# INCIDENCIA DEL FACTOR HUMANO EN LA SEGURIDAD DE LA INFORMACIÓN DE LAS ORGANIZACIONES PÚBLICAS DE CATEGORÍA 6.

**LUIS JONALBER FERNÁNDEZ**

**UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD**
**ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)**
**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**
**TOLEDO NORTE DE SANTANDER**
**2020**

# INCIDENCIA DEL FACTOR HUMANO EN LA SEGURIDAD DE LA INFORMACIÓN DE LAS ORGANIZACIONES PÚBLICAS DE CATEGORÍA 6.

**LUIS JONALBER FERNÁNDEZ**

**Director**

**MBA Christian Angulo Rivera**

**UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD**

**ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)**

**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**

**TOLEDO NORTE DE SANTANDER**

**2020**

Nota de Aceptación

_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Diciembre de 2020

## DEDICATORIA

Este trabajo está dedicado primero al que lo ve y permite todo, el Dios padre celestial, a los dos pilares de mi vida mi madre y mi abuelita, a las personas que han pasado por esta etapa los cuales fueron soportes para poder dedicarme a la realización de esta meta y claro a la universidad que me ha dado las herramientas para llegar a este punto de mi carrera profesional.

## AGRADECIMIENTOS

Mi gratitud ante Dios, quien ha estado presente en mi vida y actúa en ella de diferentes maneras, él cual me bendijo con una madre y abuelita excepcionales al igual que otros seres queridos que por cuestiones de la vida ya no están presentes físicamente, pero si espiritualmente.

A mi madre, abuelita y abuelito, aunque él no esté ya en este mundo fue un pilar fundamental en mi niñez y que me permitió ser lo que soy en día, estas tres personas que han estado presente en las diferentes etapas de mi vida siendo una gran fuerza motivadora para lograr cada una de mis metas y seguir adelante después de cada uno de mis fracasos.

Agradecimientos a las personas de las alcaldías que me permitieron realizar la recolección de información que fue un gran insumo para este trabajo.

También mis sinceros agradecimientos a los tutores y directores quienes me guiaron en el transcurso del programa de especialización y que me permitieron realizar este trabajo.

## RESUMEN

En la presente monografía de investigación se explica cómo el factor humano sigue siendo uno de los eslabones más débiles de la seguridad de la información, esto debido a su carencia de conocimientos básicos de seguridad, que pueden comprometer a un alto nivel la información de las organizaciones, en especial se aborda las entidades estatales, como son las alcaldías de categoría 6, que son las instituciones del estado que menos pueden invierten en este campo de la seguridad debido a diferentes factores.

La información recopilada se realizó a través de encuestas a empleados de diferentes dependencias, tanto de planta como contratistas, ya que permiten entender los diferentes factores de riesgos que existen para estas entidades, no solo el grado de conocimiento si a factores como la rotación que existe por la dinámica de estas.

Las entidades gubernamentales en la actualidad son el "tercer sector que más recibe ataques cibernéticos cada día con 83.756 ataques por día"[1], muchas cuentan con los recursos para implementar sistemas de gestión de la seguridad de la información, según su categoría también dependen sus recursos, dentro de estas se encuentra la categoría 6, la que menos tiene recursos, ya que en ocasiones no cuentan con el presupuesto para implementar mecanismos que permitan salvaguardar la información que existe en esta, así como los procesos que interactúan con ella, dejándola susceptible ataques, esto no solo por la falta de elementos de protección a nivel de Software y Hardware, sino con la complicidad no consentida de los empleados, por la falta de aplicación de metodologías, marcos de gestión del riesgo, que permitan formular políticas o controles que minimicen los riesgos asociados al factor humano, que son el eslavo débil en los sistemas de seguridad, esto a través de diferentes técnicas que los delincuentes explotan.


[1] Revista Dinero. Los sectores económicos más impactados por el cibercrimen en Colombia Citado por La firma de seguridad informática Digiware. [En línea] Revista Dinero. 2017, 1 p. Disponible en https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321

## ABSTRACT

This research monograph explains how the human factor continues to be one of the weakest links in information security, due to its lack of basic security knowledge, which can compromise the information of organizations at a high level, in particular, state entities are addressed, such as category 6 mayors, which are the state institutions that invest the least in this field of security due to different factors.

The information collected was carried out through surveys of employees of different dependencies, both plant and contractors, since they allow us to understand the different risk factors that exist for these entities, not only the degree of knowledge but also the rotation that exists for their dynamics.

Government entities are currently the "third sector that receives the most cyber attacks every day with 83,756 attacks per day",[2] many have the resources to implement information security management systems, depending on their category, their resources also depend, Within these is category 6, the one with the least resources and at the same time the greatest risk, since sometimes they do not have the budget to implement mechanisms that allow safeguarding the information that exists in it, as well as the processes that interact with it, leaving it susceptible to attacks, this not only due to the lack of protection elements at the Software and Hardware level but with the non-consensual complicity of the employees, due to the lack of application of methodologies, risk management frameworks that allow the formulation of policies or controls that minimize the risks associated with the human factor, which are the weak Slav in security systems,this through different techniques that criminals exploit.



Keywords: Risk, information, human factor, ignorance, technology, methodology.


[2] Revista Dinero. Op. cit., p. 1

## Tabla de contenido

# LISTA DE TABLAS

# LISTA DE FIGURAS

# LISTA DE ANEXOS

# INTRODUCCIÓN

El presente trabajo se realizó luego de determinar un tema de estudio que pueda aportar a la comunidad, más específicamente a las entidades públicas que representan el pueblo, luego de realizar una investigación sobre como las personas, por la falta de conocimiento sobre el manejo de la información, se convierten en un blanco de los cibercriminales, siendo el integrante más débil de la seguridad informática y no como un activo valioso de esta. Con esta investigación se permitirá dar algunas pautas que permitirán mitigar de algún modo esta problemática, ya que cada día los ataques cibernéticos son más frecuentes, más específicos y más sofisticados, que pueden tomar días meses o años para lograr sus objetivos por lo que tener el personal consciente de ello permitirá disminuir los riesgos asociados a esto.

La sociedad siempre cree que la seguridad de la información depende de otros y que la responsabilidad es mínima para cada quien, más en las empresas u organizaciones no son conscientes y delegan todo esto a un departamento, área o grupo de personas, derivándose una serie de problemas que afectan a la seguridad de la información. Por eso, es importante que cada entidad u organización vele por la seguridad de su información y esto se puede lograr a través de capacitaciones, sobre algunos niveles básicos de los conocimientos de los empleados, a los que les permitan identificar unos mínimos riesgos y poder reportar comportamientos indebidos, que atenten contra los intereses de la empresa u organización, sobre todo cuando representa algún representa algún riesgo dineros públicos e información que puede ser aprovechada por los cibercriminales en perjuicio de otros.

# 1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad la gran parte de procesos de empresas privadas como del estado, están siendo llevados al ámbito digital, donde la información que reside en ellos es de vital importancia por los beneficios que representa tenerla en el ciber espacio, pero sin desconocer que en muchos casos estos procesos quedarán más expuestos a terceros que quieran tener dicha información con diferentes propósitos.

Esta información solo debe estar disponibles para las personas que están autorizadas, teniendo en cuenta que el gobierno viene implementando una estrategia llamada Gobierno en Línea hoy conocida como Gobierno Digital, la cual fue reglamentada en el Decreto 2693 de 2012 y que se actualizo con el decreto 1078 de 2015, entre sus funciones ha permitido la prestación de servicios del gobierno por medios electrónicos, como también la digitalización de la información.

Es importante la implementación de estrategias de protección, sabemos que entidades tanto de orden nacional como de tipo departamental, cuentan los recursos y diferentes maneras de proteger la información, los cuales se apoyan en otras entidades del estado como el Ministerio de Tecnologías de la Información y las Comunicaciones, el Centro Cibernético Policial (CCP), el Comando Conjunto Cibernético de las Fuerzas Militares(CCOC) y colCERT que entre sus objetivos se encuentra: “Coordinar y asesorar a CSIRT's y entidades público y privadas, promover el desarrollo de capacidades locales/sectoriales”[3] de los cuales se obtiene información para llegar a implementar un Sistema de Gestión de Seguridad de la Información(SGSI).

De manera que, se deben establecer planes para la gestión de incidentes en la seguridad de información, que por lo general requieren de unos recursos tanto humanos como de hardware y software, sin ser estos dos últimos el recurso más

[3] Ministerio de defensa, colCERT, Acerca de colCERT [En línea] Ministerio de defensa. 2017, 1 disponible en http://www.colcert.gov.co/?q=acerca-de

importante para las empresas u organizaciones.

Tal y como lo afirma la ex directora de National Cyber Security Centre (NCSC) Emma w "La seguridad de la información ha sido tradicionalmente liderada por la tecnología y como resultado, se ha pasado por alto el rol y el valor de las personas",[4] puesto que se descuida por completo este factor o "Como resultado, las organizaciones tienden a tratar a los usuarios como personas que deben hacer lo que se les dice, pero ellos no lo hacen siempre, y muchas veces la razón es simplemente porque no pueden"[5] debido a lo complicado de las políticas, controles establecidos los cuales no son prácticos. Por otro lado, el NCSC recomienda que se tenga una compresión sobre el cómo las personas puede llegar a ser un activo de seguridad y no el eslabón más débil, se pueden formular políticas que garanticen unos mínimos de la seguridad, ya que el empleado en muchos casos posibilita el riesgo a través de las redes sociales, que siendo bien usadas no representan peligro, pero como dijo Christie Terrill ex colaboradora de forbes "La información que sus empleados publican libremente en las redes sociales puede ser utilizada en contra",[6] acorde a esto y según un reporte CCP del 2017 "la mayor modalidad de ciber crimen es la estafa que se aprovecha de técnicas como la ingeniería social".[7]

De lo anterior se puede formular la siguiente pregunta ¿Cómo afecta el factor humano en las vulnerabilidades de la seguridad de la información especialmente en las entidades públicas de categoría 6 y que metodologías son recomendables para minimizar los riesgos asociados?, a esta pregunta se le intentara dar respuesta en este documento.

---

[4] ASHFORD, Warwick. La gente puede ser el eslabón más fuerte en la ciberseguridad, dice NCSC. [En línea] searchdatacenter. 2017, 1 p. Disponible en https://searchdatacenter.techtarget.com/es/cronica/La-gente-puede-ser-el-eslabon-mas-fuerte-en-la-ciberseguridad-dice-NCSC

[5] Ibíd., p. 1.

[6] TERRILL, Christie. What You Need To Know Now About Cybersecurity And Social Media, [En línea]. Forbes Media LLC. 2017, 2p. Disponible en https://www.forbes.com/sites/christieterrill/2017/04/28/what-you-need-to-know-now-about-cybersecurity-and-social-media/#6c98b6793a16

[7] Centro cibernético Policial, Policía Nacional, DIJIN. costos del cibercrimen en Colombia 2016-2017 [En línea] Policía nacional Dirección de investigación criminal e INTERPOL. 2017. 8p Disponible en https://caivirtual.policia.gov.co/sites/default/files/costos_del_cibercrimen_v4.pdf

# 2. JUSTIFICACIÓN

Entendiendo la importancia de la información en la actualidad, donde muchos de los procesos se realizan electrónicamente y otros se están sistematizando tanto a nivel privado como público, los procesos que están involucrados representan mucho dinero, que hacen parte tanto de particulares como de las entidades, en la cuales está la información y que puede representar todo lo que tenemos a nivel económico ya sea a nivel personal, empresarial o institucional.

Se entiende que sin la información y los mecanismos que se utilizan para el procesamiento de las actividades pueden verse afectada por la no disposición de esta o en casos más extremos la perdida de la información o alteración de la misma, conlleva a un detrimento de los recursos para particulares o para la entidad, ya sea por la pérdida de servicios o a nivel monetario por alteraciones.

De acuerdo con un artículo de la Revista dinero del año 2017, ocurren en "El sector Gobierno: 83.756 ataques por día"[8] es decir, los ataques cibernéticos se presentan en un 15% de los ataques diarios, de los cuales muchos son intencionados. Por lo que este sector tiende a invertir cada día más en ciberseguridad, aunque no es un hecho generalizado, un ataque efectivo puede representar una pérdida de dinero que en entidades de categoría 6 puede representar un gran problema para su desarrollo afectando al municipio en general, atrasando obras, incrementando costos, entre otros problemas asociados a la vulneración de la información.

Como se ha dicho, las empresas y entidades deben garantizar los tres pilares de la información la integridad, disponibilidad y confidencialidad, las cuales se ven afectadas por diferentes factores que pueden ser mitigables. Como lo hace notar un estudio realizado por el Ministerio de Tecnologías de la Información y Comunicaciones, junto con la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) sobre Colombia, en el cual se destaca

[8] Revista Dinero. Op. cit., p. 1

que: “De las organizaciones encuestadas más del 60% incurrieron en costos cercanos al millón de pesos por los daños relacionados con ciberataques, mientras que el 20% gastaron entre 1 y 15 millones de pesos, el 15% entre 15 y 235 millones y el 5% presentó valores desaforados de hasta 4.000 millones de pesos”,[9] debido a los incidentes de vulneración tecnológica.

Todas estas observaciones se relacionan también con que el sector gobierno es el tercero más atacado. De acuerdo con un informe de CCP del 2017, el cual revela que: “Por puertas traseras por infección de malware y la utilización de RAT Remote Access Tool para la ejecución de software malicioso que sirve para la transferencia ilegal y no consentida de Dinero, Información del sector público y Bases de datos las cifras de hurto por este delito ascienden a más de 50 mil millones de pesos solo en alcaldías a nivel nacional”.[10]

En consecuencia, se observa el elevado costo que pierden estas entidades si solo tenemos en cuenta el valor por este tipo de ataques, debido a que las entidades de categoría 6 son las que tienen menos recursos de libre destinación, por ello deben de implementar mecanismos para su protección, donde la aplicación de metodologías en la GSI (Gestión de la Seguridad de la Información) es una buena opción, ya que permite estructurar proyectos que estén orientados a optimizar los recursos, tanto económicos como los asociados al factor humano, donde se garantice la seguridad de la información.

[9] Revista Dinero. Op. cit., p. 1

[10] Centro cibernético Policial, Policía Nacional, DIJIN. costos del cibercrimen en Colombia 2016-2017 [En línea] Policía nacional Dirección de investigación criminal e INTERPOL. 2017. 12 p Disponible en https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf

# 3. OBJETIVOS

## 3.1 OBJETIVO GENERAL

Realizar un análisis de las diferentes metodologías que permiten detectar vulnerabilidades y amenazas propiciadas por el factor humano en los sistemas de la seguridad de la información en entidades de categoría 6.

## 3.2 OBJETIVOS ESPECÍFICOS

Efectuar un análisis que permita determinar que metodologías son aplicables para encontrar vulnerabilidades en los sistemas de información debido al factor humano en alcaldías de categoría 6.

Analizar el grado de conocimiento que tienen los empleados de una entidad de categoría 6 en cuanto a la seguridad de la información a través de la recolección de información que permita conocer la importancia de ella en sus trabajos.

Identificar las principales causas relacionados al factor humano que aumentan los riesgos de la seguridad de la información en la entidad de categoría 6 que permitan ser la guía para la toma de medidas.

Proponer un documento que permita la formulación de políticas de seguridad de la información de fácil aplicabilidad enfocadas en el factor humano que ayuden a reducir los niveles de vulnerabilidad que existen en las entidades de categoría 6.

# 4. MARCO REFERENCIALES

## 4.1 MARCO CONCEPTUAL

Se debe definir algunos términos para tener claro que se busca con este proyecto, es necesario investigar sobre algunos conceptos que son eje clave para orientar el trabajo de investigación. En primera instancia donde se puede presentar más confusión para las personas son dos términos ligados, pero que tienen diferentes concepciones, estos son la seguridad de la información y la seguridad informática, los cuales van ligados, que mejor manera para entenderlo a través del siguiente cuadro comparativo.

**Tabla 1 cuadro comparativo**

| | **Definición** | **Características** | **Diferencias** |
|---|---|---|---|
| **Seguridad de la información** | busca proteger la información independientemente de su formato como puede ser electrónico, papeles audio, conocimiento entre otros. | Proteger la información de las empresas u organizaciones, aunque en términos generales esto a través de la formulación de estrategias que correspondan a los tres factores fundamentales como la confidencialidad, disponibilidad e integridad.<br><br>Buen funcionamiento de los datos de las empresas y la transmisión de información de unos usuarios<br><br>Garantiza el adecuado funcionamiento de los datos y la respectiva transmisión de la información a los usuarios que están autorizados. | Se enfoca a nivel estratégico la cual determina la operatividad de la<br><br>seguridad informática.<br><br>Estable las pautas a seguir para la que la información se encuentre protegida. |

Tabla 1. (Continuación)

| | | | |
|---|---|---|---|
| **Seguridad Informática** | La seguridad informática es todo aquello que busca proteger la información que esta almacena en un sistema digital, se realiza a nivel operativo atendiendo a los tres aspectos que busca la Seguridad de la información agregando la protección física. | La seguridad informática garantiza la privacidad de la información.<br><br>Minimiza las vulnerabilidades de los sistemas.<br><br>Evita daños ocasionados por amenazas.<br><br>Se encarga de la seguridad física del sistema.<br><br>Y de la seguridad lógica. | Se encarga de la parte operativa de la protección de la información como es la instalación de antivirus, realizar pruebas a los sistemas utilización de software especializados como nessus, john the ripper entre otros. |

Fuente: Propia del autor

De la anterior tabla se entiende que la seguridad de la información y la seguridad informática buscan cumplir con los tres pilares de la información.

**Activos de información:** Son activos en la información los recursos que se utilizan para las organizaciones funcionen y que pueden afectar en diferente grado a los tres pilares de la información.

**Amenazas:** Es todo aquello que pueda afectar la seguridad de la información ya sea de manera intencional o no, partiendo de la existencia de una vulnerabilidad.

Pueden presentarse de manera lógica ataques de virus, acceso a sistemas sin autorizaciones.

Pueden ser de tipo físico como las ocasionadas por la naturaleza, daños físicos como instalaciones eléctricas dañas, daño en las conexiones de comunicación.

**Confidencialidad:** Este pilar se fundamenta en la cualidad que debe tener la información de no ser divulgada a terceros estos terceros son los que no están autorizados.

**Disponibilidad:** Este pilar tiene como fundamento que la información siempre debe ser accesible para los usuarios autorizados, independientemente de las circunstancias que se presenten como ataques cibernéticos o cualquier incidente que no permita tener acceso a la respectiva información. Un ejemplo de la actualidad es el acceso al banco por aplicaciones y se presentan incidentes donde los usuarios cuando estas no está disponible.

**Ingeniería social:** Definido por el Glosario Terminología Informática (GTI) como: "Técnicas de engaño utilizadas para inducir a alguien a revelar algún tipo de información sensible que comprometa la seguridad de un sistema informático".[11] Donde se explota factores como la curiosidad, la vanidad, el miedo, la ambición de las personas. Una definición más de ingeniería social es la manipulación psicológica llevando hacer que otras personas realicen no que uno quiere sin que se den cuenta. Otra definición es el arte del engaño para sacar información privada para el uso indebido de esta.

**Integridad:** Este pilar es el que garantiza que la información no sufra ningún tipo de manipulación, cambio o alteración por parte de terceros, debe mantenerse intacta preservar la exactitud y la coherencia en la información que se tenga almacena, la información solo pueda ser modificada por los usuarios autorizados.

