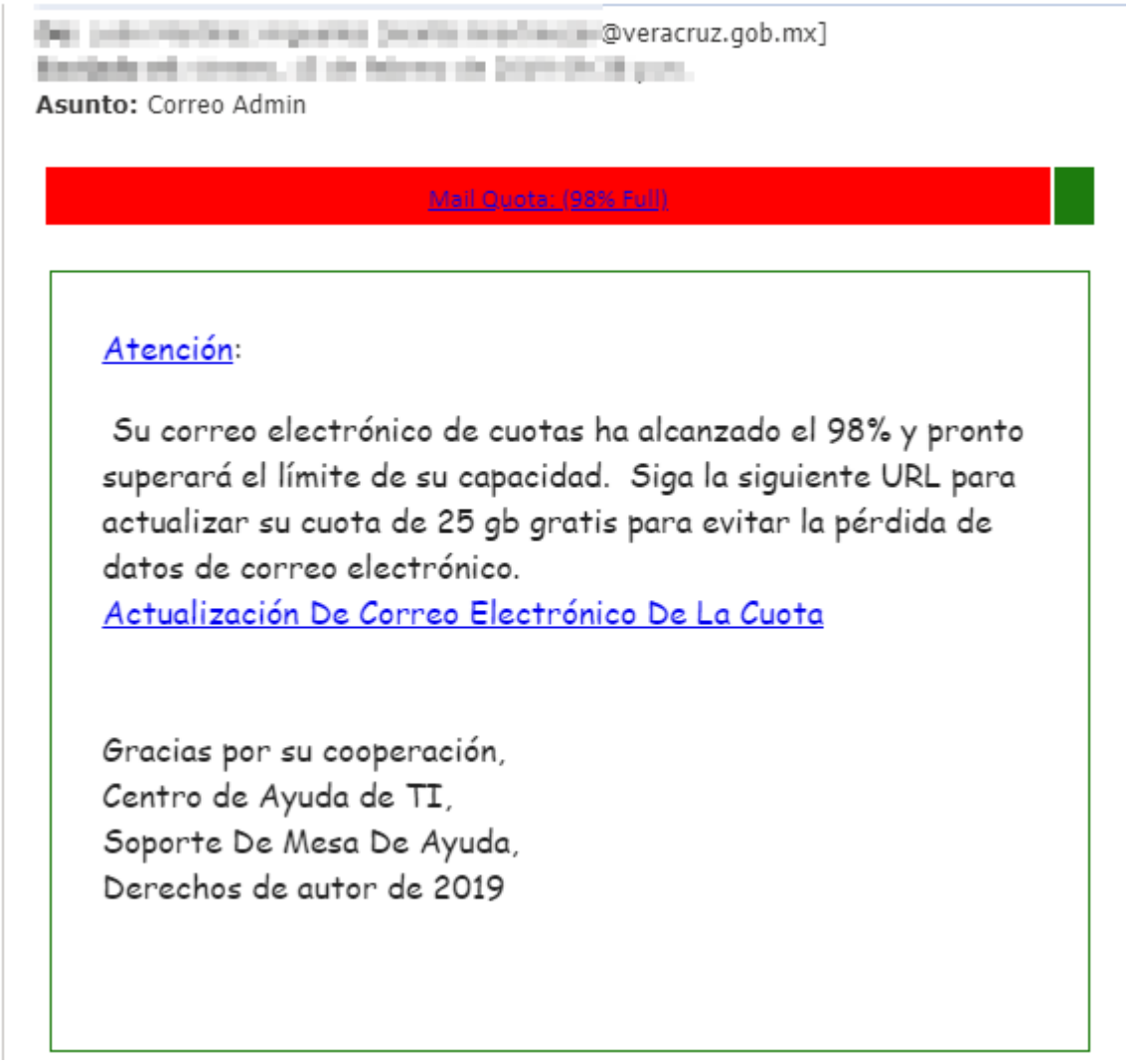
Tomado de: Fuente propia.

Ilustración 7, Intento de ataque desde dominio veracruz.gob.mx



Tomado de: Fuente propia.

Ilustración 8, Intento de ataque desde dominio veracruz.gob.mx



Tomado de: Fuente propia.

Ilustración 9, Intento de ataque desde dominio brain.net.pk

[redacted]@brain.net.pk]
[redacted]
Para: undisclosed-recipients:
Asunto: (no subject)

--
Su contraseña caducará en 2 días para mantener su cuenta, HAGA CLIC AQUÍ y siga las instrucciones para mantener una cuenta de correo electrónico O HAGA CLIC EN ESTE ENLACE:

correo web-buzón-actualización http://webcoredo.aircus.com/

Si no actualiza su cuenta de correo electrónico, se desactivará, ¡le avisaremos!

PA 19104
IT Help Desk © 2018 Todos los derechos reservados.

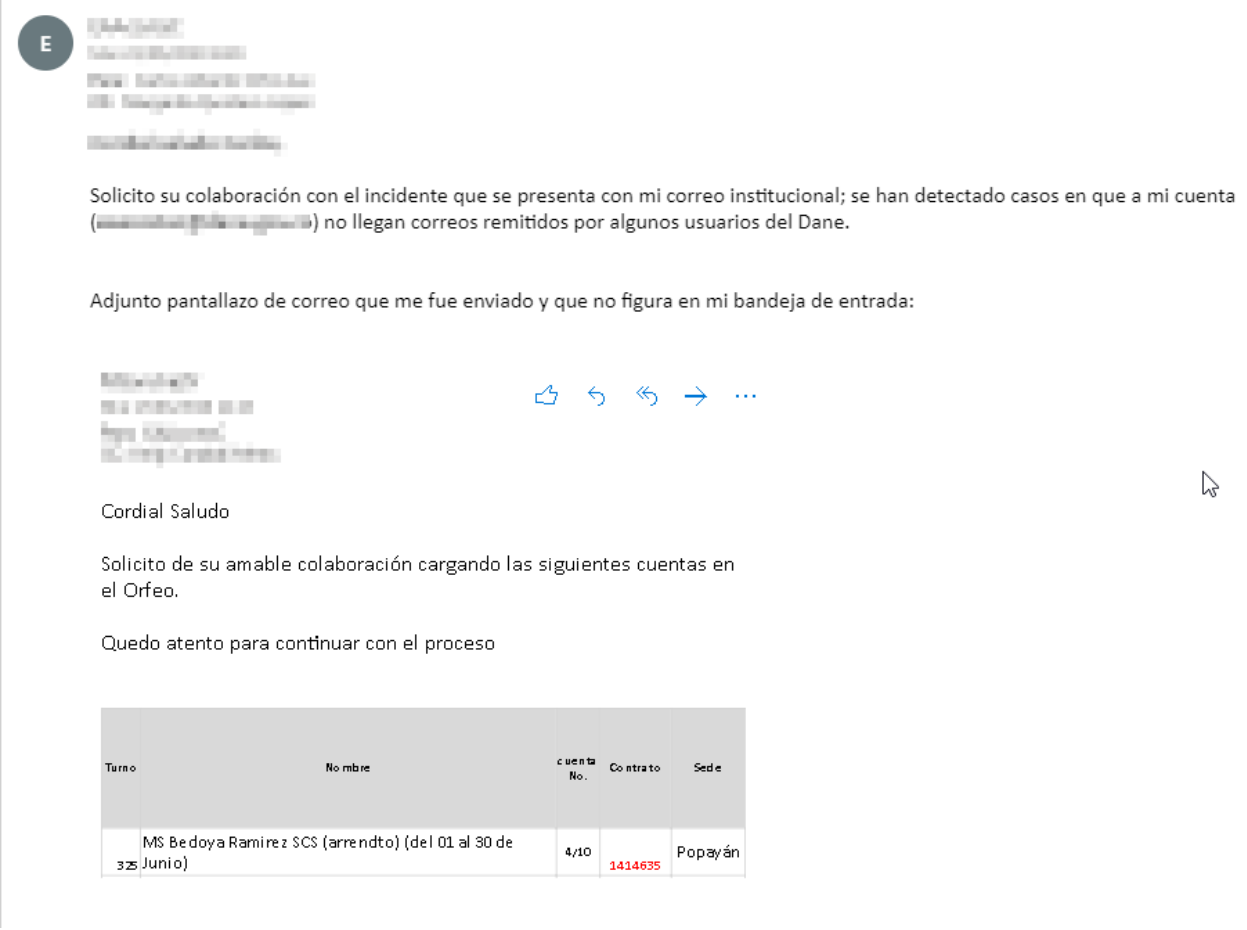
Tomado de: Fuente propia.

Ilustración 10, Intento de ataque desde dominio co.bancofalabella.com

Tomado de: Fuente propia.

- Código Malicioso: Algunas infecciones a través de canales no definidos han causado problemas en las comunicaciones internas de la entidad:

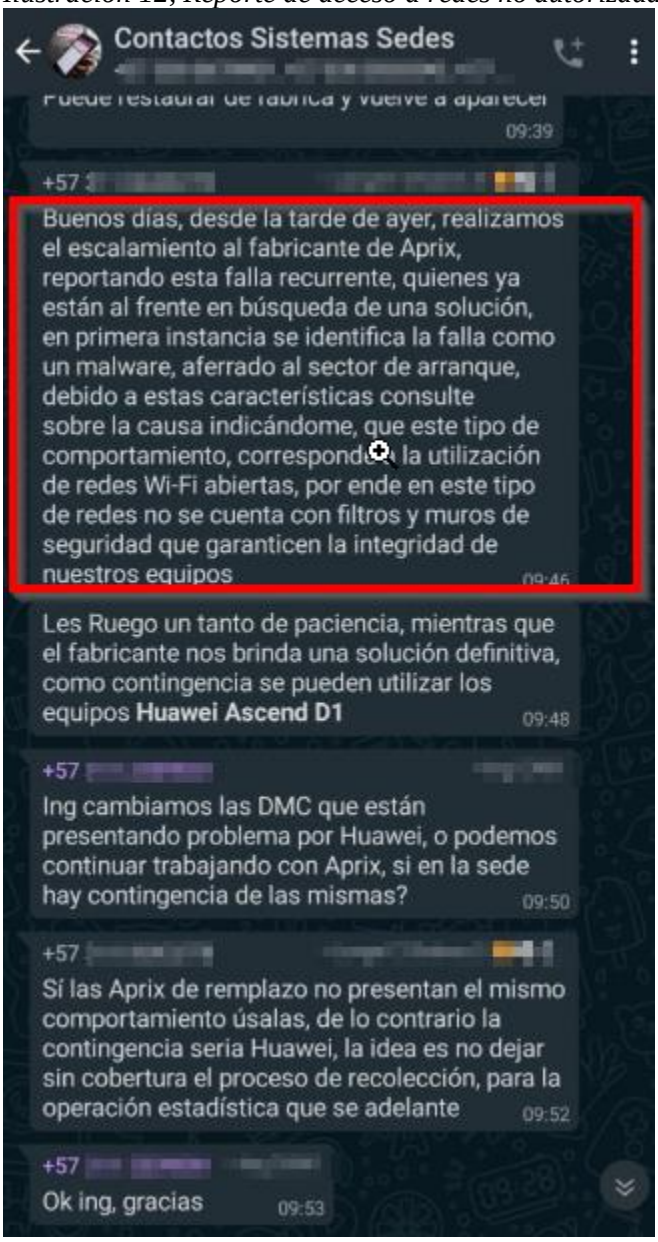
Ilustración 11, Bloqueo de cuenta de correo por infección.



Tomado de: Fuente propia.

- Cuentas no inactivas: dado el requerimiento de uso de Dispositivos Móviles de Captura, principalmente smartphones en los operativos de campo, el control de las cuentas a aplicaciones en éstos es bajo, por lo que aquellos usuarios que ya no deberían tener acceso a las aplicaciones y servicios instalados en estos dispositivos se convierten en una debilidad en seguridad durante el tiempo que aún cuenten con los mismos sin hacer la debida devolución a almacén de la entidad.