**Normas de Seguridad**: "Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la

[11] PRIETO,José Luis ingeniería social [En línea] 1 p. Disponible en http://www.tugurium.com/gti/termino.php?Tr=social%20engineering&Tp=T&Or=0

Comisión Electrotécnica Internacional (IEC)".[12] Las cuales buscan instaurar estándares y guías para los sistemas de gestión en cualquier organización a nivel mundial.

**Políticas De Seguridad:** Son directrices de carácter técnico las que pueden ser de carácter físico o de índole humano las políticas deben enfocarse a las personas, ya que estos en los sistemas de la información son el jugador más importante depende de ello el funcionamiento de muchos procesos.

**Riesgos:** Son vulnerabilidades y amenazas a lo que está expuesta la información, la posibilidad de que esto ocurra y que genere impacto a nivel organizacional llevando a daño o perdida de información. Se presentan dos factores importantes en el riesgo como es el análisis y la administración de riesgos se pueden prevenir, pueden ser de tipo de seguridad, integridad, pertinente, disponibilidad e infraestructura, se pueden presentar desde el exterior o interior de la organización.

**Seguridad Legal:** Toda organización debe cumplir un marco legal sobre el territorio donde esta como son las leyes, normas y decretos.

**Vulnerabilidades:** Son ciertos fallos que presenta un sistema de información los cuales los exponen, estas se presentan en el entorno, facilitando que las amenazas pasen a ser vulnerabilidades.

[12] Gobierno de España, Normas ISO sobre gestión de seguridad de la información [En línea] 2014. 1 p. Disponible en http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

## 4.2 MARCO LEGAL

### 4.2.1 Legislación colombiana.

El estado colombiano que a partir de la constitución de 1991 modifico su hoja de ruta para buscar una mejor sociedad, fundamentado en lo dispuesto en ella se aprobó “la ley 136 de 1994 que buscaba modernizar el funcionamiento de los municipios la cual es la entidad fundamental de la división político administrativa del estado”,[13] en cuyo artículo 6 define las categorizaciones basados en dos características o requisitos para su categorización, como son la población existente, sus recursos fiscales, esta ley fue modificada con la Ley 617 de 2000 y la Ley 1551 de 2012, la cual establece nuevas modificaciones y se definen los requisitos que se deben cumplir para pertenecer a una categoría, si por población pertenece a una pero por sus ingresos por libre destinación no corresponden a esta, entonces estará en la categoría de los ingresos obtenidos, como se expresa en la siguiente tabla:[14]

**Tabla 2 Categoría municipios 1**

| Categoría | Población | Requerimiento adicional |
|---|---|---|
| Especial | Igual o superior a 500.001 habitantes | N/A |
| Primera Categoría | Entre 100.001 y 500.000 habitantes. | N/A |
| Segunda Categoría | Entre 50.001 y 100.000 habitantes. | N/A |
| Tercera Categoría | Entre 30.001 y 50.000 habitantes. | N/A |

Tabla 2, (Continuación)

[13] CONGRESO DE COLOMBIA, LEY 136 DE 1994(junio, 02, 1994). Por la cual se dictan normas tendientes a modernizar la organización y el funcionamiento de los municipios. El Congreso. Bogotá D.C., 1994. 37 p.
[14] CONGRESO DE COLOMBIA, LEY 1551 DE 2012 (Julio, 06, 2012). Por la cual se dictan normas para modernizar la organización y el funcionamiento de los municipios. El Congreso. Bogotá D.C., 2012. 15p. ARTÍCULO 7o.

| | | |
|---|---|---|
| Quinta Categoría | **Entre 10.001 y 20.000habitantes** | **Que tenga ingresos corrientes de libre destinación anuales que sean superiores a quince 15.000 y hasta 25.000 smlmv** |
| Sexta Categoría | Igual o inferior a 10.000 habitantes. | Ingresos corrientes de libre destinación anuales: No superiores a quince mil smlmv. |

Fuente: CONGRESO DE COLOMBIA, LEY 1551 DE 2012 (Julio, 06, 2012). Por la cual se dictan normas para modernizar la organización y el funcionamiento de los municipios. El Congreso. Bogotá D.C., 2012. 15p. [Consultado: 11 de octubre de 2019] ARTÍCULO 7o.

Siendo la categoría mínima para los que no tienen ingresos anuales de libre destinación de un valor de $ 12.421.740.000 a fecha de 2019, por lo que los recursos que ellos tienen son priorizados y no tienen mucho margen para contratar servicios especializados para el desarrollo de políticas de seguridad de la información, entre las funciones del estado está la protección de la ciber seguridad, la cual se define: "Como la capacidad del Estado para minimizar el nivel de riesgo cibernético al que están expuestos los ciudadanos, en áreas como transacciones financieras, protección a la información y propiedad intelectual",[15] entonces es deber de las entidades garantizar y proteger la información que en estas existen más cuando la información que reside en ella es de la ciudadanía y le compete a todos.

### 4.2.2 Normativa colombiana en el marco de la seguridad de la información

La primera norma que rige a todos los colombianos y personas que están en el territorio es la constitución de 1991, por lo cual cualquier norma o ley no debe ir en contra de ella, según el proyecto de investigación de Borrero Cortés los siguientes son artículos que ven con la función del estado y las garantías que este debe de dar

[15] Borrero, Cortés, Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia Citado por BNamericas, Business insight in Latin America, Colombia elabora política de ciberdefensa y ciberseguridad.[En línea] 2014, p. 19 http://www.bnamericas.com/es/news/tecnologia/colombiaelabora-politica-de-ciberdefensa-y-ciberseguridad

contemplados en el 2, 15, 20,23, 74, y el 78, lo cuales de manera o indirecta, aseguran al pueblo colombiano tener el acceso a la información de manera oportuna y autentica tratando el Estado de cumplir con ello aprobado algunas leyes que van en caminado a tal fin.

**Tabla 3 Leyes 1**

| Ley | Propósito |
|---|---|
| **527 de 1999** | Comercio electrónico y de las firmas digitales |
| **599 de 2000** | Código penal colombiano. |
| **603 de 2000** | Legalidad de los softwares |
| **962 de 2005** | Racionalización de trámites (Ley antitrámites) |
| **1150 de 2007** | Modificación al estatuto de contratación pública. |
| **1266 de 2008** | Habeas Data. |
| **1273 de 2009** | Delitos Informáticos. |
| **1341 de 2009** | Sociedad de la información y las TIC |
| **1581 DE 2012** | Protección de Datos Personales. |

*Fuente:* Borrero, Cortés, Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia [En línea] Revista de Derecho Comunicaciones y Nuevas Tecnologías Universidad de los Andes. 2015. 17 p[Consultado: 11 de octubre de 2019] . Disponible en https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics227.pdf

Las anteriores leyes así como los decretos Decreto 2693 de 2012 - Gobierno en línea y Decreto reglamentario 1377 de 2013 - protección de datos personales, en especial con el Decreto de Gobierno en Línea, del cual se especifica su evolución con las diferentes modificaciones hasta la más reciente del presente año, es importante conocer los decretos que la rigieron y rige actualmente, ya que este decreto es el que coloca la información a disposición de los ciudadanos, así como de muchos procesos que se llevan a cabo en las entidades territoriales como son las entidades de categoría 6, la evolución de la estrategia es:

## Tabla 4 evolución de la estrategia Gobierno Digital

| Decreto | Versión | Nombre |
|---|---|---|
| **Decreto 1151 de 2008** | Versión 1 enero 2010 | Manual para la implementación de la Estrategia de Gobierno en Línea |
| **Decreto 1151 de 2008** | Versión 2 Julio de 2011 | Manual para la implementación de la Estrategia de Gobierno en Línea v.2.0 |
| **Decreto 2693 de 2012** | Versión 3 2012 | Manual para la implementación de la estrategia de gobierno en línea 2012-2015 |
| **Decreto 1078 de 2015. Título 9. Capítulo 1 (Incorpora el Decreto 2573 de 2014)** | Versión 4 | 2015 Manual Estrategia de Gobierno en Línea |
| **Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1. - (Preliminar)** | Versión 5 agosto de 2018 | Manual para la Implementación de la Política de Gobierno Digital |
| **Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1.** | Versión 6 diciembre de 2018 | Manual para la Implementación de la Política de Gobierno Digital |
| **Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1.** | Versión 7 abril de 2019 | Manual para la Implementación de la Política de Gobierno Digital Incorpora los lineamientos para la integración al Portal Único del Estado Colombiano |

Fuente: República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. MANUAL DE GOBIERNO DIGITAL Implementación de la Política de Gobierno Digital Decreto 1008 de 2018 [En línea]. Bogotá: 2018. 89 p. [Consultado: 3 de febrero de 2020]Disponible en https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

De las anteriores leyes y decretos que nos han regido hasta a la actualidad, la mayoría de ellos están en mora de ser actualizados, ya que tiene más de 20 años de antigüedad, lo que nos dice que para ese entonces el país fue un referente en legislación, esto porque considero varios de los delitos que en la actualidad se sigue cometiendo, pero muchas de las nuevas modalidades no están bien tipificadas en la ley 1273 de 2009 plasmada en sus dos capítulos y artículos de la cual se hace una reseña a continuación:.

**CAPÍTULO I - Ley 1273 de 2009**

Trata sobre los atentados contra los tres pilares de la información y los sistemas informáticos:

Artículo 269A: Trata sobre el acceso abusivo a los sistemas informáticos. El cual es de los delitos más cometidos hoy en día, a través de las diferentes herramientas que se consiguen en internet, por lo que el que este consagrado es importante para ley colombiana, en este entrar los crackers, haciendo anotación que un hacker de sombrero blanco, no entraría en este artículo ya que lo estaría haciendo con permiso de los dueños del sistema para encontrar dichas falencias, ya que sin este permiso. se considera un delito.

Artículo 269B: Abarca la obstaculización ilegítima de los sistemas informáticos o redes de telecomunicación de manera no autorizada, en este se tratan delitos como la denegación de servicio, como les ha pasado a varias páginas del estado, que son las que más se ven atacadas por esta forma de delito informático.

Artículo 269C: Comprende la interceptación de manera ilegal de los datos informáticos, es un artículo que si se aplicara hoy en día generaría un caos judicial, pues es común ver cómo le interfieren las redes sociales a las personas, esto a través de diferentes medios como sería la utilizan de algunas aplicaciones que son de uso ilegal, como la clonación de aplicaciones o utilizaciones propias de las aplicaciones por nombrar una la opción de WhatsApp web que permitirá que una

persona que tenga acceso pueda activar dicha opción teniendo información de la otra persona sin ser autorizadas.

Artículo 269D: Comprende los daños Informáticos que sean producidos con conciencia de esto, donde afecta no solo la parte lógica sino física, provocando algún daño en los equipos, por ejemplo, daño al sistema operativo, un programa, un disco duro, computadores, redes entre otros, es decir, un cracker.

Artículo 269E: Trata sobre el uso de software malicioso, este articulo entra a definir las herramientas que los crackers usan como un delito más de los que comenten.

Artículo 269F: Comprende la violación de datos personales, para este caso el robo de una cuenta de correo electrónico, bancaria, etc., se considera en Colombia como un delito y presenta una multa grande, pero que lamentablemente, no se aplica por desconocimiento de las personas que sufren de este tipo de delito.

Artículo 269G: Comprende la suplantación de sitios web para capturar datos personales, esto se puede observar en un ejemplo común, como es la captura de la información de las cuentas de redes sociales tales como Facebook, una modalidad seria a través de páginas similares donde las personas ingresan sus datos creyendo que es la original dejando sus datos en ella y luego son redirigidos a los sitios originales, lo que se denomina clonación de páginas.

> Artículo 269H: Comprende las Circunstancias de agravación punitiva, donde se aumentarán de la mitad a las tres cuartas partes si la conducta se comete siendo servidor público en ejercicio, o para la obtención de provecho para sí o para un tercero, entre otros.
> CAPÍTULO II de la Ley 1273 de 2009
> De los atentados informáticos y otras infracciones
> Artículo 269I: Hurto por medios informáticos y semejantes.
> Artículo 269J: Transferencia no consentida de activos.[16]

[16] CONGRESO DE COLOMBIA, LEY 1273 DE 2009 (enero, 05, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. El Congreso. Bogotá D.C., 2009. 2 p.

### 4.2.3 Leyes, resoluciones y lineamientos que deben cumplir las entidades.

El ministerio del TIC y otras entidades de orden nacional buscan la implementación de estrategias que permitan garantizar los tres pilares de la seguridad, haciendo al estado desde sus diferentes entidades un estado seguro en el ciberespacio para esto, propuso algunas resoluciones, decretos, leyes encaminadas a la seguridad informática, pero lo que se puede observar es que en muchas situaciones esto, no es una realidad debido a las falencias que se encuentran en la aplicación las mismas.

Es por esto por lo que todas las entidades deben diseñar e implementar algunas estrategias, en especial aquellas que son fundamentales para garantizar la seguridad de la información, tal como muestra el Plan Estratégico de Tecnologías de la Información PETI, el cual define algunas metas realizables para las entidades u organizaciones a corto mediano y largo plazo.

Conviene subrayar que lo que se pretender lograr es "Verificar si existen falencias sencillas a través de las encuestas a realizar, como el procedimiento que deberían realizar ante cualquier situación anómala que se presente en las entidades como daño por virus, entre otras situaciones, más sabiendo que existe el decreto 1078 de 2015, el cual establece los lineamientos generales de la Estrategia de Gobierno en Línea".[17]

Por otra parte, el ministerio aporta guías que permiten evaluar los problemas que se pueden presentar, también aporta Técnicas aplicadas para la autoevaluación como son MRAE Marco de Referencia de Arquitectura y el MPSI (Modelo de Seguridad y Privacidad de la Información).

[17] República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. MANUAL DE GOBIERNO DIGITAL Implementación de la Política de Gobierno Digital Decreto 1008 de 2018 (14 de junio de 2014) [En línea]. Bogotá: 2018. 89 p. Disponible en https://www.mintic.gov.co/portal/604/articles-5271_Peti.pdf

## 4.3 MARCO TEORICO

### 4.3.1 El factor humano en la seguridad de la información

#### 4.3.1.1 La ingeniería social como determinante en la seguridad de los sistemas

Lo que respecta a la conducta de las personas en la seguridad de la información se puede abordar desde la ingeniería social la cual aprovecha la conducta humana para que este sea la vulnerabilidad del sistema.

La ingeniería social se basa en tres factores:

- La confianza que la persona siente sobre el otro.
- La autoestima a través del fomentar el ego por medio de alabanzas, cumplidos, etc.
- El deseo y la curiosidad aprovechándose de la ingenuidad de las personas con mensajes en los correos o redes sociales en lo que se regalan cosas, descuentos, noticias espectaculares, que la gente le es difícil de evitar y terminan siendo aprovechadas por los cibercriminales.

#### 4.3.1.2 Tipos de ingeniería social

De acuerdo con la mirada teórica de Pablo F. Iglesias Consultor de Presencia Digital y Reputación Online, se puede considerar que existen dos grandes tipos de ingeniería social, el primero el Hunting, el cual se enfoca en ataques donde se tiene la menor exposición con la víctima, tiende a ser un solo contacto, como por ejemplo a través de un correo, donde el atacante genera el enlace para la recolección de información, el segundo es el Farming el cual es lo contrario del hunting, donde busca un contacto mayor, para mantener un engaño por más tiempo, para extraer la mayor cantidad de información posible, donde no es fácil de conseguir a través de medios que no impliquen contacto con la persona, ya sea por medio físico o a través de algún medio de comunicación, también se podría distinguir dos

clasificaciones, las que se dan de manera física con iteración humana y las que utiliza los medios de la tecnología.

Dependiendo de su funcionalidad y el tipo de ataque se pueden clasificar de diferente forma, de acuerdo con el autor Emiliano Piscitelli especialista en ingeniería social, quién en la revista USERS edición 293, plantea algunas concepciones sobre las formas de ataques, tales como:

**Tailgating:** Explota la buena fe de las personas, al ganarse la confianza u aprovechándose de situaciones para la explotación de ellos

**Dumpster Diving:** Esta técnica se trata de buscar en la basura de las personas, aunque parezca raro esta técnica puede permitir encontrar información importante, ya que las personas al votar la basura no son conscientes de la información que va en esa basura, como datos de cuentas, correos hasta contraseñas escritas en papeles, información que para un atacante es de suma importancia.

**Distracción o Misdirection**: Esta técnica se basa en la utilización del ilusionismo o magia, donde lo que busca es distraer a las personas, para realizar la actividad planeada, por ejemplo, realizar una conversación con temas que entretenga a la víctima, mientras se observa o consigue alguna información relevante, o el robo de algún elemento si es en el caso físico.

**Baiting:** Es una técnica que se aprovecha de la curiosidad de las personas, la forma en que se usa usualmente es dejando una USB, que será conectada a un equipo por la persona que se la encuentro, lo que permitirá la instalación de programas ocultos en archivos como fotos, que al abrir dichos archivos instalar programas para el robo de información, por lo general esta técnica es utilizada con información recabada anteriormente para una fácil explotación.

**Shoulder Surfing:** Una técnica sencilla, pero en muchos casos efectiva y se trata de espiar a la persona, como el simple hecho de mirar por encima del hombro, por un espejo, con lo que se pueda ver información relevante, como por ejemplo cuando ingresan un patrón en un celular o una contraseña de alguna aplicación, permitiendo observar que fue lo digitado.

**Redes Sociales:** Este tipo de técnica puede ser usada con dos propósitos, el primero y el más utilizado es para el robo de información, que las personas sin ser consientes suben, como por ejemplo fotos en las empresas donde trabajan con información, que no debería estar expuesta a tercero, como equipos, datos entre otros elementos. También se usa para la recolección de datos de las personas, que permita tener información para realizar un ataque, el otro propósito es buscar ganarse la confianza de las personas, esto a través de contactos falsos, que permitan la recolección de información más confidencial.

El siguiente tipo de ataque es al que más está expuesto las personas, más de organizaciones o entidades como es el caso de las entidades del gobierno, ya que los cibercriminales antes de realizar un ataque tratan de tener la mayor cantidad de información posible, para realizar de manera efectiva un ataque, que los lleve a la explotación del eslabón más débil de muchas organizaciones, como es el talento humano.

**Phishing:** Esta técnica como ya se ha mencionado es de las más utilizadas, se trata de la suplantación, como su nombre nos indica es pescar a incautos, la modalidad más explotada es a través de correos electrónicos, que aparentan ser de un contacto que tenemos registrado o de empresas reconocidas, los cuales vienen generalmente con enlaces que llevan a paginas clonadas o páginas que permiten la descarga de malware, la otra modalidad es la que trae documentos adjuntos que tienen consigo los malware, que al abrir dichos archivos se ejecutaran sin que el

usuario se dé cuenta, infectando su equipo permitiéndole al atacante obtener información, como usuarios, contraseñas entre otra información confidencial. Dentro de este tipo de ataque se puede clasificar en 4 tipos según, Wolfgang ERHARDT [18].

- El “phishing” común, el cual se utiliza por correo electrónicos o por chats, a través del engaño, haciéndole creer a la víctima que su comunicación es con una persona u organización confiable, confiado de ello abre enlaces o archivos que permitirán la vulneración de los sistemas informáticos.

- El “spear phishing” es similar a la anterior, pero es mucho más personalizada ya que el atacante ya tiene información de la víctima lo que permite que la comunicación sea más creíble y la persona caiga fácilmente.

- El “clone phishing” esta es una técnica más elaborada, ya que la comunicación con la victima va a ser de un correo legítimo, dando total seguridad a la víctima que el mensaje que recibe es efectivamente de esa persona, realizando lo que quiere el atacante por la confianza que la víctima tiene depositada en el remitente, llevándola a descargar los archivos con confianza o a entrar a sitios clonados como consecuencia un ejemplo de esto sería dando su información.

- El cuarto tipo es el “whaling” este tipo de phishing es el más elaborado, ya que va dirigido a un individuo en específico por lo que antes ya han usado más técnicas de recolección de información que permitan realizar un ataque efectivo.

[18] ERHARDT, Wolfgang. Identifica los diferentes tipos de phishing [En línea] 2017. 1 p Disponible en https://www.forbes.com.mx/identifica-los-diferentes-tipos-de-phishing/

Tal y como lo hace notar una encuesta realizada por el instituto SANS en el 2017, en la cual se encontró que entre las mayores amenazas están: "Phishing (72%), spyware (50%), ransomware (49%) y troyanos (47%)",[19] siendo la primera susceptible a la ingeniería social y lo más preocupante es que: "74% de las amenazas ingresadas como un archivo adjunto o enlace de correo electrónico, el 48% ingresó al navegador",[20] lo que indica que las personas son las que se encargan de ingresar las amenazas, ya sea por archivos adjuntos o enlaces que creen son confiables.

Por otro lado, un informe de investigadores de seguridad de IBM (IBM X-Force Researc) en 2014 dio a conocer que: "Un 95 por ciento de las ataques o incidentes en materia de seguridad se deben a fallos humanos".[21] Asimismo, un informe IBM X-Force Threat Intelligence Index – 2019 dice que: "Casi un tercio (29 %) de los ataques analizados por X-Force IRIS involucraron compromisos a través de correos electrónicos de phishing".[22] De donde se infiere que, 1 de cada 3 ataques se realizan por la modalidad de Phishing, que cada día son más personalizados y profesional, siendo estos dirigidos con objetivos claros, dejando como consecuencia costos significativos para las organizaciones o entidades.

Por otra parte, es importante destacar el reporte realizado por el FBI en relación a Estados Unidos el cual reveló que: "El fraude BEC ha estado creciendo rápidamente en los estados unidos y en todo el mundo, lo que les ha costado a las organizaciones

[19] NEE, Lee 2017 Threat Landscape Survey:Users on the Front Line[En linea] SANS Institute 2017. 27 p. Disponible en https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910

[20] Ibíd., p. 10.

[21] Ccn-cert El 95 por ciento de las incidencias de seguridad se deben a errores humanos internet [En línea] CCN-CERT2014 1 p. Disponible en https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/1152-el-95-por-ciento-de-las-incidencias-de-seguridad-se-deben-a-errores-humanos.html

[22] IBM Security X-Force Threat Intelligence Index2019 [En línea] IBM 2019 36 p. Disponible en https://www.ibm.com/downloads/cas/ZGB3ERYD

$ 12.5 mil millones al último recuento",[23] lo anterior es lo que representa en estados unidos, debido al verse comprometidos los correos electrónicos comerciales y que de estos el 36% corresponde a phishing los cuales van de la mano de la ingeniería social.

Todo esto, reafirma la importancia de estar preparado para el Phishing, junto con el spamming, que además está ligado al ransomware, e indica que en la seguridad el factor humano es el mayor causante de los problemas en las organizaciones, en donde los ataques se centran en las personas y no en la tecnología, de lo anterior radica la importancia de formular estrategias encaminadas a la identificación de las vulnerabilidades y riesgos, debido a este factor en los sistemas de información.

### 4.3.2 La conducta humana como factor de riesgo.

La conducta humana tiene diferentes factores que pueden ser explotados por su naturaleza algunos de estos factores son:

#### 4.3.2.1 Factores explotables.

- **La confianza:** No la que se tiene en sí mismo sino la que se deposita en los demás, este valor que se fomenta tanto a nivel personal como delas empresas u organizaciones para mejorar la productividad de ellas, siendo un factor clave del comportamiento organizacional, para este caso resulta ser un inconveniente sobre todo cuando es aprovechada por técnicas para recolectar información, como la ingeniería social haciendo esto más sencillo para el atacante sin tener que realizar una ingeniería social compleja, al ganarse la confianza fácilmente de una persona, por ejemplo por redes sociales donde es fácil encontrar información que permita hacerle creer que

[23] Ibíd, p. 7.

tienen similitudes o cosas en común, permitiendo explotar este valor a favor del ciberdelincuente.

- **La rutina:** La costumbre de realizar cada vez lo mismo tanto en la parte personal como laboral, es otro factor que influye como de riesgo ya sea para un ataque de ingeniería social o en el aprovechamiento de esto, para la obtención de información de manera física con otros propósitos, al tener claro los horarios de la persona interesada, permitirá saber a qué horas entran y salen, hasta los horarios de descanso y en que los usan, tanto a nivel físico como en el ciber espacio, siendo esto todos los días puede llegar a ser un factor a tener en cuenta como un de riesgo.
- **El ego:** El exceso de valoración sobre sí mismo, permite que el ingeniero social se aproveche de esta situación para llevar acabo sus actividades, valiéndose del ego de la víctima para de cierta manera ganarse su confianza de manera fácil, permitiendo cumplir el objetivo de sacar la información requerida, más cuando se complementa con otros factores, que influyen a que las personas puedan realizar acciones que no quiere, como averiguar información de otras o datos sensibles, al igual a realizar acciones como no debe, un ejemplo de ello es conocer algo de la persona y presentarle un reto a través de un red social u otro medio, que permita abrir enlaces que posibiliten la ejecución de códigos maliciosos.

- **La autoestima:** Es una condición que puede ser explotada, más cuando una persona pueda llegar a tener una autoestima baja, se puede volver una persona influenciable lo que para un ingeniero social u otra persona permita la instrumentalización de dicha persona para lograr sus objetivos, induciéndola a realizar actividades que cree que le permiten tener aceptación así sea de un desconocido o de una persona cerca que se quiere aprovechar de esto también.

- **La mentalidad:** Este factor puede variar según las culturas y sociedades, pero todas tienen en común que son la representación de una sociedad, el cual es explotable según el individuo que se aborde y su formación, con un estudio a sus comportamientos se puede determinar quién es susceptible para el aprovechamiento de esta condición, un caso común es la aceptación de algunos hechos que van en contra de las normas, pero que culturalmente puede estar arraigado en dicha sociedad.
- **La aceptabilidad:** Esta va en conjunto con la mentalidad, tomando de referencia el país de Colombia su cultura es aceptado la corrupción en cierto grado, con justificaciones como que este robo pero hizo, aunque esto vaya en contra de las normas o leyes, tienen de a ser aceptados algunos hechos como normales, lo que hace que algunos individuos puedan ser abordados para la consecución de información a cambio de beneficios de índole material o de consecución de logros como podría ser un mejor empleo, un ascenso entre diferentes incentivos que pudieran usarse para dicho propósito.
- **La responsabilidad:** Este valor es uno inherente a la educación y la sociedad, que en cierto punto puede afectar a una empresa, debido a que muchas personas toman solo por responsabilidad lo que se le es asignado, sobre todo donde se tienen manuales de funciones y responsabilidades, los empleados solo se sienten comprometidos y responsables de lo que se les asigno, más no de lo que no esté ahí, como popularmente se dice “no es mi problema”, esto refleja una cultura de una sociedad que logran ver los impactos en el sistema como tal.
- **La lealtad:** Este valor que representa una virtud de una persona hacia otra persona, empresa, organización entre otros, este compromiso permite tener un grado de responsabilidad mayor, el cual en algunas ocasiones puede ir en contra de otros valores, en algunos casos por la lealtad se quebrantan otros, que la persona cree que lo correcto es su lealtad con la persona u organización, el problema de este valor radica cuando a través de un

chantaje se pueda utilizar a una tercera persona para la explotación de otra, en muchos casos se presenta en la delincuencia común.

- **Conocimiento:** Según la RAE la define como: “La acción y efecto de conocer”,[24] esta capacidad que tiene las personas para comprender de manera racional los sucesos que lo rodean, sobre lo que conocen, es un problema cuando no se tiene el debido conocimiento y a las personas nunca les gusta demostrar que no sabe, porque se piensa que será catalogado como un ignorante, por lo cual realizan acciones empujados por esto, siendo esto un problema, un ejemplo de ello son llamadas para extraer información haciéndose pasar por algún organismo de control que necesita alguna información importante, la otra parte es cuando la persona sabe demasiado y tiende a querer que los demás realicen tal cual sea su pensamiento, creyendo su manera de pensar basado en lo que conocen es la única manera .

- **Miedo:** Esta condición humana permite que ante algunas situaciones las personas actúen de cierta maneras que no son coherentes, esto es muy utilizado para la explotación, sobre todo en la navegación por internet, en páginas contaminadas donde las personas pueden ingresar buscando una información o por curiosidad, en la cual encontraran mensajes tales como que el equipo se encuentra infectado, generando algún tipo de impacto y reacción en las personas, llevándolas a seguir una serie de pasos que recomienda en dichos mensajes que va llevando a realizar lo que el atacante desea, terminando por conseguir la información necesaria para realizar algún tipo de ataque o el ataque en sí.

Existen muchos factores en la personalidad que se podrán utilizar para explotar una persona a conveniencia de la ingeniería social, no solo en este campus son explotables, sino también en muchos ámbitos de la vida, como por ejemplo las

[24] Real Academia Española, conocimiento [En línea] Disponible en https://dle.rae.es/conocimiento

estafas que eran comunes con la suplantación de identidades de manera física falsificando papeles, hoy en día estas están el ciber espacio y son el pan de cada día en sus diferentes modalidades.

ante estas modalidades delictivas tanto físicas como virtuales las personas siguen cayendo en ellas, a pesar de conocer los métodos como las llamadas, un ejemplo de ello son las llamadas de los bancos, los familiares, sobrinos, entes gubernamentales entre otros, los cuales nunca se verifica si son ellos y la información dada es cierta, ahora que la delincuencia se está sofisticando y evolucionando constantemente, tal y como lo expresa Cecilia Pastorino, Security Researcher de ESET Latinoamérica donde hace referencia a que: "La mayoría de estos engaños van mutando con el tiempo, por eso decimos que son difíciles de erradicar porque por más que se eduque a los usuarios, los atacantes van cambiando la forma y las técnicas para engañar",[25] de aquí la importancia de que las personas tenga un conocimiento más estructurado sobre la seguridad informática o seguridad de la información, aunque las modalidades de ciberataques vayan evolucionando..

Así lo plantea John Stewart, vicepresidente sénior y Director de Seguridad en Cisco, quien afirma que: "Con la sofisticación que utilizan los adversarios, es difícil saber si se debe hacer clic en un enlace o abrir un archivo adjunto cada vez".[26] De donde se infiere que, por más que se le enseñe un proceso a una persona siempre va existir el riesgo para los empleados y las empresas de caer en las trampas de los cibercriminales.

[25] CANCINO, Héctor. Factor humano: ¿cómo combatir al eslabón más débil en la cadena de la ciberseguridad? Citado por Cecilia Pastorino [En línea] Revista AméricaEconomía 2019 3 p. Disponible en https://tecno.americaeconomia.com/articulos/factor-humano-como-combatir-al-eslabon-mas-debil-en-la-cadena-de-la-ciberseguridad

[26] Ibíd. P 2.

De acuerdo con el último reporte de ESET [27] publicado en el 2019 en Colombia, en el cual se encontró que de las empresas encuestadas los incidentes ocurridos en los últimos 12 meses, el 19% correspondió a ataques de ingeniería social, así mismo este reporte permite ver las preocupaciones de las empresas, que para este caso de estudio es importante tener en cuenta, ya que el 20% de las empresas colombianas se preocupan del uso inapropiado de la infraestructura y el 26% de la falta de disponibilidad de servicios críticos, cómo podemos ver en nuestro medio es importante el factor humano en los incidentes directos como es la ingeniería social.

#### 4.3.2.2 Virtudes de los ingenieros sociales

Una vez conocidas las diferentes miradas teóricas sobre la ingeniera social, se debe conocer que es un ingeniero social, sus virtudes y su importancia, basados en una de las frases del famoso libro chino el Arte de la Guerra para Negocios dice: "Conoce a tu enemigo y conócete a ti mismo, así en 100 ... así en 100 batallas nunca estarás perdido",[28] esto no es más que si se cuáles son las cualidades de las personas que pueden atacar un sistema, permitirán establecer estrategias claras y bien estructuradas, que sean robustas e integras a la hora de enfrentar en este caso las técnicas de ingeniería social, que son hechas con mucha astucia y creatividad.

- **Persuasión:** Es la capacidad que tiene una persona para influenciar en las creencias, actitudes, intenciones, comportamientos entre otros factores, esto lo logran con el convencimiento a través de la forma de actuar, permitiendo cambiar el pensamiento o actitud para que realicen una actividad, muchas veces se utilizan los gustos en común que hacen creer que se tienen, mensajes u acciones de demanda inducida, lo que significa hacerle creer que está ante una posibilidad única que no puede dejar pasar, o con estrategias

[27] ESET, LLC y ESET, spol. s.r.o. Compare la seguridad de su empresa con las de su país [En línea] ESET 2019 1 p. Disponible en https://security-report.eset-la.com/

[28] SUN ,Tzu. El arte de la guerra, siglo V a. C. antigua china

elaboradas con participación de varias personas, como por ejemplo la creación de grupos que induzcan a la víctima a realizar una acción, todo esto lo sabe explorar muy bien un ingeniero social quien elabora las estrategias según el estudio que le realiza a la víctima.

- **Elocuencia:** La capacidad de hablar de manera fluida con propiedad, en muchos casos de manera elegante y persuasiva, es un requerimiento que debe tener un ingeniero social, ya que en la elaboración de sus estrategias debe utilizar diferentes medios de comunicación, como correos electrónicos donde los mensajes escritos deben ser muy convincentes, para que la víctima presione o haga click sobre lo que contiene el mensaje, en los casos de extracción de información de manera personal esta característica sale a relucir, como es el caso de los estafadores, donde se puede decir que engañan a las personas con la manera de expresarse sin que dejen que la víctima actué.
- **Imaginación:** Las personas que tienen imaginación, tienden a tener empatía y habilidades sociales, que van de la mano con la creatividad, lo que le permite a las personas que tienen esta habilidad desarrollada, fantasear con posibles futuros o posibilidades, por ejemplo elaborar posibles estrategias en la mente sin que esto necesite llevarse a cabo, permitiendo realizar una especie de laboratorio, lo que le permite tener diferentes planes de acción o tener la capacidad de responder rápidamente ante un suceso, o anticipar antes de que ocurra o esté sucediendo.
- **Innovación:** Esta capacidad no solo significa inventar algo nuevo, como es el caso de los ciber delincuentes que a una amenaza muchas veces le cambian es la cara para realizar lo mismo, esta capacidad de realizar lo mismo pero de diferentes maneras, en la práctica sería una vez que es detectado la forma de operar de una infección por los diferentes mecanismos de seguridad como antivirus, firewalls, ids entre otros, estos cambian algunos factores para lograr una vez más, así como en la historia las personas han

utilizado herramientas del pasado que son retomadas en la actualidad, como es el caso de la criptografía que fue utilizado en el pasado por los egipcios o los romanos, cuando no existía la computación pero cifraban la información, hoy en día se utiliza esos mecanismo pero aplicados a nivel computacional, por lo que reinventar algo algunas veces puede ser más grandioso que crear algo nuevo.

# 5. DESARROLLO DE LA INVESTIGACIÓN.

## 5.1 ANÁLISIS DE METODOLOGÍAS APLICABLES PARA ENCONTRAR VULNERABILIDADES DEBIDO AL FACTOR HUMANO EN LAS ALCALDÍAS DE CATEGORÍA 6.

### 5.1.1 Metodologías para la gestión de la seguridad de la información

Basados en los temas tratados en el marco teórico como son los métodos de ataques para robar información como la utilización de la ingeniería social, Phishing entre otros, radica la importancia de contemplar la puesta de un SGSI en cualquier organización o ya sea la aplicación de una norma como la ISO 27001 o el anexo A de esta norma.

El SGSI ( Sistema de Gestión de la Seguridad de la Información) definido por ISO 27001 como: "En preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización",[29] aunque en muchas organización y entidades no se tiene implementado un SGSI, el cual permite establecer políticas de seguridad y los diferentes procedimientos para tener el menor riesgo posible de las amenazas a las que están expuestas, así como garantizar la continuidad del negocio, si se puede implementar diversas metodologías en el análisis de riesgos, entre las que más sobre salen son: **Magerit, Octave, Mehari, NIST SP 800 – 30, así como la gestión del riesgo ISO 31000, ISO 27005, OHSAS 18001, COSO.**

[29] Iso27000.es ¿Qué es un SGSI? [En línea] 2005 1 p. Disponible en http://www.iso27000.es/sgsi.html

- **Magerit:** "Es la metodología de análisis y gestión de riesgos de la información desarrollada por el Consejo Superior de Administración Electrónica",[30] está enfocada a las organizaciones grandes, ya sean comerciales o no, su análisis es cuantitativo y cualitativo, permite el hallazgo, la planificación de medidas oportunas, logrando la mitigación de los riesgos existentes en los sistemas de información, se centra en sensibilizar sobre los riesgos que existen y la importancia de contener estos a tiempo, es de libre uso, entre sus desventajas se encuentra que es costosa su aplicación.

- **Octave:** Esta metodología está enfocada en organizaciones públicas y privadas, sin tener en cuenta su tamaño, busca los riesgos en las organizaciones e involucra a todo el personal de la organización, permite identificar la infraestructura y sus vulnerabilidades, es de uso gratuito, entre sus desventajas esta que requiere amplios conocimientos técnicos.

- **NIST SP 800-30:** Este método está dedicado al análisis y la gestión de riesgos de la seguridad de la información, utilizada por organizaciones gubernamentales y no gubernamentales, se enfoca en la evaluación de riesgos de seguridad en la infraestructura de TI, en las que también se encuentra las persona que apoyan y utilizan el sistema de información en busca Vulnerabilidades tanto en Hardware, Software y el personal.

- **Mehari:** Enfocado en grandes y medias empresas que son sin ánimo de lucro, al igual que las que son de servicios públicos, sin excluir a organizaciones de índole privado, siendo un método en la evaluación de riesgos, bajo las normas ISO/TEC 27005:2008, utiliza el análisis de manera

[30] Ccn-cert MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de InformaciónLibro I - Método[En línea] Ministerio de Hacienda y Administraciones Públicas Gobierno de España. 2019. 127 p. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

cuantitativo como cualitativo, posea una base de datos con manuales y guías que permiten el análisis de los riesgos.

- **ISO 31000:** Permite la administración proactiva libre de riesgo, también aumenta la probabilidad del cumplimiento de los objetivos y mejora el aprendizaje organizacional.
  Convierte los riesgos positivos en oportunidades y permite identificar los riesgos que son una amenaza.
  Aumenta la seguridad y confianza lo que permite la prevención de pérdidas
  Permite mejorar la información financiera, los controles, la capacidad de recuperación organizacional, así como la prevención de las pérdidas y una mejor administración de incidentes, mejorando la eficacia y su eficiencia operativa, así como la seguridad, la protección del medio ambiente y la salud.
  Tiene presente tanto los factores humanos como culturales.
  Es dinámica, iterativa y susceptible al cambio.[31]

- **ISO 27005:** No tiene herramientas, técnicas, ni comparativas de apoyo para la implementación, además funciona como complemento de la norma ISO 27001 E ISO 27002.

  Una de las ventajas es que es un estándar internacional, la cual está orientada a la revisión y monitorización de riesgos, también para un análisis de la gestión de los riesgos su alcance es completo, finalmente permite un análisis cuantitativo.