Ilustración 12, Reporte de acceso a redes no autorizadas con equipos no reintegrados oportunamente.



Tomado de: Fuente propia.

Vale la pena también recalcar casos en los cuales se ha proliferado supuestos riesgos en la seguridad de la información, lo que se ve reflejado en el común manifiesto de la población objeto de investigaciones en campo en cuanto a la utilización de datos recopilados por fuera del menester estadístico que cita la misión de la entidad.

En un sentido similar, incidentes como el ocurrido en enero del año 2018 fueron registrados, momento en el cual en el marco del operativo del Censo Nacional de Población y Vivienda se inició la modalidad virtual para el diligenciamiento, con el fin de obtener agilidad y minimizar costos para la recolección, lo cual fue alertado como una vulnerabilidad por una ingeniera de nacionalidad colombiana trabajando Microsoft, según la cual la página del DANE no brindaría seguridad informática a los colombianos.

Ilustración 13, Reporte de vulnerabilidad contraseña para el operativo de Censo Nacional de Población y Vivienda 2018.

Tomado de: Fuente propia.

Análisis de Resultados

En el transcurso evolutivo de la entidad se observa una reciente actualización en herramientas tecnológicas que coadyuvan a sobrellevar los riesgos y amenazas circundantes en cuanto a seguridad de la información. Los recientes acontecimientos referentes al SARS-COVID 19 han impulsado millonarias inversiones en la inclusión tecnológica en las labores diarias de muchos trabajadores alrededor del mundo y en el Departamento Administrativo Nacional de estadística no se encuentra excepción.

A pesar de que el Plan de Seguridad Informática no se encuentra debidamente actualizado, sí se evidenciaron incrementos en los esfuerzos e inversión monetaria para reforzar todas las actividades de la gestión en seguridad de la información. Se destaca en esta lucha los procesos de sensibilización que orientan a la comunidad laboral local a prevenir muchos inconvenientes relacionados con el tema de estudio, no obstante lo anterior aún queda camino por recorrer en este fortalecimiento.

En general, la parte documental del tratamiento y prevención de ataques de ingeniería social está en un nivel bajo según lo recopilado por las entrevistas a los distintos roles contactados, a pesar de que se hayan realizado actividades y perfeccionando procesos, la falta de una completa documentación al respecto permite que exista una brecha que impacte en el logro de los objetivos y horizontes demarcados en la misión de la entidad, desde los operativos en campo hasta la meta de reporte estadística que se presenta continuamente en todos los operativos de investigación vigentes en la entidad.

Continuidad Laboral y Experticia

En ese mismo sentido, la experiencia de los funcionarios se lleva a la marcha frente a las acciones cotidianas en la lucha contra este tipo de ataques, sin embargo, hay un elemento clave que genera una debilidad notoria concerniente a la falta de continuidad laboral en la entidad, dado que la mayoría de la fuerza de trabajo se encuentra en personal contratista que debe participar en convocatorias que en ocasiones son dos o tres por año, lo cual hace muy variable el pool de trabajadores y bajo este parámetro, la capacitación en prevención contra ataques de ingeniería social es una tarea que cada tanto encuentra un retroceso.

Esto sin duda alguna debe ser fortalecido como en cualquier otra entidad, sin embargo, el camino más próximo es incrementar los esfuerzos en las propias capacitaciones de cada convocatoria para elevar el índice de conocimientos en este aspecto.

En una mejor alternativa, se encuentra fortalecer con técnicas pedagógicas específicas a aquellos funcionarios de avanzada edad que suelen ser más vulnerables en estos ataques, obviando así la renuencia de falta de impulso para tener un entrenamiento continuo y perseverante hasta que cada espacio vulnerable sea sellado a través de la aplicación de buenas prácticas.

Impacto de Incidentes

De los incidentes registrados, aquellos que pueden llegar a tener una relación con la ingeniería social suman el 9% de los incidentes reportados. Entendiblemente existirán muchos más no registrados, además de otros tantos que se ocultaron voluntariamente por cierto infundado temor a represalias por parte de la organización.

Se denota un modus operandi principal en los ataques de ingeniería social, siendo que en el tiempo reportado se usó principalmente la plataforma de correo electrónico Zimbra, elegantemente los ataques venían dirigidos con esa temática. Esto es común verse hasta el punto de hacer una combinación de dominio origen (previamente afectado) + temática específica relacionada + víctima vulnerable.

En otro aparte de logs de reporte se destacan muchas ocasiones de inclusión de direcciones de correo en listas de spam, causadas por esta misma modalidad. Los engaños son cada vez más sofisticados y en caso de verse comprometida una cuenta de correo electrónico, se convierte automáticamente en un ente replicador de la misma amenaza hacia otros clientes internos y externos. Se logró determinar que todos las solicitudes de soporte relacionadas con correos sin llegar a su destino fue por categorización como remitentes riesgosos tras haberse comprometido la dirección de correo del usuario. Esto a su vez causa traumatismos, como por ejemplo retrasos en la consecución de la información porque no se alcanzan las fuentes de manera oportuna.

Con ocasión del COVID-19, los ciber criminales aumentan en número y técnica en todo tipo de ataque, nunca dejando por fuera aquellos de ingeniería social, por esta razón algunas mejoras convenientes para las organizaciones son:

RETOS TÉCNICOS PARA LOS PROGRAMAS EN SEGURIDAD DE LA INFORMACIÓN[35]		
Controles de Proceso de las Entidades	**Controles Persuasivos**	**Controles de Cumplimiento**
Entender los procesos de	Mantenimiento de niveles de	Adhesión de estándares del

[35] Lanz, Joel, Sussman I., Bruce. Information Security Program Management in a COVID-19 World. The CPA Journal, June 2020.