- **OHSAS 18001:** Estable los requisitos básicos para efectuar un análisis que posibilita la identificación de los riesgos, los peligros y la su estimación, también permite realizar una valoración de los mismo que permiten razón si son tolerables o no y cuales atacar desde su origen.

- **COSO** Proporciona un marco de referencia para las empresas u organización donde involucra a todos los empleados.

[31] GONZALEZ, Hugo. GESTION DEL RIESGO – ISO 31000 [En línea] 2016. 1 p. Disponible en https://calidadgestion.wordpress.com/2016/10/28/gestion-del-riesgo-iso-31000/

“Posibilita respuestas más rápida y mejor a los cambios diferentes cambios del entorno, a los mercados y a las partes involucradas.

Permite alcanzar un conocimiento completo de los riesgos de la organización. Las probabilidades de éxito en la implementación de la estrategia son mayores a otras y la toma de decisiones son más seguros con un mejor proceso.”[32]

De acuerdo con el artículo de metodología para el análisis de riesgos en los SGSI realizado por Helena Alemán Novoa y Claudia Rodríguez Barrera donde se abordan las diferentes metodologías que trabajan el riesgo realizan un análisis sobre estos y destacan una tabla comparativa de sus respectivas ventajas y desventajas que cada una de estas tienen, así mismo se puede observar en la siguiente tabla del análisis realizado por Novoa y Rodríguez.

**Tabla 5 Ventajas y desventajas de las metodologías de análisis de riesgos**

| METODOLOGÍA | ÁMBITO DE APLICACIÓN | VENTAJAS | DESVENTAJAS |
|---|---|---|---|
| **OCTAVE** | Pequeñas y medianas empresa, públicas y privadas. | Permite que lo desarrollen los integrantes de la organización donde se puede conformar un grupo multidisciplinario.<br>Involucra a todos los integrantes de la organización.<br>Permite la identificación de perfiles de amenazas basado en los activos.<br>Proporciona la identificación de las vulnerabilidades asociadas a la infraestructura.<br>Desarrolla estrategias y planes para la seguridad.<br>Implica los procesos, activos, dependencias, recursos, amenazas, vulnerabilidades, y salvaguardas.<br>Permite la asociación de amenazas y vulnerabilidades.<br>Es gratuito solo para uso interno. | No tiene en cuenta el principio de no repudio de la información.<br>Usa demasiados documentos en el proceso de análisis de riesgos.<br>Necesita de amplios conocimientos técnicos.<br>No define claramente los activos de información.<br>Para uso externo se tiene que comprar una licencia. |

Tabla 5 (Continuación)

[32] Isotools. COSO como metodología de gestión de riesgo [En línea] Isotools 2015 1p. Disponible en ttps://www.isotools.org/2015/01/12/iso-90012015-coso-como-metodologia-gestion-riesgo/

| | | | |
|---|---|---|---|
| **MAGERIT** | **Gobiernos, compañías grandes comerciales o no, Pequeñas y medianas empresas.** | **En el análisis y gestión del riesgo tiene un alcance completo. Está metodología se encuentra bien documentada en recursos de información, amenazas y tipos de activos. Utiliza un análisis de riesgo cuantitativo y cualitativo muy completo. Su licencia para su uso es libre. En su proceso divide los activos en diferentes grupos, lo que permite identificar más riesgos y lograr tomar contramedidas para evitar los diferentes riesgos. Se centra en tres objetivos: Concientizar, ofrecer y planificar las medidas oportunas para mantener los riesgos bajo control. Permite preparar a una organización en los procesos como de auditoría, evaluación, certificación o acreditación. manteniendo el proceso en todo momento bajo control, contemplando aspectos prácticos para la realización del análisis y gestión de riesgos.** | **Este modelo no contempla los procesos, recursos, ni sus vulnerabilidades. Posee deficiencias en el inventario de políticas. Es considerada una metodología costosa para su implementación.** |
| **NIST SP 800 – 30** | Organizaciones gubernamentales y no gubernamentales. | A través de la guía que tiene permite valorar los riesgos de la seguridad de la infraestructura TI. Presenta un resumen de los elementos clave de las pruebas de seguridad técnica y la evaluación con énfasis en técnicas específicas, sus beneficios, limitaciones y recomendaciones para su uso. Tiene una guía que permite a través de herramientas la valoración y mitigación de los riesgos. Permite que los sistemas informáticos que almacenan, procesan y transmiten información sean seguros. Permite el mejoramiento de la administración partiendo de los resultados del análisis de los riesgos. Se aplica para el análisis y la gestión de los riesgos. | Este modelo no contempla elementos como los procesos ni tampoco activos y las dependencias. |

Tabla 5 (Continuación)

| | | | |
|---|---|---|---|
| **CORAS** | | **Tiene diversidad de herramientas de apoyo para el desarrollo del análisis de los riesgos, provee un editor gráfico basado en UML y soportar la elaboración de los modelos realizados en Microsoft Visio.**<br>**Tiene un repositorio con paquetes de experiencias que se pueden reutilizar.**<br>**Permite obtener un reporte de las vulnerabilidades encontradas.**<br>**De gran utilidad para el desarrollo y correspondiente mantenimiento en los nuevos sistemas.** | **No realiza un análisis de riesgos cuantitativo.**<br>**Este modelo no contempla elementos como son los procesos y las dependencias.** |
| **CRAMM** | Organizaciones públicas y privadas. | Conlleva un análisis de riesgos tanto cualitativo como cuantitativo.<br>Se puede aplicar en cualquier tipo de organización, se puede utilizar en todas las etapas del ciclo de vida del sistema de información, por medio del desarrollo e implementación del mismo.<br>Logra identificar y evaluar las amenazas y las vulnerabilidades a niveles de riesgos identificando los controles que se necesitan.<br>Conformada por más de 4.000 contramedidas reunidas en grupos y subgrupos con los mismos aspectos de seguridad, incluyendo activos de, hardware, software y protecciones medioambientales. | Este modelo no contempla elementos como los procesos o los recursos. |
| **EBIOS** | Enfocada en el sector público principalmente los Ministerios, y el sector privado. | Es utilizado por las diferentes organizaciones para obtener un mejor reconocimiento en las actividades de seguridad debido a que tiene un buen entendimiento con las normas internaciones entre ella la ISO dando cumplimiento a estándares como ISO 27001, ISO 27005 Y ISO 31000.<br>Es utilizada en con diversidad de finalidades y procedimientos de seguridad. una ventaja es que de código libre.<br>Esta herramienta involucra a las diferentes partes de la organización como directivas, empleados y usuarios.<br>Tiene una base de conocimiento que describe tipos de entidades, métodos de ataque, vulnerabilidades, objetivos y requerimientos de seguridad. | Se usa más como herramienta de soporte. |

Fuente: Alemán, Helena, Rodríguez Claudia Metodologías Para el Análisis de Riesgos en los SGSI [En línea] 2015. 14 p [Consultado: 11 de octubre de 2019] Disponible http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1754

Varias de estas metodologías tienen la ventaja que se pueden implementar a la vez, complementándose y permitiendo subsanar desventajas de una con las ventajas de la otra, dependiendo del tipo de organización en la que se quiere implementar un tipo de SGSI eficiente con todas las condiciones, es decir, el de contar con personal, tiempo, presupuesto y sobre todo compromiso de las directivas, gerentes o funcionarios de alto rango.

### 5.1.2 Marcos de gestión del riesgo.

Como todo propósito de la gestión del riesgo el marco busca ayudar a las organizaciones a gestionar los riesgos que se pueden presentar en los diferentes procesos que se desarrollan en ellas, uno de estas son las actividades derivadas del factor humano.

- **COBIT:** Es un marco de gestión de buena práctica para el control de la información, el cual proporciona herramientas que ayudan a desarrollar, organizar e implementar estrategias para la información y la gobernanza, se utiliza para implementar un gobierno de TI.
  Un ejemplo de la aplicabilidad de este marco es la búsqueda de factores relacionados al componente del talento humano un ejemplo de esto es:

  **Amenaza:** Ingeniería social.

  **Vulnerabilidad:** Falta de conocimiento del personal que permita mitigar este tipo de método de intrusión, como la falta de programas de capacitación para ello.

  ***Riesgo:*** Perdida de información clasificada.

Lo que permite la identificación de todos los factores que generan un riesgo determinando, cuáles pueden ser tolerados y cuáles deben ser mitigados o eliminados.

Una de las desventajas de este marco es que requiere de grandes esfuerzos para la organización, para llevar a término la adopción de los estándares.

- **ITIL:** Es un marco enfocado en la administración de servicios de tecnología de la información, la cual ayuda a tener una mejor eficiencia y calidad en los servicios. A través de un conjunto de buenas prácticas, el cual se base en un ciclo de vida del servicio.

  Algunas de sus desventajas son que requiere de compromiso del personal, es esencial este factor, al igual que Cobit requiere de tiempo y compromiso para la implementación y sobre todo requiere de inversión.

  Este marco se implementa cuando se quiere mejorar la calidad de los servicios, enfocándose en mejorar la calidad al cliente cumpliendo todas las expectativas, cuando se tiene una falta de control y monitorización en los procesos y con una mala gestión de proyectos TI.

Todo esto va de la mano con los compromisos que adopten las organizaciones o entidades, ya que las aplicaciones de estos permiten sentar las bases para una gestión eficaz de los riesgos que se encuentran en estas, no solo en infraestructura sino a hechos como son la corrupción, un factor atribuible a las cualidades y cultura de las personas.

Por otro lado, existen metodologías enfocadas en el Software, en su creación, al igual que para su mantenimiento, esto a través de auditorías como es el caso de OWASP (Open Web Application Security Project) la cual ratifica que un sistema nunca es 100% seguro, que las amenazas nunca se pueden eliminar al 100% pero

si se pueden reducir su amenaza, esta metodología busca encontrar y eliminar las causas que hacen inseguro un Software.

Dicho brevemente, esta metodología está dedicada para desarrolladores de Software a los cuales les permite asegurarse que el código diseñado no sea vulnerable a ataques, enfocada para los testers de software y especialistas de seguridad informática, ya que puede identificar las vulnerabilidades que están presentes en los sistemas, donde aplicara el estándar de seguridad en aplicaciones de OWASP, lo que se enfoca al Software por lo que esta metodología no es viable para la búsqueda de vulnerabilidades en el factor humano directamente ya que permite encontrar fallos atribuidos a ellos, pero si una entidad llega a producir software debería aplicarla.

De todo lo anterior no existe una metodología que este enfocada exclusivamente en el factor humano como su riesgo principal, en casi todas las metodologías y marcos de gestión del riesgo el factor humano es uno, al no contar con tiempo, recursos u otros factores que impidan la implementación de alguno de los mencionados u otro existen herramientas que se pueden aplicar para minimizar riesgos como son las Guía de buenas prácticas para la seguridad de la información, así como las diferentes guías que aporta el MinTic.

### 5.1.3 Aplicaciones controles ISO 27001 que disminuyan el riesgo asociados al personal de las entidades.

El MinTic busca que las entidades tengan un SGSI basado en la norma NTC/ISO 27001, el cual brinda las pautas para lograr la implementación de sistemas de calidad en los diferentes niveles que la componen, para el ministerio en sus herramientas de control está norma, al igual que la ISO/IEC 27002 basado en (14) catorce dominios principales con sus controles más especificados en su aplicabilidad, esto están en aplicación dentro de las entidades del gobierno como

se puede corroborar en: “ La guía N° 8 Controles de Seguridad y Privacidad de la Información”.[33] Siendo esta para la implementación de dichos controles dentro de las entidades, pero no solo está presente en la guía sino en su instrumento de evaluación del MSPI la cual es: ”Una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas”.[34] Al igual que se contempla en dos políticas del Modelo Integrado de Planeación y Gestión como son Gobierno Digital y Seguridad Digital que conllevan a la aplicabilidad de estos controles.

En resumen, se pueden evidenciar todos los controles que se deben implementar en las entidades y que según el ministerio deberían existir, por lo que la aplicabilidad de estos es una regla de oro dentro de las entidades, que permitan cumplir con el objetivo de ser seguras o garantizar un mínimo de ello, no solo desde el factor humano sino todo lo que puede comprometer la información, razón por la cual se debe implementar el instrumento MSPI aportado por el MinTic, el cual es fundamental para saber cómo está la seguridad de la información en la actualidad, como también proyectar algunas estrategias a corto mediano y largo plazo.

Lo anterior, con el propósito de ser integrado en los diferentes planes que da el MinTic para su implementación, con miras a ser un estado inteligente y seguro, si esta norma estuviera implementada en las entidades no se encontrarían falencias como las que se evidenciaron en la recolección de información, por tanto, se debería aplicar dichos controles en este tipo de entidades con asesoramiento de expertos que ayuden en dicho proceso ante la falta de personal especializado o con conocimientos para su aplicabilidad.

[33]República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. Modelo de Seguridad [En línea]. Bogotá: 2016. 1 p. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf
[34]Ibíd. P 1.

## 5.2 ANÁLISIS DEL GRADO DE CONOCIMIENTO DE LOS EMPLEADOS SOBRE LA SEGURIDAD DE LA INFORMACIÓN.

Para realizar el análisis del conocimiento de los empleados en las entidades de categoría 6, se seleccionaron las alcaldías municipales de Toledo y Labateca del departamento de Norte de Santander, se realiza a través del instrumento de recolección de información siendo este una encuesta, enfocada en determinar cuál es el conocimiento de los empleados en temas de seguridad de la información y cómo puede ser un riesgo para ellas.

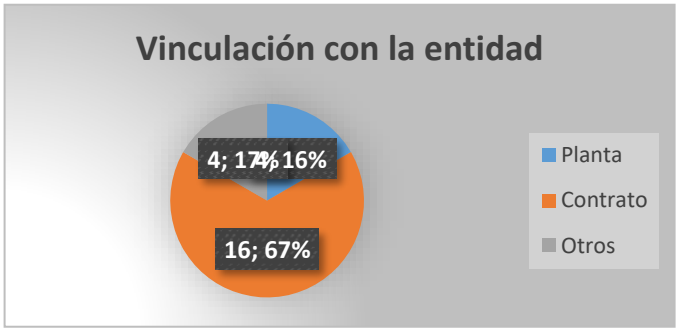
Se realizaron en total 24 encuestas, de dos tipos, en primer lugar la encuesta llamada tipo 1, enfocada en el personal que no es de libre nombramiento, sin tener en cuenta el tipo de vinculación que tienen con la entidad los cuales pueden ser de planta, orden de prestación de servicios (OPS) u otro, los cuales tienen en su trabajo, funciones que requieren del uso de dispositivos tecnológicos e interactuar con la información de las entidades, la encuesta consta de 22 preguntas que permiten identificar también el **riesgo de la seguridad de la información asociados al factor humano.**

La encuesta 2 llamada de tipo 2, esta enfocadas en los altos cargos de las entidades como son los secretarios de despachos , quienes deberían tener un grado mayor de conocimiento que un empleado promedio en cuestiones de seguridad, debido a la información que estos manejan, como son el caso de secretaria de hacienda y asuntos fiscales o nombres que varían según la entidad pero cumplen las mismas funciones, ya que en ella recae la responsabilidad de los equipos que tienen la información más relevante en cuanto al aspecto económico.

Un dato de suma importancia de la información recolectada y que es conocer el tipo de vinculación con las entidades de las 24 personas encuestadas, entre los dos tipos de encuestas formuladas, en la siguiente Figura se puede evidenciar la

información recolectada.

*Figura 1 Tipo de Vinculación*




Fuente: Autoría propia.

De la anterior figura se puede decir que de planta solo existen 4 personas correspondiente al 16% lo que indica que se puede tener un gran problema no solo asociado a la ciberseguridad sino a muchos más temas, por eso, es importante traer a discusión el análisis realizado por Performia Colombia en el año 2016, el cual afirma que la rotación de personal puede ocasionar que: "las perdidas en las empresas sean como mínimo $1.155.687 pesos mensuales por la mala contratación"[35], pero este no es el mayor problema, sino cuando se invierte por parte de las organizaciones en capacitar empleados, que al no ser de planta y más en el caso de este tipo de entidad que se está analizando, por lo general un contrato podría duras hasta un máximo 4 años, que es el tiempo del periodo de un alcalde y su equipo de trabajo, por lo que las capacitaciones que se realizan a empleados a corto o mediano plazo terminan perdiéndose, ya que estos dejan sus cargos y funciones sin trasmitir el conocimiento a sus sucesores.

De lo anterior es una posibilidad que conlleva a realizar nuevas capacitaciones para suplir las necesidades o falencias debido a estos cambios, al igual genera menor productividad en los tiempos de empalme a los nuevos empleados en sus

[35] Performia Colombia. La rotación de personal perjudica significativamente a las empresas [En línea] 2016 1 p. Disponible en http://www.performia.com.co/la-rotacion-de-personal-perjudica-significativamente-a-las-empresas/

respectivos cargos, esto no solo pasa en las entidades públicas sino en cualquier organización.

Según el DANE en la presentación del boletín sobre Formación para el trabajo, donde las cifras queda son: “Sobre el total nación, correspondiente del trimestre de abril a junio de 2015 hubo 34,3 millones de personas mayores de 15 años, de las cuales el 9,7% asistió a cursos de formación para el trabajo”,[36] es decir que de los que se capacitan según su tipo de posición en el mercado son “para el trimestre comprendido entre abril y junio del año 2015, correspondiendo a un 13,0% de los desocupados, de los ocupados un 12,5% y de la población considerada inactiva un 3,2%, asistieron al cursos de formación para el trabajo, Asimismo, destaca que en el mismo período del año anterior, asistieron el 12,9% de los desocupados, el 12,4% de los ocupados y el 3,1% de los inactivos”,[37] lo que indica una inversión de tiempo y dinero por parte de las entidades, que a corto y mediano plazo puede que no les sea de utilidad dependiendo de los cargos y capacitaciones recibidas.

### 5.2.1 Resultado de la recolección de información de la encuesta tipo 1.

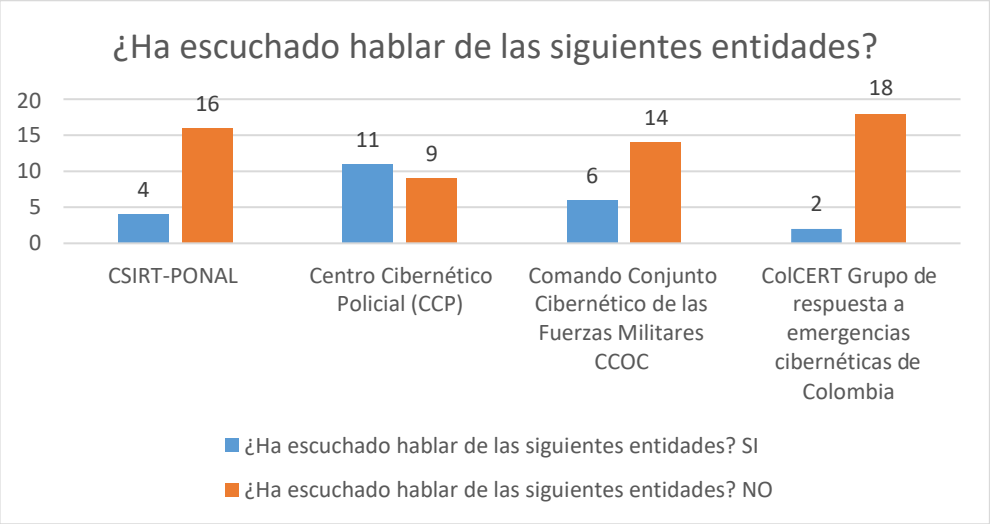
Las preguntas realizadas con los datos obtenidos y lo que representa dicha información esta desglosada pregunta por pregunta:

[36]Departamento Administrativo Nacional de Estadística. Boletín técnico FORMACIÓN PARA EL TRABAJ O[En línea]. 2016. 21 p. Disponible en https://www.dane.gov.co/files/investigaciones/boletines/ech/formacion/GEIH_FormacionTrabajo_abr_jun15.pdf

[37]Ibíd p. 8.

✓ **¿Ha escuchado hablar de las siguientes entidades?**

Figura 2 Han escuchado hablar de los organismos de ciberseguridad.

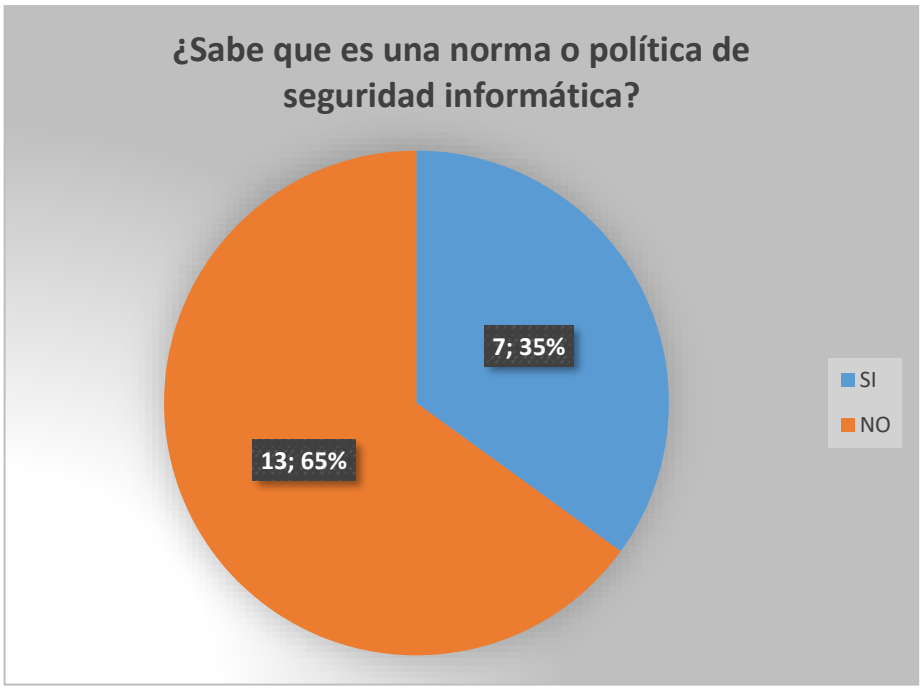



Fuente: Autoría propia.

Los resultados que se evidencian de la primera pregunta es que los empleados de las entidades en su gran mayoría desconocen los organismos que se encargan y ayudan al estado en la ciberseguridad, exceptuando al Centro Cibernético Policial (CCP), donde la mayoría responde que si lo conoce, siendo solo un poco más de la mitad de los encuestados con el 55%, lo que significa que el no conocer estos organismos en su mayoría demuestra el grado de desconocimiento que tienen, lo que puede hacer más segura la ciberseguridad en estas entidades, desconocen que por ejemplo en la página de CSIRT-PONAL tiene una herramienta de gran utilidad como es sandbox que les permite analizar un archivo o una URL y saber si estos se encuentran infectados o no son legítimos, la cual puede ser de una gran utilidad en la prevención ante cualquier sospecha de archivo o página que se crea que no es la legitima lo que evitara una infección.

✓ **¿Sabe que es una norma o política de *seguridad informática?***

Figura 3 Conocen que es una norma o política de seguridad informática

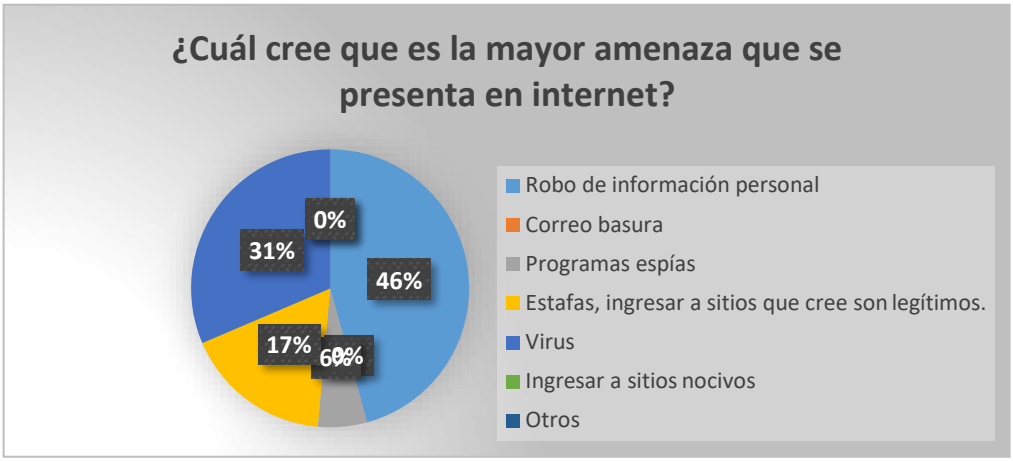



Fuente: Autoría propia.

Con el desarrollo de esta pregunta se conoce si las normas o políticas de la seguridad informática son conocidas por parte de los integrantes de las entidades, también permite saber el grado de conocimiento de ellos con respecto al tema, del resultado se puede ver que la mayoría no saben, indicando que existe una vulnerabilidad en esto ya sea por la falta de ellas o por la no socialización.

✓ **¿Cuál cree que es la mayor amenaza que se presenta en internet?**

Figura 4 Cuál cree que es la mayor amenaza de internet.

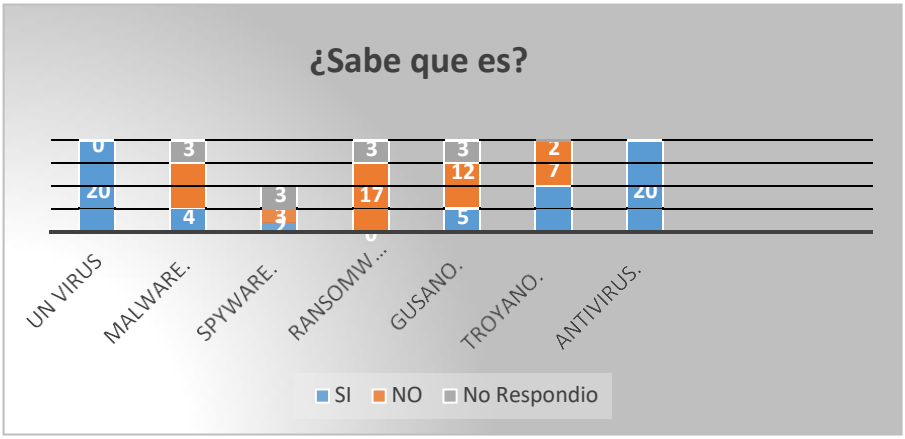



Fuente: Autoría propia.

El análisis de esta pregunta permite entender que la gran mayoría de personas ven con preocupación la perdida de información, principalmente la de índole personal, a pesar que la encuesta va dirigida al ámbito laboral esto se detona también con la pregunta 10 de esta encuesta, realizada que es la navegación en redes sociales por eso también la preocupación es la perdida de información, siendo una preocupación para ellos los virus y las estafas por internet, lo que puede ser un punto de partida para el desarrollo de estrategias para mitigar los riesgos debido a estos factores.

✓ **¿Sabe que es?**

Figura 5 Conocen a la amenaza que considera más peligrosa.




Fuente: Autoría propia.

Esta pregunta permite conocer ya específicamente que conocimientos puntuales tienen los empleados sobre las diferentes amenazas que existen, preguntando por alguna de ellas tal y como se evidencia en la figura 5.

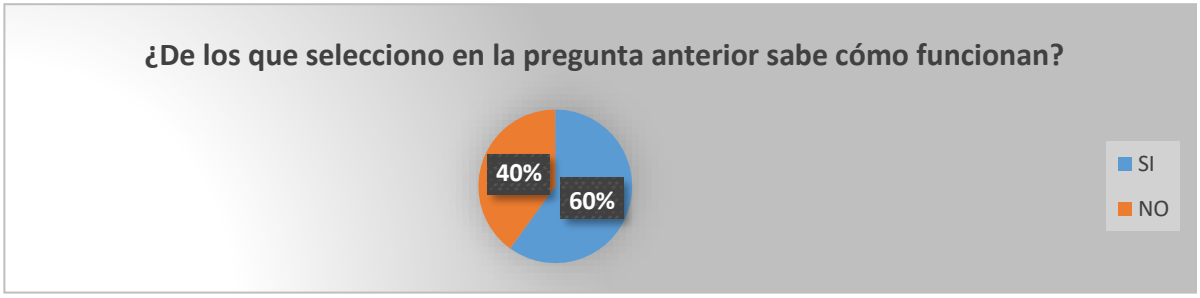
Se pudo determinar que los empleados saben qué es un virus y un antivirus, lo preocupante es con RANSOMWARE, MALWARE sobre todo el primero que según el reporte de Eset Security Report atinoamérica del año 2018 "las preocupaciones de las empresas es de 57%",[38] lo que se constituye como la primera preocupación y más cuando existió un incremento de este tipo de ataque en “más de un 60% en no más de un año, donde en el último en américa latina un 40% de las empresas sufrió una infección con malware".[39] y específicamente en Colombia las infecciones por este tipo "tiene un índice de 19%",[40] donde se vio afectada por el tan famoso ransomware WannaCry el cual fue noticia mundial, por lo que es de suma importancia que las personas conozcan cómo funciona este tipo de amenaza y

[38] Eset , Eset security report latinoamérica [En línea]. 2018. 16 p. Disponible en https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf
[39] Ibíd. p. 4.
[40] Ibíd. p. 6.

sobre todo comprendan cómo proceder ante un incidente como este y en caso de ocurrir ocasione el menor daño posible.

- ✓ **¿De los que selecciono en la pregunta anterior sabe cómo funcionan?**

Figura 6 Conocen cómo funciona las amenazas que conoce.

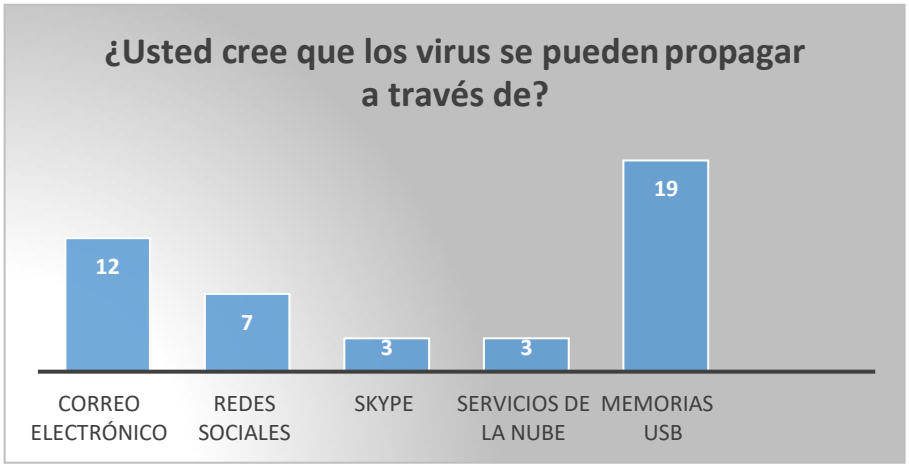



Fuente: Autoría propia.

Esta pregunta va en relación con la anterior ya que busca determinar si las personas encuestadas saben cómo funciona las diferentes amenazas, de acuerdo a esto se puedo evidenciar que el 60% de las personas no lo saben, para el caso de los antivirus saben que protege, pero no como funciona y como lo hace, lo que representa un riesgo al no entender cosas importantes como que si no se está actualizando por ejemplo el antivirus puede ser un riesgo para el equipo y el sistema al que pertenece.

✓ **¿Usted cree que los virus se pueden propagar a través de?**

Figura 7 Conoce como se propagan los virus.




Fuente: Autoría propia.

El saber por qué medios se puede propagar un virus es importante, es de aclarar que se utilizó este término globalizando todas las amenazas porque es el más común para las personas y permite identificar porque medios cree los encuestados que se propagan las infecciones.

Los resultados lo que refleja es que para la mayoría creen que es a través de memorias USB por donde llegan las infecciones, muy pocas personas creen a través de redes sociales se pueden infectar, de este desconocimiento es que los ciberdelincuentes se aprovechan para lograr sus objetivos como es la inyección de ransomware u otras infecciones, valiéndose de los correos electrónicos o mensajes por redes sociales con enlaces que llevan a sitios que permitirán vulnerar los sistemas, en este ámbito recobra importancia la ingeniería social la cual se aprovecha de las personas que por su falta de conocimiento permitan el acceso a los sistemas o aplicaciones de manera fraudulenta.

- ✓ **¿Sabe que es una contraseña fuerte?**

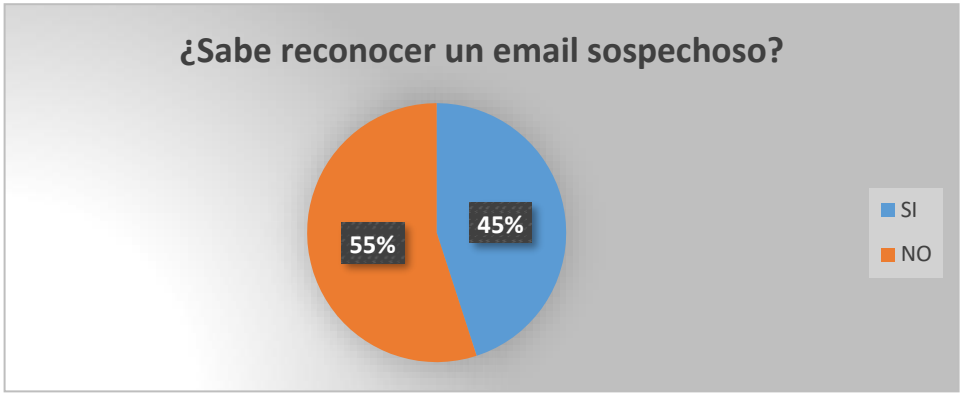
Figura 8 Conoce que es una contraseña fuerte


Fuente: Autoría propia.

Hoy en día la importancia de una contraseña fuerte es fundamental por la encriptación que con lleva estas, si se tiene una débil, la encriptación puede ser menor y puede ser rota de manera rápida, claro que esto depende también del tipo de encriptación que utilice en los sistemas, pero el problema real no es este, sino la ingeniería social que es la que más explota esta vulnerabilidad, más cuando las personas utilizan contraseñas que son fáciles de recordar y que tienden a tener datos de fácil acceso como por ejemplo fechas de nacimientos, nombres de seres queridos, pero la gente no comprende que puede realizar contraseñas fuertes con datos de fácil recordación pero que no están al alcance de los ciberdelincuentes que los consiguen a través de la técnica de ingeniería social, los resultados derivados de esta pregunta permiten observar que el 60% de los encuestados, no sabe qué es una contraseña fuerte, lo cual es preocupante y un riesgo de seguridad, ya que de estas contraseñas depende el ingreso a los diferentes usuarios que manejan en las entidades como correos corporativos, aplicaciones oficiales entre otros.

- ✓ **¿Sabe reconocer un email sospechoso?**

Figura 9 Conocen cuando un email es sospechoso.




Fuente: Autoría propia.

La propagación de phishing, malwares, ransomware, entre otros, utilizando comúnmente los archivos adjuntos o enlaces en los correos electrónicos, que el usuario abre muchas veces por desconocimiento de esto o por la simple curiosidad, sin conocer que a través de ingeniería social se puede realizar ataques específicos con diferentes modalidades, que dan mayor garantía que el usuario victima abrirá dicho archivo o enlace.

Como se describió anteriormente, el uso de correo legítimos en algunos casos específicos permite la infección, pero en muchos casos son correos similares a los reales, cambiándoles los dominios, por eso identificar algunos aspectos básicos en un correo es importante, para reducir los riesgos y prevenir la infección de amenazas serias como los ransomware que están aumentando cada día.

Esta pregunta permitió determinar que se debe que capacitar al personal en seguridad informática enfatizando en los riesgos en internet, ya que el 55% no sabe cómo identificar un correo sospechoso, esto se puede lograr a través de charlas o de instructivos que les permitan tener claro cómo identificar aspectos en un correo, que les genere dudas y tengan en cuenta los pasos a seguir, como también analizar obligatoriamente los archivos descargados.

- ✓ **¿Sabe identificar cuando una dirección URL es legítima?**

Figura 10 Identifican cuando una URL es legítima.


Fuente: Autoría propia.

Hoy en día con la clonación de sitios para realizar estafas o la propagación de códigos maliciosos es importante identificar los sitios reales de los falsos, es por eso que un empleado debe tener claro a donde está ingresando y más con la difusión de enlaces por correo electrónico, la anterior pregunta es el primer paso, ya que permite saber si están preparados o no, es importante debido a que si se presenta un caso donde las páginas son similares o idénticas a las originales y se tiene dudas se debería usar herramientas para su análisis, como la aportada por el CSIRT-PONAL para el análisis de URL, que para el caso de análisis de estas entidades se debería realizar más cuando el 85% de los encuestados no sabe cuándo un dirección URL es legítima, el mayor problema radica cuando estos desconocen que existen este tipo de herramientas.

- ✓ **¿Cada cuánto cambia las contraseñas de sus correos electrónicos o de los diferentes usuarios que tiene en redes sociales y otras plataformas.?**

*Figura 11 Tiempos de cambio de contraseñas.*

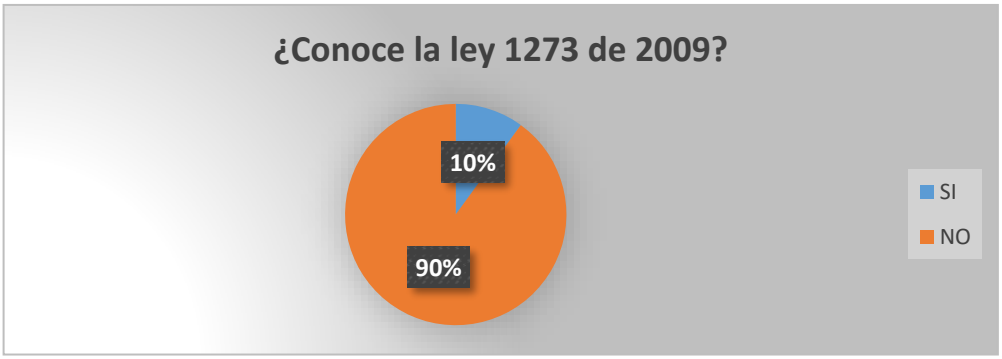

Fuente: Autoría propia.

Uno de los factores a tener en cuenta en la seguridad de las aplicaciones es el tiempo que se debe estar cambiando las contraseñas, como cada persona determina cuando cambia sus aplicaciones este tipo de pregunta fue de estilo abierta para recoger los datos que se consignaron en la figura 11 de los cuales, 16 mostrando unos patrones en sus respuestas siendo preocupante el 25% el nunca cambia sus contraseñas, lo que es un riesgo más si estos usan las mismas contraseñas en las diferentes aplicaciones para un fácil recordatorio, al igual el 15% que las cambia cada año, lo cual es un término de tiempo demasiado largo donde se puede ver expuesto alguna filtración como por ejemplo: “Los cerca de 773 millones de direcciones de correo únicas y más de 21.2 millones de contraseñas únicas las que fueron publicados de manera masiva en lo que se ha denominado

“Collection #1””,[41] esto indica que en cualquier momento una aplicación puede exponer una cuenta con su respectiva contraseña y siendo usadas estos datos en diferentes aplicaciones, plataformas o sistemas, terminan quedando expuestos, es la importancia de cambiar la contraseña como lo realiza aproximadamente el 35% de las personas encuestadas.