RETOS TÉCNICOS PARA LOS PROGRAMAS EN SEGURIDAD DE LA INFORMACIÓN[35]		
Controles de Proceso de las Entidades	**Controles Persuasivos**	**Controles de Cumplimiento**
negocios a través de los datos y los flujos de trabajo en conjunto con las vulnerabilidades y su impacto en el perfil de riesgo de la empresa. Identificar los retos particulares en seguridad de la información y en ingeniería social dentro del los ciclos del negocio. Optar por cambios estructurales en los controles y pruebas de seguridad de la información dada la contingencia.	resiliencia basados en los objetivos de gestión de seguridad informática. Incrementar protección física, lógica y logística contra ataques de ingeniería social. Minimizar el riesgo al momento de trasladar productos, procedimientos y datos a ambientes virtuales. Implementación de procesos de automatización y tecnologías de inteligencia artificial.	entorno de la entidad. Asegurarse del cumplimiento de estándares por parte de los clientes internos y externos. Cumplimiento de las normativas en ciberseguridad.

Credibilidad del Objeto Poblacional

¿Qué hace una entidad encargada de recopilar y procesar datos cuando la población fuente

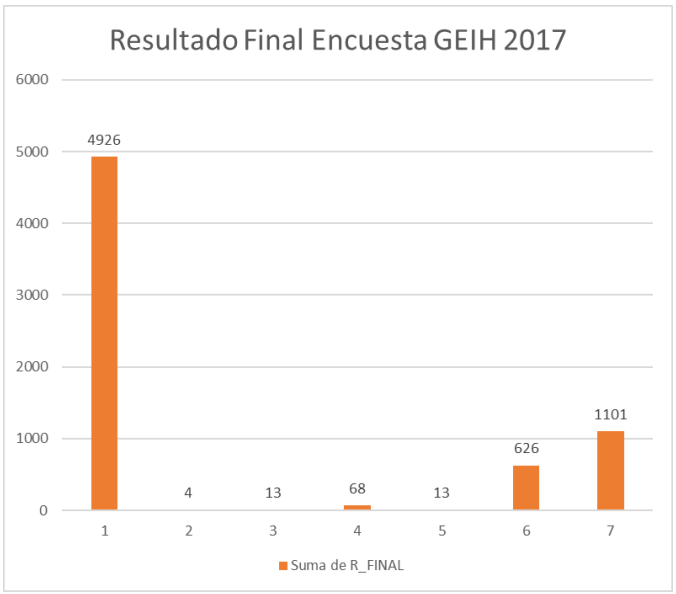
de la información pierde credibilidad en ella? Esto es quizás uno de los impactos más importantes dada la misión de la entidad. Con el escándalo ocasionado por las declaraciones de la ingeniera de Microsoft, el éxito del Censo Nacional de Población y Vivienda del año 2018 se vio severamente comprometido en un alcance a nivel Nacional, debido a que la noticia se divulgó por múltiples medios a lo largo de una prometedora campaña que optaba por los canales virtuales en pro de la eficiencia en el manejo del recurso tiempo y dinero.

Si bien directamente este no es un ataque de ingeniería social, sí se expusieron posibilidades de que fácilmente una persona a la cual se fuera secuestrado su correo a través de esta modalidad perdiera también la oportunidad de diligenciar correctamente la información del censo, y más gravemente que ésta fuera consultada por personas malintencionadas.

La percepción que tenga la población fuente de información del Departamento Administrativo Nacional de Estadística tiene una altísima incidencia en el éxito de los operativos. Para la vigencia 2018 en adelante se notó un incremento en los rechazos para la investigación insignia del Departamento Administrativo Nacional de Estadística, la Gran Encuesta Integrada de Hogares mediante la cual se solicita información sobre las condiciones de empleo de las personas (si trabajan, en qué trabajan, cuánto ganan, si tienen seguridad social en salud o si están buscando empleo), además de las características generales de la población como sexo, edad, estado civil y nivel educativo, se pregunta sobre sus fuentes de ingresos. La GEIH proporciona al país información a nivel nacional, cabecera - resto, regional, departamental, y para cada una de las capitales de los departamentos.[36]

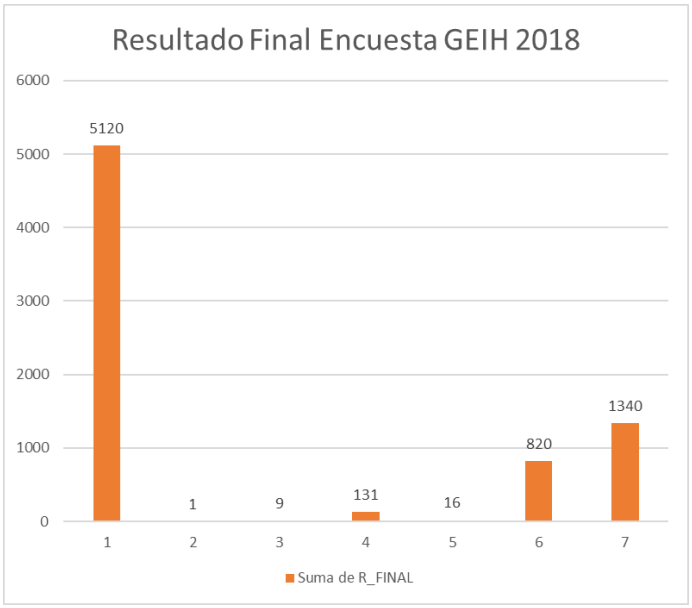
[36] "Gran encuesta integrada de hogares (GEIH) Mercado laboral – Históricos", DANE. Tomado de: https://www.dane.gov.co/index.php/estadisticas-por-tema/mercado-laboral/empleo-y-desempleo/geih-historicos

Ilustración 14, Resultado Final Encuesta GEIH Vigencia 2017

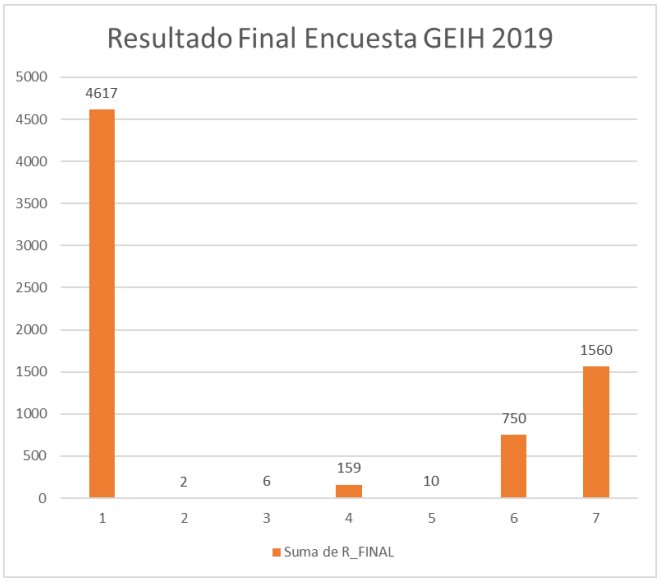


Fuente: DANE 2017

Ilustración 15, , Resultado Final Encuesta GEIH Vigencia 2018



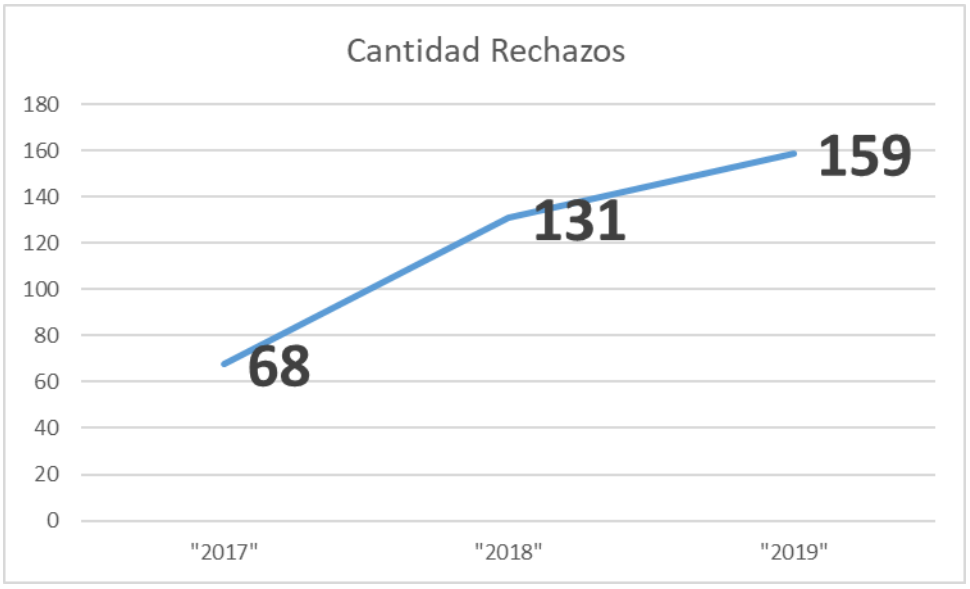
Fuente: DANE 2018



Fuente: DANE 2019

Se encuentra un notorio incremento en el ítem No. 4 correspondiente a los rechazos:

Ilustración 16, Incremento Cantidad de Rechazos Encuesta GEIH 2017 a 2019



Fuente: DANE 2019

Este resultado demarca notoriamente un impacto significativo indirecto de los ataques en

ingeniería social y sus riesgos asociados frente a la percepción de la fuente principal e insumo de trabajo para la entidad.

Conclusiones y Recomendaciones

- La entidad no cuenta con una documentación completa para la gestión de la seguridad de la información, lo cual sin duda alguna generaría una base sólida para prevenir ataques como los de ingeniería social, por lo cual se hace pertinente que se cree un esquema de logs donde se registren, clasifiquen y se le haga seguimiento a cualquier incidente de este tipo y de cualquiera relacionado con la seguridad de la información de la entidad. Se recomienda emplear una tecnología estándar para este fin, localizando los documentos tal como se describe en métodos como los descritos por COBIT, ITIL, etc.

- La capacitación es un elemento fundamental a la hora de combatir ataques de ingeniería social, por tanto, al ser tan dificultoso el menester de garantizar continuidad al personal de la entidad, se deben buscar estrategias pedagógicas a través de las cuales el mensaje llegue y sea permanente. Se recomienda la incorporación de cursos permanentemente disponibles en la intranet corporativa donde los distintos aportantes puedan alimentarse continuamente de la información relacionada como este tema, además de noticias constantes acerca de los riesgos y formas de mitigarlos frente a la protección de los datos administrados por la entidad. La creación de programas tipo Gestores TICs, en donde se responsabilicen funcionarios de cada área son excelentes estrategias para abordar el tema, creando una base de sensibilización y concientización permanente que esté presente en cada momento y actuar de los grupos de trabajo.

- El principal impacto de la ingeniería social y sus afecciones indirectas sobre los resultados y el desempeño en el marco de la gestión de la seguridad de la información para el Departamento Administrativo Nacional De Estadística (DANE) se refiere a la percepción y pérdida de credibilidad de la población fuente de información hacia la entidad. Esto dificulta de manera contundente y en un potencial alto ya que las cifras demuestran un deterioro en los aportes de la población nacional al incrementarse la tasa de rechazos para la principal investigación de la entidad. En ese orden de ideas, es pertinente divulgar de manera promocional a través de la propaganda institucional todos los pormenores y esfuerzos realizados frente a la preservación de la seguridad en la información que se recopilan en todas las investigaciones, de esta manera dando confianza en la fuente de información para que no solo se brinde la información de manera oportuna, sino que sea veraz.

- Otro impacto de la ingeniería social recae sobre las herramientas tecnológicas como el correo electrónico, el cual cuando se ve comprometido a causa de un ataque de este tipo, genera dificultades, retrasos y bloqueos en las comunicaciones que, en menor medida, pero no por eso sin importancia, logra afectar el desempeño de la entidad en su misión estadística. Una buena estrategia es incluir los plugins de correo electrónico que se integran fácilmente a los software de escritorio que se usan comúnmente para tal fin.

- La divulgación de las técnicas y buenas prácticas en seguridad de la información en la entidad tiene un amplio camino por recorrer, desde el personal contratista como el de planta. Para eso se pueden crear grupos como Gestores de Tecnologías de Información y

Seguridad Informática que promuevan y desplieguen una red de conocimiento y aplicación del mismo a lo largo de todos los grupos de trabajo de la entidad.