- ✓ **¿Conoce la ley 1273 de 2009?**

Figura 12 Conocimiento de la ley 1273 de 2009.




Fuente: Autoría propia.

Conocer el marco legal sobre el cual se trabaja es importante, pero más aún las responsabilidades que implica los hechos en los que uno pueda incurrir, por eso la mejor seguridad es la prevención y el conocerlo, saber que rige la protección de los datos y de la información representa una medida de protección, no solo para las empresas, sino para cualquier persona en Colombia, sobre todo lo relacionado con el ítem especial presente en esta ley, que hace referencia a los empleados públicos, que les aumentan las penas por su condición, ya que debería ser deber de ellos conocer la legislación que los cobija.

[41] TOMÁŠ, Foltýn. 773 millones de direcciones de correo y 21 millones de contraseñas fueron filtradas [En línea]. 2019. 1. p.Disponible en https://www.welivesecurity.com/la-es/2019/01/17/millones-direcciones-correo-contrasenas-filtradas/

Esta pregunta busca saber si se conoce esta ley que es de hace 12 años, entre los resultados se encontró que solo el 10% la conoce un porcentaje demasiado bajo, razón por la cual se debería implementar un manual que les permita entender de qué se trata esta ley y las que la puedan modificar o se llegaran a crear en remplazo de esta que no cubre todos los delitos que se cometen en la actualidad.

### 5.2.2 Resultado de la recolección de información de la encuesta tipo 2.

Esta encuesta está enfocada en los secretarios de despacho quienes son lo que tienen a cargo los empleados, por lo tanto, deben tener un mayor grado de responsabilidad con sus funciones y con la seguridad de la información en los diferentes despachos, la encuesta fue estructurada en 18 preguntas que buscan saber el grado de conocimiento de ellos quienes tienen las mayores responsabilidades dentro de la entidad.

- ✓ **¿Sabe que es un SGSI?**

Figura 13 Conoce que es un SGSI


Fuente: Autoría propia.

El conocer que es un SGSI por parte de un empleado "permite obtener una visión global del estado de los sistemas de información, para poder con todos estos elementos tomar mejores decisiones estratégicas"[42] y el entender su importancia

[42]PACHECO, Federico. La importancia de un SGSI[En línea]. 2010. 1 p. Disponible en https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

puede llevar a que ante una implementación no se vea como una carga sino como un beneficio, aunque la dificulta en este aspecto o proceso con las entidades radica con la rotación de los cargos y empleados que existe en ellas por su naturaleza.

De los resultados se deduce que la mitad de los encuestados tienen claro la importancia de un SGSI y lo que puede llegar aportar en una entidad, el mayor inconveniente para la implementación en este caso específico es que no existe el personal encargado, y que si se le asigna funciones a personal que no tienen conocimiento en esta área puede que la implementación no obtenga los resultados requeridos, contratar a una empresa que asesore y permita la implementación puede no darse por los recursos que estas poseen, pero este dato permite entender que la implementación puede ser apoyada por empleados de la misma entidad.

- ✓ **¿Manejan un marco de buenas prácticas para la gestión de seguridad de la información?**

Figura 14 Conoce si tienen un marco de buenas prácticas

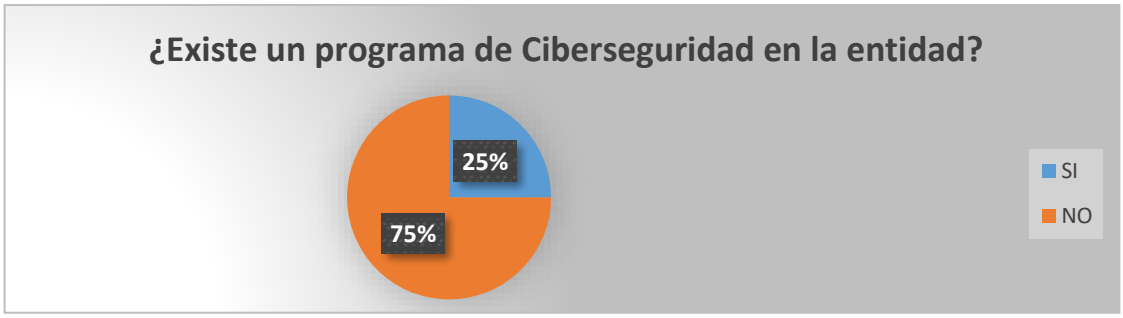

Fuente: Autoría propia.

La implementación de buenas prácticas independiente del proceso o el ámbito donde se aplica, mejora todos los procesos a favor de la entidad y de los empleados, que permiten tener una mejor productividad y efectividad, garantizando unos

estándares en dichas actividades, estos marcos permiten acercarse a un SGSI aunque estos también posibilitan la gestión de los riesgos, por lo que la implementación de estos en la empresas independientemente sino tienen mejoran los procesos que en esta existen, lo que se observa en la pregunta es que no se tienen ningún marco implementado por lo que es un ítem a mejorar en estas entidades.

- ✓ **¿Existe un programa de Ciberseguridad en la entidad?**

Figura 15 Conoce si existe un programa de ciberseguridad en la entidad.




Fuente: Autoría propia.

Esta pregunta va relacionada con otras preguntas analizadas, ya que de un programa de ciberseguridad se derivan otros, entendiendo que no se hace referencia a un software sino a una estrategia que debería estar implementada en las entidades para hacer frente a las diferentes amenazas que existen.

El 75 % dice que no existe un programa en la entidad, relacionando esto con otras respuestas en otras preguntas en la encuesta tipo 1 se determina que no existe un programa estructurado que permita enfrentar las diferentes amenazas que existen en el ciberespacio y en la parte física, esto el gobierno actual lo tiene muy claro, en especial cuando en el plan de desarrollo en el artículo **147** en el ítem 2 sugiere la "Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de

datos personales".[43] De modo que, se hace necesario formular estrategias que permitan lograr este objetivo del actual gobierno.

- ✓ **¿Existe un manual de responsabilidad en la entidad sobre los incidentes Informáticos que se puedan presentar?**

Figura 16 Existe un manual de responsabilidad por incidentes Informáticos.


Fuente: Autoría propia.

En los manuales de cada cargo debe existir aparte de sus deberes también sus responsabilidades, las cuales deben incluir la parte de la información y los equipos en los que estos intervienen en el sistema, deben estar claras para las partes tanto el empleado como las entidades y se contemplen todas las posibilidades, esto con el ánimo de darle compromiso a los empleados que conlleven a la protección de los equipos y de la información que reside en ellos, a su vez tengan claro las sanciones en las que puedan incurrir según sea los casos desde económicas hasta legales, todo esto contribuye a la prevención.

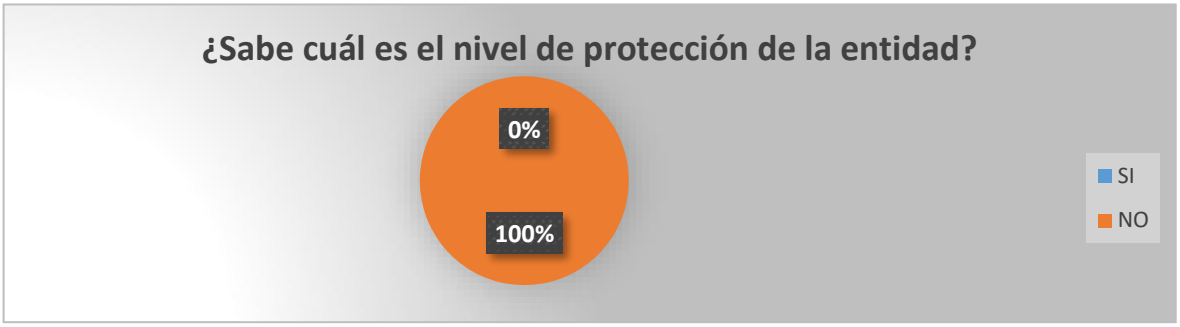
El resultado obtenido evidencia que existe un problema en las entidades, ya que no existe un manual para estos asuntos. Tal y como lo hace notar la Vicepresidencia de Innovación y Transformación Digital del Grupo Bancolombia dice: "8 de cada 10

[43] EL CONGRESO DE COLOMBIA, LEY 1955 DE 2019 (25 de mayo de 2019) . Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad". Congreso, art. 147.

de los ataques informáticos dentro de las compañías tienen origen en sus propios empleados. 60% de los errores en la privacidad de los datos de las compañías es ocasionado por los empleados Y el 46% de los ataques cibernéticos de las compañías en el mundo es realizado por exempleados",[44] queda así, una vez más confirmado que los empleados tienen mucho que ver en los incidentes, ya sea de manera premeditada o por simplemente desconocimiento, siendo esto último en la mayoría de las ocasiones permitiendo diferentes tipos de ataques de los cuales son responsables y debería existir en los manuales estas responsabilidades con las respectivas sanciones acordes a las situaciones.

- ✓ **¿Sabe cuál es el nivel de protección de la entidad?**

Figura 17 Conoce el nivel de protección de entidad.




Fuente: Autoría propia.

El saber cómo está el nivel de seguridad es el primer paso siempre que se quiere mejorar, el desconocer cómo esta una entidad en diferentes aspectos es un signo que indica que se debe tomar medidas a corto y mediano plazo que garanticen los objetivos, a la pregunta realizada los encuestados responden que no saben cuál es el nivel de la entidad y no solo en la parte de la seguridad informática, sino en otros aspectos como son los físicos lo que representa un riesgos para este tipo de

[44] Grupo Bancolombia. El eslabón suelto de la ciberseguridad: el empleado [En línea]. Grupo Bancolombia. 2018 2 p. Disponible en https://www.grupobancolombia.com/wps/portal/empresas/capital-inteligente/tendencias/innovacion/el-eslabon-suelto-ciberseguridad

entidades ya que el desconocimiento puede ser aprovechado para la explotación de vulnerabilidades.

- ✓ **¿Conoce la ley 1273 de 2009?**

Figura 18 Conoce la ley 1273 de 2009 en la encuesta tipo 2


Fuente: Autoría propia.

Esta pregunta formulada también en la encuesta tipo 1 se realiza para saber si los altos cargos de las entidades saben el marco legal específicamente la ley que rige la información y los datos en Colombia, la respuesta difiere de las respuestas a esta misma pregunta en la encuesta tipo 1 y es que todos la conocen, lo que significa que saben que puede ocurrí ante los diferentes hechos que se puedan llegar a presentar con los diferentes actores que intervienen en la información más como servidores públicos.

- ✓ **¿Existe en la entidad un inventario de activos de información en la entidad**?

Figura 19 Existe un inventario de activos de información en la entidad.


Fuente: Autoría propia.

La importancia de un inventario para una organización grande o pequeña es que representa un elemento para su desarrollo, así como de los controles que se implantan a partir de ello, eso mismo ocurre en los activos de información donde no solo ingresan la parte física sino también elementos importantes como el conocimiento como por ejemplo el que tienen los empleados que en muchos casos puede ser más importante que los activos físicos los cuales pueden ser remplazados, mientras el conocimiento no, el contar con un activo de información permite la formulación de estrategias que permitan protegerlos de los diferentes factores así como concentrar los recursos sobre los más importantes.

En este caso el 75% cree que existe un inventario de este tipo en la entidad lo cual es importante si se tiene bien desarrollado este inventario que permita la formulación de estrategias, políticas y controles en favor de la protección de la información.

- ✓ **¿Ha escuchado hablar de las siguientes entidades?**

Figura 20 Han escuchado hablar de los organismos de ciberseguridad.


Fuente: Autoría propia.

El conocer las entidades que en Colombia son las encargadas de la ciberseguridad y las que serán junto con el MinTic la encargadas de guiar a la consecución de lo planteado en los artículos 147 y 148 del Plan de Desarrollo del Periodo 2018 – 2022, el que se conozcan estos organismos, la información que estos producen en favor de la comunidad colombiana a través de herramientas e informes, los cuales permiten saber cómo está este tema en el país y en las entidades de tanto públicas como privadas, con lleva a la toma de decisiones para el mejoramiento de la seguridad en estas.

Esta pregunta fue formulada en la encuesta tipo 1 siendo el CCP el más conocido por los encuestados lo que representa algo positivo pero que a la vez evidencia la falta de estrategias, que permitan que el pueblo colombiano conozca la existencia de ellos y las funciones que cumplen al igual de cómo pueden ayudar.

De los dos tipos de encuestas realizadas indican que las políticas del gobierno nacional tienen mucho espacio para su mejoramiento uno de estos espacios lo contemplan en el plan de desarrollo 2018 al 2022 un artículo apunta a este sector

este "Artículo 147. Transformación Digital Pública. Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio TIC".[45]

Pero para que esto ocurra de manera efectiva, los empleados de las diferentes entidades deben tener capacidades para poder llevar acabo esto, ya que si estos no saben cómo distinguir un correo sospecho o cómo actuar ante un incidente, será una vulnerabilidad para un sistema cada día más interconectado dejando brechas de seguridad en un gran sistema como es el estado colombiano que requiere de compromiso de todos los que lo integran.

Por otra parte, el Plan Nacional de Desarrollo (PND) presenta también el artículo 148, el cual establece al "Gobierno Digital como Política de Gestión y Desempeño Institucional. que modifica el artículo 230 de la ley 1450 de 2011, allí se estipula que todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través del Ministerio TIC para la implementación de la política de Gobierno Digital".[46]

Es decir, formular estrategias que le permita llegar a este tipo de entidades de manera efectiva que no solo sea llevar los procesos y la información a la internet, sino que esto sea con la mayor seguridad del caso sin que estas pequeñas entidades puedan llegar a ser una vulnerabilidad en un sistema que tiende a estar interconectado, los cuales no poseen o pueden utilizar los recursos suficientes para establecer programas de seguridad informática y con difícil capacidad para la implementación de un SGSI.

[45] EL CONGRESO DE COLOMBIA, LEY 1955 DE 2019 Op. Cit art. 147.
[46] EL CONGRESO DE COLOMBIA, LEY 1955 DE 2019 Op. Cit art. 148

El organismo que debe guiar a las demás entidades y órganos del estado en proteger la información y ser congruente con los objetivos del PND es el Ministerio de Tecnologías de la Información y Comunicaciones que en su actuar tiene implementado un SGSI descrito en su Plan De Seguridad Y Privacidad De La Información Versión 1.0 que tiene por objetivo: "Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, en el Mapa de Procesos",[47] aunque está enfocado solo en la estructura de este ministerio se puede orientar a las demás entidades bajo la experiencia que se debe tener para la formulación de estrategias que permitan que las entidades públicas garantizar los tres pilares de la información.

Por consiguiente, debe buscar fortalecer el nivel de conocimiento, ya que, según las encuestas realizadas, es bajo por parte de los empleados y de nivel medio en los secretarios de despacho. Es así que el gobierno debe a través de los diferentes planes que desarrolla a través del Ministerio Tic y programas como vive digital que se mejora la capacidad de estos para que pasen de ser una vulnerabilidad a un activo de información importante.

[47] Ministerio de Tecnologías de la Información y las Comunicaciones. Despacho de la Ministra Seguridad y Privacidad de la Información. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Versión 1.0 [En línea]. Grupo Bancolombia. 2018 2 p. Disponible en https://www.mintic.gov.co/portal/604/articles-100251_plan_seguridad_privacidad_informacion_2019.pdf

## 5.3 IDENTIFICACIÓN DE LAS PRINCIPALES CAUSAS DEL FACTOR HUMANO COMO RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

### 5.3.1 Resultado de la recolección de información de la encuesta tipo 1.

- ✓ **¿Conoce de los controles implementando en la entidad sobre los diferentes procesos de la seguridad de la información?**

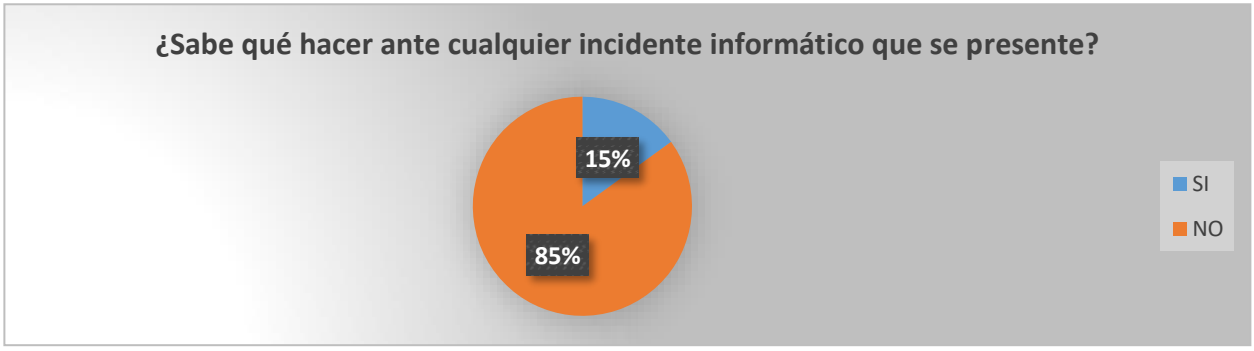
Figura 21 Conocen los controles implementados en la entidad de SI


Fuente: Autoría propia.

Siendo ya específicos para conocer más sobre la seguridad de la información de la entidad se formula esta pregunta, que permite saber si se implementan controles de seguridad a los diferentes procesos, como se ve en la Figura 21 el 85 % de los encuestado no conoce de controles, lo que representa un problema ya sea porque no existen o peor aún si existen los empleados no los conocen, por ejemplo controles básicos y sencillos como tener contraseñas en sus equipos, tener los escritorios libres de información relevante, esto nos indica que ante un ataque premeditado se estaría facilitando el accionar del atacante por parte de los empleados al no tener implementado controles.

- ✓ **¿Sabe qué hacer ante cualquier incidente informático que se presente?**

Figura 22 Conoce el procedimiento ante incidentes informáticos.




Fuente: Autoría propia.

El que los empleados entiendan qué hacer ante cualquier incidente informático es de suma importancia, pues deben tener un conocimiento mínimo independientemente si se presente de manera física o lógica, de aquí radica la importancia de estas preguntas, ya que el proceder de ellos ante cualquier situación puede minimizar los daños ocasionados por mínimo que sea el riesgo. Lo demostrado en los resultados, derivados de la respuesta a la pregunta en la figura 22, es que la mayoría de empleados nuevamente como en la anterior pregunta el 85% no sabe qué hacer, esto evidencia la falta de capacitación por las diferentes entidades que deberían exigir a los empleados que estén cualificados con un mínimo de conocimientos.

Como ejemplo de lo anterior el caso de una infección de ransomware que para evitar la encriptación total de la información se debe apagar el equipo al menor tiempo, lo que logra minimizar la encriptación de archivos en un equipo o la propagación de este entre otros factores, es por esto, que los empleados deben saber cómo proceder, razón por la cual este tema se debe abarcar más constantemente, ya que permite la formulación de estrategias de prevención.

- ✓ **¿Sabe qué pasos debe seguir ante incidentes informáticos en sus equipos de trabajo?**

Figura 23 Conoce el procedimiento ante un incidente informático en sus equipos.


Fuente: Autoría propia.