- A nivel personal, el análisis y recopilación de datos para la elaboración de esta monografía, permitieron extender en el autor los comportamientos claves dentro de la organización que pueden permitir vulnerabilidades frente a un entorno agresivamente cambiante, sobre todo en las entidades del orden público dadas las condiciones estructurales de las mismas.

- De igual manera, el resultado de todo el proceso documental, fue fuente de conocimiento acerca de la gran importancia que tiene el recurso humano frente a la lucha contra las amenazas informáticas, ya que sin importar la cantidad de tecnología física y lógica usada, el componente humano debe ser fortalecido de manera constante en lo que respecta a este conocimiento con el fin de sellar cualquier brecha existente entre estos tres componentes

Referencias

ABRAHAM, Akampurira, Project Planning and Management, An aspect of Development. Anchor Academic Publishing. Hamburgo, 2014.

AGUTTER, C. (2013). ITIL Lifecycle Essentials : Your essential guide for the ITIL Foundation exam and beyond. ITGP.

AREITIO, Javier. Seguridad de la información. Redes, informática y sistemas, Madrid : Paraninfo, 2008.

Bonham, S. S. (2005). "IT Project Portfolio Management". Artech House, Inc. 2005.

CARVALHO, Carla. "Adapting ISO 27001 to a Public Institution". 2019

COBIT. Cobit, Sumario Ejecutivo. Buenos Aires : Systems Auditand Control, 1998.

"Convention on Cybercrime", Budapest, 23 de Noviembre de 2001

Cortés Hernández, Andrés Mauricio. "INGENIERÍA SOCIAL: PHISHING Y BAITING".

Departamento Administrativo Nacional de Estadística. "Resolución 0447, Gobierno Digital". 2019.

"Fundamentos para la Dirección de Proyectos, (Guía del PMBOK) – Cuarta Edición. Project Management Institute, 2008.

HURTADO PÉREZ, Andrés, ROBAYO GONZÁLEZ, Omar. "DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI- PARA LOS PROCESOS CRÍTICOS DE LA COOPERATIVA FEBOR BASADO EN LA NORMA ISO 27001:2013" 2019

Instituto de Financiamiento, Promoción y Desarrollo de Tuluá. "Políticas de Seguridad Informática". 2017

IPQ - Instituto Português da Qualidade, I.P., «NP ISO/IEC 27001:2013 - Tecnologia de informação -- Técnicas de segurança -- Sistemas de gestão de segurança da informação - Requisitos». IPQ - Instituto Português da Qualidade, I.P., 2013.

"ISO 9001 y el ciclo PHVA". Tomado de: https://www.nueva-iso-9001-2015.com/2019/05/ciclo-phva-en-iso-9001/

IT Governance Institute. redyseguridad. 4 de Diceimbre de 2013. Tomado de: http://redyseguridad.fip.unam.mx/proyectos/cobit/seccion_informativa/pdfscobit/resumen_ejecutivo.pdf

LADINO A., Martha Isabel, VILLA S., Paula Andrea, LÓPEZ E., Ana María. "FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS".

Universidad Tecnológia de Pereira. 2011.

Lanz, Joel, Sussman I., Bruce. Information Security Program Management in a COVID-19 World. The CPA Journal, June 2020.

Ley Estatutaria 1581 de 2012, Congreso de la República. 2012.

M. MERCÈ. (2002, Dic 26). “Ingeniería Social: Mentiras en la Red”. Tomado de: http://ww2.grn.es/merce/2002/is.html

MAYA A., Paula Andrea. “Plan de implementación del Sgsi basado en la norma iso 27001:2013”. Universitat Oberta de Catalunya, 2016.

MEDINA ROJAS, Jhonatan Deyvi; RIVAS MONTALVO, Yonathan Yajanovic. “Evaluación del Rendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos” 2020.

MENDEZ BARCO, Andrés. GUÍA DE SEGURIDAD DE LAS TIC. Madrid: Ministerio de Defensa, 2008.

Merlisnky, G. “La entrevista como forma de conocimiento y como texto negociado: notas para una pedagogía de la investigación”. Revista Cinta de Moebio: Revista Electrónica de Epistemología de Ciencias Sociales. Tomado de: http://dialnet.unirioja.es/servlet/listaarticulos?tipo_busqueda=EJEMPLAR&revista_b

usqueda=2197&clave_busqueda=157274

Ministerio de Tecnologías de la Información y las Comunicaciones. “Seguridad y Privacidad de la Información”, 2016.

PARRA ALVARADO, José Francisco. “Marco de Buenas Prácticas para la Planeación de la Adquisición de Servicios de TI en las Entidades Públicas Colombianas”. Universidad Nacional De Colombia, 2019.

ROMERO, Diego. “EL ARTE DE LA INGENIERÍA SOCIAL”. Universidad Piloto de Colombia, 2016.

WIENCLAW, Ruth A., Research Starters: Business (Online Edition), 2015.

Anexos

Ficha Técnica Entrevistas

Dirección	Las entrevistas fueron dirigidas desde el diseño hasta el análisis por la Comunicadora Social Lina Isabel Martínez López, funcionaria del área de Pedagogía en el Centro de Ciencia y Tecnología de Antioquia.
Técnica	El diseño seleccionado fue semiestructurado, tendiente a perfilar las respuestas de los entrevistados hacia una extensión dinámica de los temas de interés de cada pregunta en particular. La caracterización de los entrevistados se plasmó en las 4 preguntas iniciales, mientras que las restantes 9 preguntas se relacionaron con la percepción y relación de los entrevistados con estado e incidentes de seguridad informática en la entidad.
Fecha de Realización	Junio a Julio de 2020
Entrevistados	• Francisco Zambrano, Responsable Apoyo Informático Sede Suroccidente Cali • Eduin Acosta, Apoyo Administrativo Sede Suroccidente Cali – Subsede Popayán • Jorge Flórez, Responsable Operativo Sede Suroccidente - Subsede Popayán

Resultado Entrevistas

Entrevista Responsable Apoyo Informático Sede Suroccidente Cali

1. Nombre

   Francisco Zambrano

2. Cargo

   Analista de Sistemas

3. Perfil

   Tecnólogo en Sistemas de Información

4. ¿Desde hace cuánto es usted responsable del Apoyo Informático en la Sede Suroccidente Cali?