De acuerdo con la pregunta anterior se formula esta para conocer si los empleados están capacitados para responder específicamente en sus puestos de trabajo ante cualquier situación que se les presente, los resultados de esta pregunta son alarmantes si le sumamos los resultados de las dos anteriores se puede deducir que realmente las entidades donde se aplicó estas encuestas les hace falta capacitar a los empleados debió a que el 95% no sabe qué pasos debe realizar ante un incidente informático como se ve reflejando en la Figura 23.

- ✓ **¿Utiliza redes sociales personales en las instalaciones de la entidad?**

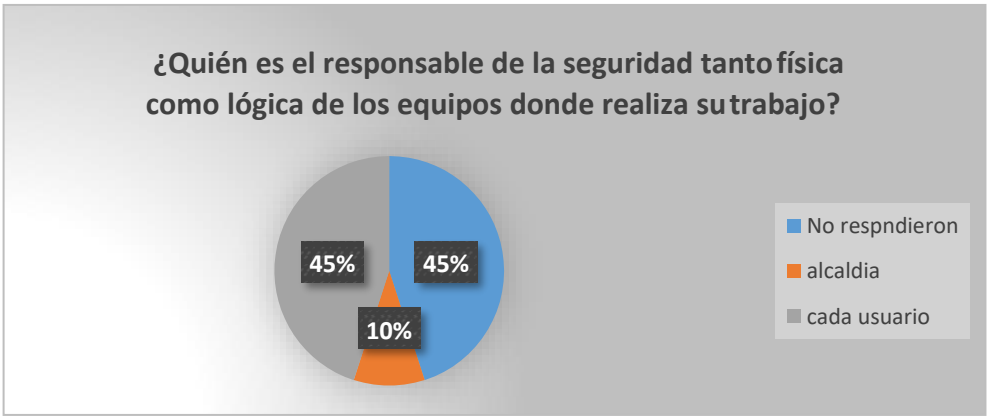
Figura 24 Utilización de redes sociales personales en la entidad


Fuente: Autoría propia.

Algo que es normal en la actualidad es que la mayoría de personas tengan redes sociales, para esto en las diferentes instituciones u organizaciones toman decisiones hasta el punto en algunos casos de prohibir la utilización de ellas en las entidades, esto por los riesgos que representan debido a que las redes sociales son aprovechadas para la de ingeniería social, las cuales son explotadas por los ciberdelincuentes para recolectar información que permitan realizar un ataque especifico con un mayor grado de probabilidad de ser efectivo, y así lograr el objetivo como puede ser el tomar control de un sistema o información de un usuario.

- ✓ **¿Quién es el responsable de la seguridad tanto física como lógica de los equipos donde realiza su trabajo?**

Figura 25 Conocen quien es el responsable de la seguridad de los equipos.




Fuente: Autoría propia.

Este tipo de pregunta se formuló abierta para determinar si el empleado conoce quién es el responsable de los dispositivos en los cuales cumple sus funciones, los resultados dieron algo muy particular y es que un 45% de los encuestados no respondieron nada lo que evidencia el desconocimiento, ya que no saben quién es el responsable de dichos equipos.

De lo anterior, se desprenden varios aspectos importantes para la seguridad de la información como el no tener claro las responsabilidades que tienen sobre los equipos y la información que reside en ellos, lo que indica que no se socializo con ellos las responsabilidades que tienen en cada puesto de trabajo, solo el 10% de los encuestados respondió que la responsabilidad es compartida entre la entidad y ellos, lo cual debería ser lo idóneo nunca solo una parte debe aceptar toda la responsabilidad.

La entidad debe preocuparse porque se garantice la operatividad de cada dispositivo y el empleado debe proporcionar con su actuar un correcto funcionamiento sobre estos, el otro 45% respondió de diferentes maneras como que

el responsable es cada usuario, con el nombre de ellos y otras formas aduciendo que cada uno es el responsable de los equipos asignados, tal y como lo muestra la figura 25 se colocaron como un solo ítem llamado cada usuario.

- ✓ **¿Realiza periódicamente una copia de seguridad de los datos más importantes que tienen los dispositivos sobre los que trabaja?**

Figura 26 Realizan copias de seguridad periódicamente.


Fuente: Autoría propia.

Los diferentes dispositivos son vulnerables a factores entre estos los ambientales que no se pueden predecir tales como desastres naturales, averías físicas entre otros, de aquí la relevancia de realizar copias de seguridad de la información vital, por todo esto debe ser una regla de oro para las personas que usan la tecnología para guardar información independientemente del dispositivo que usen, ya que ante cualquier incidente se deben tener dichas copias para cualquier eventualidad. En especial una entidad que maneja información importante, clasificada y que es necesaria en diferentes procesos.

Con esta pregunta se busca conocer cómo están las entidades en este aspecto y lo que muestra la Figura 26, es que el 50% no lo realiza, lo que es preocupante que la mitad de los dispositivos no cuenten con copias de seguridad, lo que indica que no existe por ejemplo un plan de continuidad que permita ante los incidentes

recuperarse en el menor tiempo posible, ante un caso grave como el daño de un disco duro o peor aún el robo de un equipo se perderá toda la información.

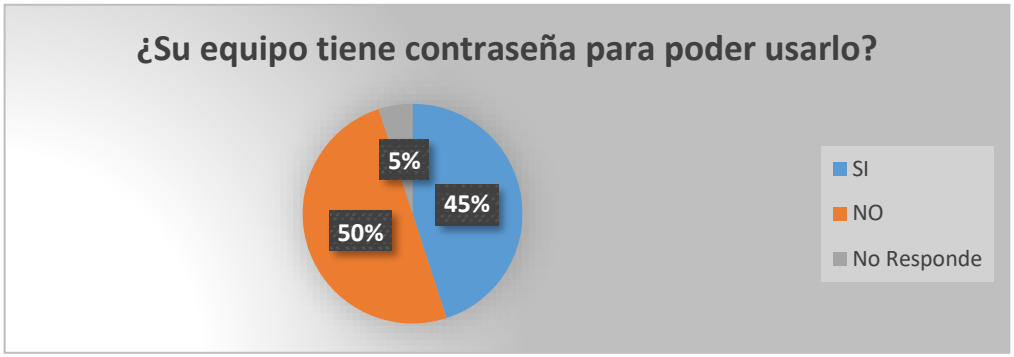
El conocer donde se realizan las copias es otro factor clave ya que es un riesgo si las copias se realizan sobre el mismo equipo que sería algo similar a no tener ante algunos eventos como los que se mencionaron.

Del 50% que respondieron que si realizaban copias de seguridad estos lo realizan principalmente en memorias USB, en disco duro externo, y tan solo el 10% realiza copias en la nube.

De lo anterior 45% están realizando las copias de seguridad por fuera de los equipos lo cual ante un eventual caso de presentarse un incidente con dichos dispositivos como pérdida o robo colocaría la información en riesgo, ya que lo más probable es que en estos dispositivos no estén cifrados.

- ✓ **¿Su equipo tiene contraseña para poder usarlo?**

Figura 27 Tiene contraseña el equipo que usan.



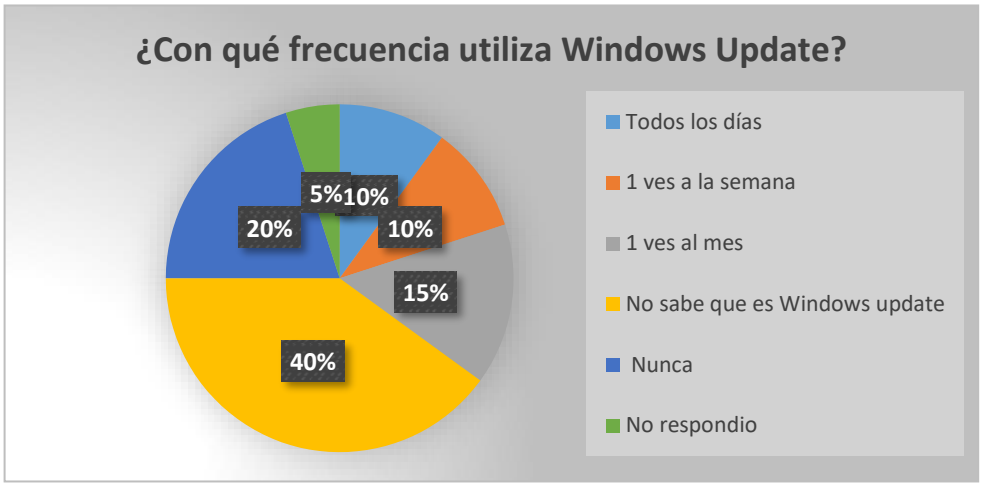

Fuente: Autoría propia.

Una de las primeras barreras para evitar intrusos en los equipos son las contraseñas tanto para los que tengan intenciones de robar información como realizar algún daño por diferentes motivos, lo que busca esta pregunta es encontrar si esto podría ocurrir

en estas entidades, como se observa el 50% de los equipos se encuentran expuestos ya que no tienen contraseña por lo que cualquier persona que tenga acceso al equipo podrá utilizarlos.

- ✓ **¿Con qué frecuencia utiliza Windows Update?**

Figura 28 Instalación de actualizaciones de Windows.




Fuente: Autoría propia.

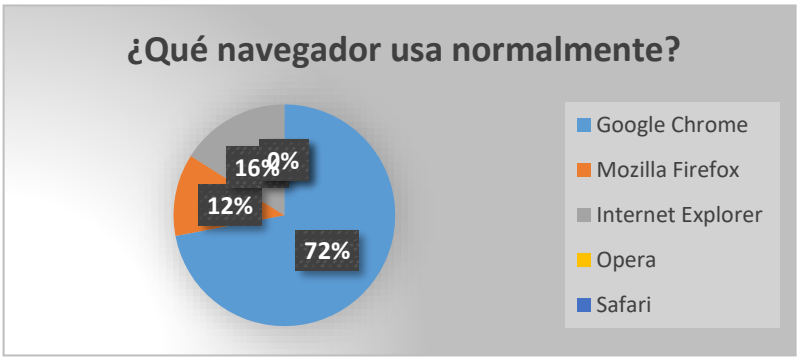
La aplicación de parches de seguridad es un ítem de importancia para mantener a salvo los equipos, para evitar el aprovechamiento de vulnerabilidades, por esta razón se debe actualizar los sistemas operativos o de aplicaciones de terceros como programas, navegadores, complementos, entre otros.

Esta pregunta busca saber si al menos el sistema operativo se encuentra al día con los parches de seguridad que la misma Microsoft ofrece, arrojando que el 40% de los encuestado no sabe que es Windows Update, y que el 20% no lo hace, junto con el con el 5% que no respondió, lo que indica que puede ser explotados algunos equipos al realizar un análisis que determine que Windows tienen los dispositivos y así a través por ejemplo: "El sistema Common Vulnerabilities and Exposures (CVS) de la lista de las vulnerabilidades conocida y en las cuales el 2016 se

descubrieron 6.447 y en 2017, 14.714, un incremento significativo",[48] lo que permite que se puedan vulnerar dichos equipos, de aquí la importancia de la aplicación de parches de seguridad que permitan reducir dichos riesgos.

- ✓ **¿Qué navegador usa normalmente?**

Figura 29 Navegador más usado.




Fuente: Autoría propia.

En la actividad diaria tanto laboral como personal se utilizan navegadores para ingresar a internet, existe varios que permiten la navegabilidad los cuales poseen ventajas como también pueden traer riesgos asociados como vulnerabilidades conocidas si no se actualizan, algunos lo realizan de manera automática otros no, también puede que fallen estos procesos automáticos dejando expuesto a vulnerabilidades.

Conocer por cuales navegan los empleados permite tomar decisiones que conlleven a la protección, medidas como por ejemplo recomendar para algunas actividades un navegador especifico y para otras uno diferente, que en caso de verse afectado

[48] Panda Security. ruityArmor: ciberdelincuentes que aprovechan las vulnerabilidades de Windows 2019. [En línea].2019 2. p.Disponible en https://www.pandasecurity.com/spain/mediacenter/seguridad/ciberdelincuentes-aprovechan-vulnerabilidades-windows/

no exponga datos sensibles, en este caso sería para la navegación institucional un navegador y para las demás actividades otro dando un grado más de seguridad.

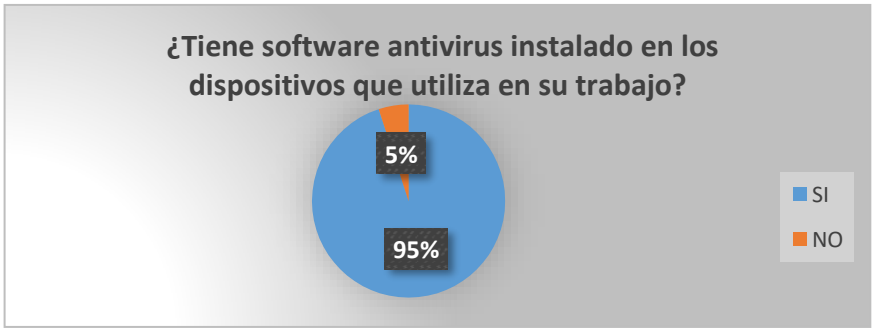
Esta pregunta permite saber que el navegador más usado es el Google Chrome con una gran mayoría por lo que es indispensable que se tenga actualizado, se puede observar que en la encuesta realizada 25% utilizan dos navegadores, lo que indica que tienen algún grado de conocimiento o que en sus actividades es requerido un navegador especifico lo que es bueno en cierto grado en caso de verse expuesto uno de los dos navegadores no tendrían acceso a todos los datos que el empleado utiliza en la red, esto dependiendo claro del tipo de vulnerabilidad y lo que permite.

- ✓ **¿Actualiza el navegador o verifica que se encuentre actualizado?**

El verificar que un navegador se encuentre actualizado debe ser una responsabilidad del personal encargado, así como de los empleados que tengan equipos a su cargo, debido a la explotación de vulnerabilidades que existe asociados a esto, en esta pregunta se puede ver que el 55% de los encuestado no actualizan o no verifican que los navegadores se encuentren actualizados dejando una posible brecha de seguridad.

- ✓ **¿Tiene software antivirus instalado en los dispositivos que utiliza en su trabajo?**

Figura 30 Conoce si tiene instalado un antivirus.




Fuente: Autoría propia.

La importancia en la actualidad de tener un antivirus es de gran relevancia independientemente del dispositivo y del sistema operativo que se tenga, pero no solo es tener un antivirus sino las necesidades que estos cumplen como la protección de virus, ransomware, spyware, adwares entre otras amenazas.

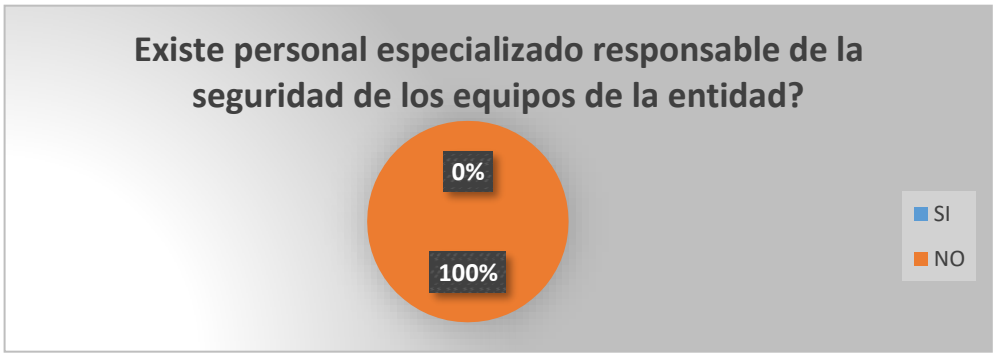
El 95% de las personas encuestadas dicen que tienen instalado un antivirus por lo que es un índice de que los equipos tienen un cierto grado de protección, ante las diferentes amenazas existentes, pero no garantiza nunca el 100% de seguridad.

### 5.3.2 Resultado de la recolección de información de la encuesta tipo 2.

Este tipo de preguntas fueron enfocadas en los altos cargos de la entidad, es decir los secretarios de despachos y quienes tienen un alto grado de responsabilidad en sus dependencias con la información que reside en estos equipos, al igual que la que está en físico.

- ✓ **¿Existe personal especializado responsable de la seguridad de los equipos de la entidad?**

Figura 31 Existe personal especializado para la seguridad de la entidad.




Fuente: Autoría propia.

La primera pregunta determina el compromiso que tiene la entidad con la seguridad de la información y con la seguridad informática, esto debido a la inversión que deben de realizar para tener personal capacitado en el tema de estudio, pero

mayormente este tipo de entidades no disponen del presupuesto para tener el personal idóneo por los costos asociado a esto.

Aunque la estrategia del gobierno sea tener el personal capacitado sobre todo por el plan de tecnología Vive Digital en el nodo de innovación ciberseguridad, el cual entre sus objetivos se enfoca en la "Educación, formación y divulgación en Ciberseguridad uno de los factores fundamentales para garantizar un adecuado conocimiento y desenvolvimiento de los funcionarios públicos, y de la sociedad en general, en temas relacionados con ciberseguridad, radica en la educación y formación de calidad y de alto nivel del recurso humano".[49]

De manera que debería existir personal que tenga esta responsabilidad y que vele por el cumpliendo de esta estrategia, pero lo que nos indica la encuesta es todo lo contrario, ya que del 100% como se puede observar en la Figura 31 de los encuestados respondieron que no cuentan con personal especializado que se encargue de ello, por lo que la estrategia nacional del MinTic a través del plan Vive Digital no está funcionando por lo menos en estas entidades.

[49] República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. AGENDA ESTRATÉGICA DE INNOVACIÓN:CIBERSEGURIDAD [En línea]. Bogotá: 2014. 14 p. Disponible en https://mintic.gov.co/portal/604/articles-6120_recurso_2.pdf

- ✓ **¿Tiene implementado algún programa para incidentes de seguridad de la información?**

Figura 32 Tienen implementado un programa para incidentes de SI


Fuente: Autoría propia.

El conocer que programas o planes existen para enfrentar eventos en cualquier organización es importante, en muchos casos por ejemplo los planes de evacuaciones, que casi todas las organizaciones deberían tener, los cuales por lo general tienen simulacros para comprobar su efectividad y tomar decisiones con respecto a ellos, esto mismo debería ocurrir para los planes que involucran la seguridad de la información más cuando esta se encuentra de por medio, la cual puede ser vital para una organización o entidad para la prestación de sus servicios, el que los empleados tengan claro cómo proceder debe ser parte de las responsabilidades de cada uno, por todo lo que puede representar desde lo económico hasta el funcionamiento de las entidades.

Esta pregunta permite entender que no existe un plan a nivel general, esto ya que el 75% de los secretarios dicen no tener implementado un programa ante incidentes, lo cual es relevante para la seguridad de la información, debido a que, si ocurriese algo, los resultados para la entidad podrían ser muy graves.

- ✓ **¿Tienen programa de monitoreo de las estaciones de trabajo y red de la entidad?**

Figura 33 La entidad cuenta con programa de monitoreo de los equipos.


Fuente: Autoría propia.