   Llevo 4 años y medio como contacto de sistemas en la sede pero he trabajado como técnico en sistemas por más de 7 años.

5. ¿Ha contribuido a la gestión de seguridad de la información en la entidad desde roles diferentes a este?

   Solo he pertenecido al área de sistemas, y desde el ingreso al área recibí la recomendación para incentivar las buenas prácticas en seguridad de la información.

6. ¿Cuál es el grado de madurez que usted considera tiene la entidad en cuanto a implementación de políticas de gestión de seguridad de la información?

   La documentación que debe desplegar estas políticas aún está en construcción, aunque los aportes hasta el momento son bastante pertinentes. Hemos tenido ya varias reuniones los responsables de sistemas para tratar de este tema, otras más con los funcionarios para

tratar de socializar las políticas. Creo que estamos en un nivel medio, ya se ha divulgado la intención, las responsabilidades y deberes con respecto a este tema.

7. ¿Cuál es el grado de madurez que usted considera tiene la entidad en cuanto a implementación de técnicas de gestión de seguridad de la información?

   En los últimos años se ha mejorado mucho en este aspecto, esto se ve influenciado mucho por las políticas de dirección, algunos directores de la entidad pueden considerar esto más importante que otros. En esta última administración se han visto mejoras considerables en todo lo tecnológico que a su vez se replica en la lucha para la seguridad de la información, pero aún es un esquema en construcción, considero que está en un nivel bajo ya que a pesar de que se inició, aún se está en espera de los resultados de toda la inversión económica y de tiempo de los respectivos responsables.

8. ¿Existe alguna brecha entre los objetivos de seguridad de la información planteados en la entidad y los resultados obtenidos?

   Si, hasta ahora se han planteado muchos aspectos que deben tener en cuenta todos los miembros de la entidad, sin embargo los resultados de análisis de la oficina central de sistemas, sobre los que esperamos un avance, aún no han sido divulgados. Por lo pronto, si bien no hemos tenido incidentes de seguridad graves, no dejan de existir vulnerabilidades sobretodo con los funcionarios.

9. Qué factores considera usted inciden en el logro de los objetivos de la gestión de seguridad de la información en la entidad?

   Seguramente el factor principal es el factor humano ya que, en muchas ocasiones, los incidentes que tuvimos que reportar a la oficina central de sistemas en Bogotá fue por error humano. A veces incluso los usuarios no describían todo el incidente por miedo a

represalias, entonces se debía ahondar más en la investigación haciendo que el tiempo que se invirtiera en diagnosticar el riesgo y prevenirlo o mitigarlo fuera mayor de lo necesario.

10. ¿Cómo considera usted que las herramientas usadas para la gestión de seguridad de la información en la entidad ayudan a dicha labor?

    Definitivamente hay un avance significativo al usar medios en la nube para reemplazar servicios que teníamos a nivel local, por ejemplo, el correo electrónico era un dolor de cabeza cada que a un usuario se le olvidó la contraseña, cuando no se recibían correos enviados desde nuestro dominio porque estábamos en spam entre otros. Un aprendizaje importante es que la administración de ciertos servicios resulta ser una labor mejor adquirirla que mantenerla. En el caso del correo electrónico que usábamos, en Zmbra, la administración era una tarea muy compleja, y lo que lo hacía compleja era el sector humano. Ahora que tenemos un proveedor externo y de gran reconocimiento se invierte menos tiempo aunque deba invertirse económicamente, pero la seguridad si mejoró considerablemente, ya no tenemos tantos incidentes en ese tema.

    Por otro lado, usamos Barracuda como control de filtros de contenido, lo cual también ayuda mucho a prevenir ataques, mas no previene que se accedan a algunas páginas clonadas con engaños en los cuales a pesar de las capacitaciones dadas, algunos funcionarios caen en el timo.

    En definitiva, las herramientas ayudan en un porcentaje altísimo a salvaguardar la privacidad y confidencialidad de la información, y lo que no alcanza a proteger es por error humano.

11. ¿Qué propone usted para mitigar las fallas acaecidas en las posibles deficiencias en gestión de seguridad de la información si es que ocurren?

    Profundizar en la capacitación a los funcionarios y contratistas, y tratar de dar más continuidad a los trabajadores, porque aquella situación de entrada y salida rápida de trabajadores en el DANE también genera un desgaste administrativo y una barrera a la hora de tratar de fortalecer y mantener nuestra seguridad de la información, pero la capacitación es esencial.

Entrevista Responsable Apoyo Administrativo Sede Suroccidente Cali – Subsede Popayán

1. Nombre

   Eduin Acosta

2. Cargo

   Profesional Universitario, Coordinador Administrativo Subsede

3. Perfil

   Administrador de Empresas

4. ¿Desde hace cuánto es usted Apoyo Administrativo de la Subsede Popayán?

   Llevo 8 meses.

5. ¿Ha contribuido a la gestión de seguridad de la información en la entidad desde roles diferentes a este?

   Antes de este cargo era el profesional encargado de la investigación de índices la cual consume mucho tiempo operativo. Generalmente la concentración en el operativo me impedía percibir cualquier otro tema administrativo, entonces es solo ahora que vengo a visualizar el tema de seguridad de la información y lo que hago es delegar al contacto de sistemas de la sede para que apropie las actividades que se dirigen desde Bogotá.

6. ¿Cuál es el grado de madurez que usted considera tiene la entidad en cuanto a implementación de políticas de gestión de seguridad de la información?

   No podría realmente calificar este tema porque como mencioné no tuve mayor responsabilidad en este tema. Si he visto en intranet varios anuncios que promueven acciones en pro de la seguridad de la información, la mayoría deben partir de políticas establecidas para eso, pero no sé en qué estado está todo el sistema de seguridad del DANE.

7. ¿Cuál es el grado de madurez que usted considera tiene la entidad en cuanto a implementación de técnicas de gestión de seguridad de la información?

   Lo que conozco es que se mejoró mucho con el correo electrónico, el sharepoint y el firewall que usamos para que no se accedan a contenidos peligrosos y así coadyuvar con el proceso, pero tampoco conozco todas las técnicas asociadas a la seguridad de la información como para emitir un concepto que mida como vamos en su avance.

8. ¿Existe alguna brecha entre los objetivos de seguridad de la información planteados en la entidad y los resultados obtenidos?

   Considero que sí hay diferencia entre lo que se espera y lo que se obtiene, porque el objetivo del director es que no se escuche acerca de ningún incidente de seguridad, y éstos si ocurren.

9. Qué factores considera usted inciden en el logro de los objetivos de la gestión de seguridad de la información en la entidad?

   El acceso a las instalaciones sobre todo en sedes como la nuestra que no tiene portero puede causar que roben un equipo y con él se vaya información valiosa y confidencial, pero no es lo único, también hay gente que se lleva los equipos a las casas y allá no se tiene el mismo control sobre la información, además que pueden navegar en páginas que podrían robar información.

10. ¿Ha sufrido usted algún incidente en seguridad de la información?

    Personalmente no, pero si vi que a varios compañeros les fallaba el correo electrónico, enviaban mensajes a las fuentes y no llegaban, o llegaban a spam.

11. ¿Cómo considera usted que las herramientas usadas para la gestión de seguridad de la información en la entidad ayudan a dicha labor?

El control de contenidos Barracuda ayuda mucho, hay gente que trata de acceder a páginas que pueden llegar a ser peligrosas para la seguridad de la información y cuando no pueden acceder tienen que solicitar un permiso que evalúa sistemas para saber si lo concede o no, seguramente evaluando también el nivel de seguridad del sitio.

12. ¿Qué propone usted para mitigar las fallas acaecidas en las posibles deficiencias en gestión de seguridad de la información si es que ocurren?

    Que la gente sea concientizada constantemente, hay capacitaciones en las que nos entrenan pero como a cada rato cambia tanto contratista, meter ese tema en la capacitación de los aspirantes les deja a mucho 2 horas y no es suficiente para que los nuevos entiendan qué responsabilidad tienen y cómo deben actual frente a la protección de los datos que manejamos.

13. ¿Cuáles creen que son sus aportes a la seguridad de la información desde el rol que desempeña actualmente?

    Básicamente mi aporte es facilitar el espacio y exhortar a los responsables para que ejecuten y acaten las normativas al respecto.

Entrevista Responsable Operativo Sede Suroccidente - Subsede Popayán

1. Nombre

   Jorge Flórez

2. Cargo

   Profesional Universitario, Coordinador Operativo

3. Perfil

   Ingeniero Electrónico

4. ¿Desde hace cuánto es usted Apoyo Operativo de la Subsede Popayán?

   Llevo 6 años en este encargo.

5. ¿Ha contribuido a la gestión de seguridad de la información en la entidad desde roles diferentes a este?

   Si, desde que entré al DANE como contratista y por mi perfil en tecnologías, sé un poco de seguridad y cómo debemos apoyar este tema como usuarios internos, no con propiedad, pero siempre traté de ilustrar a los compañeros en ciertos errores que podían cometer, como por ejemplo dejar carpetas por fuera del archivo sin supervisión, el riesgo de prestar equipos, que las contraseñas no fueran tan fáciles, etc.

6. ¿Cuál es el grado de madurez que usted considera tiene la entidad en cuanto a implementación de políticas de gestión de seguridad de la información?

   Aparentemente ya con las mejoras que se han tenido, el sistema está andando, pero es reciente, todo lo planteado está desplegado, pero hace falta su evaluación.

7. ¿Cuál es el grado de madurez que usted considera tiene la entidad en cuanto a implementación de técnicas de gestión de seguridad de la información?

Igual que lo anterior, tanto las políticas como las herramientas han sido mejoradas sustancialmente, en este último periodo, pero con lo de la pandemia no se han emitido resultados de estos avances.

8. ¿Existe alguna brecha entre los objetivos de seguridad de la información planteados en la entidad y los resultados obtenidos?

   Sí, aún falta llegar al 100%, pero si se percibe una mejoría en la administración de los datos. Quizás el siguiente paso sea un detalle más específico de las políticas aplicadas en conjunto con un fortalecimiento del talento humano, sobre todo en lo que tiene que ver con la continuidad.

9. Qué factores considera usted inciden en el logro de los objetivos de la gestión de seguridad de la información en la entidad?

   Generalmente la inconciencia de algunas personas, ayudada con cierto bajo nivel de manejo de las tecnologías y la falta de apersonamiento por parte de los integrantes nuevos de la entidad.

10. ¿Ha sufrido usted algún incidente en seguridad de la información?

    Alguna vez intentamos enviar muchos correos con información que podría tener un riesgo de información, pero se logró mitigar interrumpiendo el envío masivo porque se pretendía enviar a más de doscientas personas en grupos de 10 para que el correo no fuera marcado como spam, y nos dimos cuenta en los primeros 10 que resultaron siendo colaboradores de la misma subsede, no alcanzó a filtrarse información al exterior.

11. ¿Cómo considera usted que las herramientas usadas para la gestión de seguridad de la información en la entidad ayudan a dicha labor?

Muchísimo, el firewall, el control de acceso, ahora con la pandemia la seguridad implementada a través de la VPN y el FTP contribuyen de manera colosal a la labor de seguridad informática.

12. ¿Qué propone usted para mitigar las fallas acaecidas en las posibles deficiencias en gestión de seguridad de la información si es que ocurren?

    Crear compromisos específicos y focalizados en seguridad de la información para el personal nuevo, que es donde se ve la mayor vulnerabilidad.

13. ¿Cuáles creen que son sus aportes a la seguridad de la información desde el rol que desempeña actualmente?

    Las recomendaciones que se le hace a los compañeros, además de las maniobras que implican el ejercicio de coordinador operativo de todas las investigaciones en curso en la subsede para la correcta salvaguarda de la información por parte de funcionarios y contratistas.