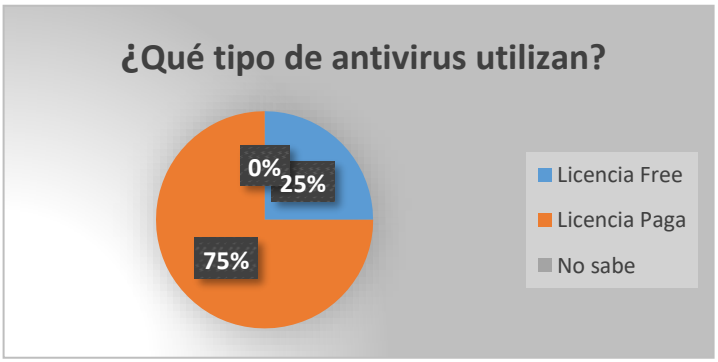
Aunque no es obligatorio tener dispositivos o equipos que permitan monitorear la red de la entidad, sobre todo enfocándose principalmente a lo que tiene que ver con el uso de la red, es importante como herramienta para tener un mayor control, contra posibles intrusos y comportamientos extraños en la misma que permitan anticipar o evitar incidentes.

La respuesta de las personas encuestas permiten ver que en las entidades no existe este tipo de programa, esto puede deberse a diferentes factores, el primero y el más evidente es la falta de personal especializado que se encargue de estas funciones, como determinar si algún equipo tiene tráfico de red más de lo usual, lo que puede representar un problema de seguridad, o un posible consumo en exceso de las megas contratadas al proveedor de internet, que ralenticen la red, entre otros aspectos.

La falta de recursos es un aspecto no solo para la contratación de personal sino de la disposición de equipos y software que se requieran, esto en caso de querer implementar un sistema que permitan obtener información en tiempo real.

✓ **¿Qué tipo de antivirus utilizan?**

Figura 34 Tipo de antivirus que se usan en la entidad.




Fuente: Autoría propia.

Es importante la protección de los diferentes dispositivos con programas especializados, en este caso la pregunta formulada busca conocer si el antivirus es de licencia gratuita o paga, esto porque es muy claro las diferencias que existen entre las versiones las dos versiones, como el tipo de protección que ofrecen, por ende, la cantidad módulos que protegen contra las diferentes amenazas.

Se observa que el 75% de las personas dijo que utilizan una versión paga, aunque no estaba formulada en la encuesta a los que respondieron que era paga se les preguntó ¿Que versión tiene instalada? la respuesta fue ESET Endpoint Security en la alcaldía de Labateca e internet Kaspersky small office en la alcaldía de Toledo, las cuales son versiones para empresas lo que es un grado de protección contra amenazas comunes y algunas específicas como ransomware, al igual que tiene un módulo para la gestión de redes, también permite el manejo de contraseñas, lo que puede garantizar un grado más de seguridad para las entidades.

La licencia que presentan los antivirus es por 1 año, si uno de los inconvenientes para este tipo de entidades son los recursos, la inversión de este tipo de software debería realizarse con un plan, que permita un mayor tiempo de protección y un

ahorro, porque los antivirus ofrecen paquetes a 2 o 3 años reduciendo considerablemente los costos en la compra de ellos.

- ✓ **¿Utilizan sistemas de autenticación de doble factor**?

Figura 35 Uso de sistemas de autenticación con doble factor.


Fuente: Autoría propia.

Con la suplantación en los diferentes sistemas y las repercusiones que estas traer, la utilización de un factor extra de seguridad es de importancia, para este caso los secretarios que sobre ellos recae información confidencial y de gran valor, por lo que deben tener claro esto, estar aplicándolo en la mayoría de aplicaciones a las que tienen acceso, tanto las personales como las institucionales y que son susceptibles a diferentes ataques.

Un método extra de seguridad permite un grado mayor de esta ante una anomalía, como el intento de ingreso desde otro sitio, si se activa opciones como autenticación a través de SMS que es lo más recomendado y no a un correo, en este último la inseguridad radica en que si estos fueron tomados por el atacante, este podrá tener acceso a aplicaciones o plataformas al igual que podrá tener más fácil el acceso a los correos asociados, lo preocupante de las respuestas obtenidas de las personas encuestadas el 100% es que no tienen protecciones de doble factor, lo que representa un gran riesgo tanto para la entidad como para ellos.

- ✓ **¿La conexión a la red interna de la entidad ya sea física o inalámbrica tiene limitantes, controles para la conexión?**

Figura 36 Controles en la conexión de la red interna de la entidad.

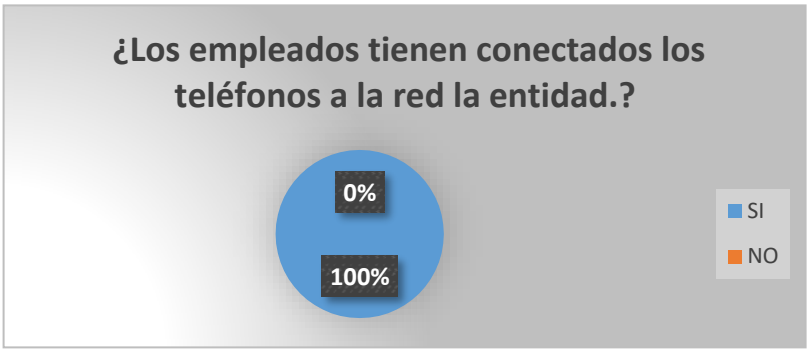

Fuente: Autoría propia.

El aislar las redes de intrusos es de vital en la actualidad para evitar diferentes tipos de ataques, más si relacionamos la pregunta realizada a las personas sobre redes sociales donde casi en su totalidad las utilizan y que se conectan a la red de la entidad, en este caso si no se cuentan con medidas que restrinjan el acceso se puede considerar como una vulnerabilidad para las entidades, ya que como se explicó en el ítem del factor humano, algunos valores pueden ser explotados por estas redes lo cual representan riesgos, la posibilidad que compartan las contraseñas de las redes inalámbricas de la entidad es muy factible, más si es con personas cercanas y esto termina en una cadena, permitiendo tener acceso a la red a personas que puedan utilizar para otros fines, ocasionando diferentes inconvenientes, no solo de seguridad, también llegando a saturar las redes congestionándolas, según el uso que le den.

Las respuestas a la pregunta formulada fue que el 50% dicen que, si existe limitantes, lo que quiere decir que la mitad de las redes están desprotegidas siendo un problema de seguridad y estabilidad en los servicios que usen estas.

- ✓ **¿Los empleados tienen conectados los teléfonos a la red la entidad.?**

Figura 37 Conexión de dispositivos personales a la red de la entidad.




Fuente: Autoría propia.

Continuando con el tema tratado en la anterior pregunta se buscó saber si tienen sus teléfonos conectados a la red de la entidad, estos debido a que, al ser de tipo personales, no solo se conectan a esta red sino a una gran variedad de redes donde puede ser contaminados, lo que puede propagar alguna infección en las entidades.

La respuesta obtenida de los encuestados es que el 100% de los empleados tienen conectado los teléfonos a la red de las entidades, lo cual representa riesgos asociado a esto, también pueden deberse a la utilización de aplicaciones instituciones en dispositivos por mayor facilidad.

Se deberían establecer controles sobre estos dos aspectos, tanto sobre el uso de estos dispositivos en el ámbito laboral como el de la utilización de las redes de la entidad.

- ✓ **¿Usted cree que Los empleados tienen la capacidad para reconocer un email sospechoso?**

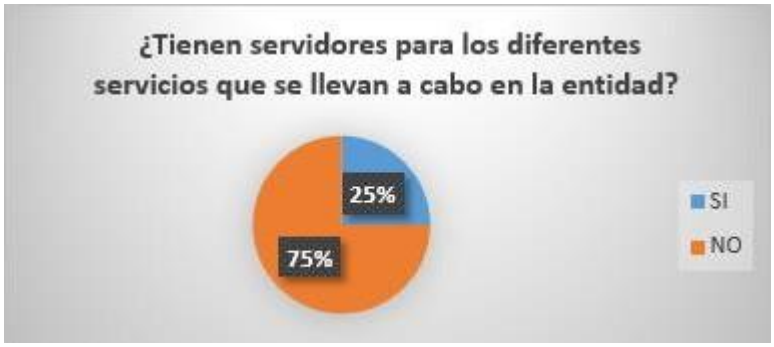
Figura 38 Capacidad de los empleados para reconocer un email sospechoso.


Fuente: Autoría propia.

La percepción que tienen los secretarios sobre los empleados es un factor a considerar en las responsabilidades asignadas, como es el caso de permitir el uso de correos institucionales y aplicaciones institucionales, que requieren de unos mínimos de seguridad, esta percepción se puede ver reflejada en la pregunta formulada y es que la mitad cree que los empleados si tienen capacidades para distinguir un correo sospechoso, que va relacionado con la pregunta 14 formulada en las encuestas de tipo 1 y no están muy lejos de la realidad siendo que respondieron que el 45% si reconoce un email sospechoso, pero ese porcentaje es inseguro por lo que no se debería permitir que otros usaran estos correos o aplicaciones para disminuir riesgos.

- ✓ **¿Tienen servidores para los diferentes servicios que se llevan a cabo en la entidad?**

Figura 39 Cuenta con servidores la entidad.




Fuente: Autoría propia.

El conocer con que equipos cuenta una entidad u organización es importante para ella, así como para las personas en cargadas de su seguridad, al igual para tener claridad de como son los procesos que ocurren en esta y como intervine dichos dispositivos en ellos.

De la pregunta formulada se observa que el 75% de los encuestados respondieron que no existen servidores en la entidad, partiendo de ello se puede afirmar que los empleados desconocen que estos existen, esto puede deberse a que solo unos cuantos son los que lo utilizan, los cuales pueden ser los que respondieron que si existen como se observa en la figura 39, lo que también puede llegar a ser un riesgo, ante sucesos que se puedan presentar y los empleados no tengan conocimiento del procedimiento a seguir ante ellos como por ejemplo el correcto apagado de estos.

- ✓ **¿Tienen personal encargado para instalar o desinstalar los programas y aplicaciones informáticas en su empresa?**

Figura 40 Cuenta con personal para el manejo de las aplicaciones de la entidad.


Fuente: Autoría propia.

Esta pregunta permite validar ciertos controles que deberían de tener en las entidades como que solo personal específico sea el encargado de instalar o desinstalar programas, aplicaciones o lo que se requiera, lo que evita problemas de seguridad como por ejemplo que un empleado instale un software que tenga virus o que infrinja los derechos de autor u otro problema de seguridad.

El resultado de la pregunta es un claro problema de seguridad para las entidades, debido a que el 100% de los encuestados dicen no tener personal para dicho proceso.

### 5.3.3 Causas de riesgo del factor humano

A partir del análisis de los resultados obtenidos de las encuestas realizadas, se encuentra que la principal causa es el desconocimiento, esto asociado a los factores propios del carácter de las personas, pueden llegar a ser un gran riesgo para los sistemas de la seguridad de la información, debido a todo lo que se puede asociar a la falta de conocimiento desde básico hasta especifico que se requiera en las actividades que se desarrollan.

Este tipo de vulnerabilidad, que existe en los sistemas de las entidades, al igual que en las organizaciones, donde no se es consciente en los diferentes niveles que componen las organizaciones u entidades, debido a factores como la falta de compromiso, interés, responsabilidad, amor propio entre muchos más, que son específicos de las personas.

El comportamiento de las personas implica también el aprovechamiento por parte de los atacantes de los factores de riesgos citados en el aparte de La conducta humana como factor de riesgo, que van desde perdida de información, daño en equipos, pérdida de productividad entre muchos más factores, que afectan a una organización o como es en este caso una entidad pública.

Todo esto puede estar no solo asociado a hechos como la falta de conocimiento que si bien es la primera causa, otros factores pueden involucrarse como es el carácter académico o preparación de las personas que puede influir en la forma en que actúan, basándonos en las diferencias de las respuestas de las encuestas de tipo 1 y tipo 2 siendo estas últimas para los secretarios, se puede observar que ellos tienen mayores conocimientos sobre este tipo de temas, lo cual puede deberse a que para ocupar dichos cargos ellos deben cumplir con ciertos requisitos como lo dice el manual de funciones y de competencias laborales establecidos en cada entidad y que responden a “la ley 909 de 2004 y el decreto ley 785 de 2005.”[50]

Por lo que se debe buscar combatir el desconocimiento no solo desde la parte técnica sino en general, que permitan tener empleados que identifiquen comportamientos riesgosos, que eviten colocar en estas situaciones a las entidades u a otras personas, ya que los ataques no solo van dirigidos a una organización sino también a sus integrantes donde ellos de manera directa o indirecta se pueden afectar, ocasionándoles también pérdidas para ellos.

[50] Función Pública. Concepto 20101 de 2016 Departamento Administrativo de la Función Pública [En línea]. El mundo. 2015 5 p. Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=68295

Entre los factores de riesgos mencionados a la conducta humana es de destacar el compromiso junto con la ética, estos dos son de destacar ya que los empleados no solo deben de realizar lo que les indique su manual de funciones y responsabilidades, sino ir aún más allá de estos, como es por ejemplo que si en un manual de funciones no existe una responsabilidad en un tema determinado, el hecho que no esté en el no implique que no lo realice, un ejemplo seria que vea a personas ajenas a la entidad conectadas a la red, lo lógico sería avisarle a los encargados de la seguridad para que tomen las medidas pertinentes.

El que no exista en los manuales de funciones responsabilidades también implicaría un fallo por parte del control interno de las entidades, que debe realizar dichos correctivos a medida que se van presentando y realizar una actualización de estos, los cuales deben construirse junto con los empleados ya que ellos deben proponer cuáles son sus responsabilidades siempre en pro de la entidad, más compromiso debe haber por parte de ellos, más en este tipo de entidades que están hechas para servir al pueblo.

Un factor asociado que aunque no parecieran que tuvieran que ver directamente con el factor humano es la infraestructura, la razón es debido a que puede reflejar el compromiso de los funcionarios públicos con la entidad, se entiende que en la actualidad la información es un valor vital, por lo que la inversión en la protección y procesamiento de esta debe ser un factor de inversión y no de gasto, siendo en este tipo de entidades de pocos recursos una decisión difícil de tomar, donde los presupuestos son ajustados y el tomar rubros para invertir en este campo puede generar diferentes efectos, que los mandatarios no quieran asumir y por ende no toman la decisión como por ejemplo el rechazo que pueda tener por parte de la comunidad a una inversión grande en dotación de equipos que permitan tener segura la entidad.

### 5.3.4 Principales vulnerabilidades y amenazas encontradas.

Amenazas:

- Rotación de personal de orden de prestación de servicios (OPS).
- Falta de continuidad en los procesos.
- Desconocimiento de los organismos colombianos que están a cargo de la ciberseguridad.
- Carencia en el conocimiento de las políticas o inexistencias de estas en las entidades.
- Deficiencia en la preparación para identificar las amenazas que existen en el ciber espacio.
- Falta de compromiso con la misión y visión de las entidades.
- Precariedad en la aplicación de mecanismos de seguridad en plataformas y aplicaciones.
- Mal uso de los correos electrónicos.
- Cambio de contraseñas en periodos demasiado largos o utilización de la misma contraseña en diferentes plataformas y aplicaciones.
- Desconocimiento de la ley que rige la protección de la información en Colombia.
- Equipos sin contraseñas.
- Falta de personal capacitado en seguridad informática y de la información.
- Conexión de dispositivos personales para uso particular a las redes de las entidades.
- Falta de infraestructura para la implementación de seguridad física y lógica.
- No manejar un marco de buenas prácticas (no implementarlo)
- Manuales de funciones no acordes a la actualidad, evasión de las responsabilidades.
- No tener un inventario de activos de información.
- Falta de procedimientos para la atención de incidentes informáticos o físicos.
- Ingreso a las redes wifi sin restricciones salvo la contraseña de ingreso.
- Falta de asignación de funciones a los diferentes funcionarios públicos.

- Facilidad de la aplicación de ingeniería social en los empleados de las entidades.

**Vulnerabilidades:**

- Falta de actualizaciones o parches de seguridad de sistemas operativos.
- Navegadores desactualizados y versiones con vulnerabilidades conocidas.
- Falencia en controles para resguardar la información.
- No contar con procesos de criptografía.
- Redes inalámbricas sin protección de seguridad.
- Falta de seguridad lógica como antivirus.
- Falta de monitoreo de las redes y estaciones de trabajo.
- Falta de la realización de copias de seguridad.
- No cumplir con norma ISO 27001

## 5.4 PROPOSICIÓN DE UN DOCUMENTO PARA LA FORMULACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN ENFOCADAS AL FACTOR HUMANO.

Para la formulación de estrategias de ciberseguridad se deben tener en cuenta todos los aspectos, enfocándose en los riesgos pero lo que siempre va a existir son amenazas por lo que se deben disminuir y de la recolección de información realizada, se puede decir que aparte de la implementación de herramientas para la protección, es la divulgación del conocimiento sobre todos los que interactúan de manera directa o indirecta con la información, para que ellos sean la primera barrera de seguridad ante las amenazas existente.

De las entidades donde se recolecto la información se evidencio que no existe personal especializado en la seguridad de la información o que tengan el perfil para aplicar las guías dadas por el MinTic, el cual orienta la aplicación de políticas, lo que

si debe ocurrir en otras entidades que disponen de recursos para implementarlas recomendaciones del Ministerio Tic como la implementación de un SGSI, o planes para el control de riesgos de la información, para la gestión de riesgos o un plan de continuidad del negocio.

Aunque se tenga personal especializado no se puede garantizar la seguridad en un 100% como lo dice el especialista Cristián González un profesional en este campo "no puede evitar que los sistemas sean vulnerados, lo que puede hacer es estar preparado y entrenado para enfrentar una crisis de ciberseguridad y mitigar el ataque".[51] si con profesionales puede ocurrir incidentes, sin ellos las probabilidades de que los daños ocasionados en un incidente sean más graves son mayores, de aquí el acompañamiento que deben realizar las diferentes entidades del estado encargadas de la protección de la información en Colombia.

La implementación de estrategias de protección no siempre significa inversiones costosas en equipos y software para la protección, esto es debido a que ante la ausencia del compromiso de los empleados y faltas de capacitación pueden hacer vulnerable un sistema, si solo dependiera de equipos para la protección las grandes empresas no sufrirían ningún tipo de violación de sus sistemas, como indica el periódico El mundo[52] la red social Facebook que reconoció la filtración de datos de más de 120 millones de usuarios esto por falla en sus sistemas, que permitió que una aplicación de un tercero obtuviera esta información y teniendo en cuenta que las redes sociales son importante para la realización de ataques personalizados, es algo muy grave, y así como esta empresa sufrió esta filtración de información de sus usuarios, otras empresas les ha ocurrido los mismo las cuales fueron noticias

[51]GONZÁLEZ, Cristián. citado por AméricaEConomía.com. 4 tips para elaborar estrategias de ciberseguridad [En línea]. 2019 1 p. Disponible en https://mba.americaeconomia.com/articulos/notas/4-tips-para-elaborar-estrategias-de-ciberseguridad

[52]Periódico digital El mundo. Facebook reconoce la filtración de datos de más de 120 millones de usuarios [En línea]. El mundo. 2018 2 p. Disponible en https://www.elmundo.es/tecnologia/2018/06/30/5b35f2f4468aeb22438b457d.html

a nivel mundial como Yahoo! o Gmail por nombrar algunas de reconocimiento mundial.

Por lo que la protección de un sistema no solo se limita a los que hacen parte de ellos directamente como sus empleados, sino también de terceros que interactúan con las organizaciones u entidades, por lo que un atacante puede tener acceso a través de terceros como es el caso de los contratistas, proveedores entre otros a los cuales robando sus cuentas pueden ir escalando en el acceso a un sistema hasta llegar a tener control de él.

En la implementación de estrategias de mitigación del conocimiento se pueden implementar a través de los expertos que tengan las diferentes entidades del gobierno a nivel nacional o departamental, sin que esto incurra en mayores gastos para las entidades a través de posibles convenios interinstitucionales, que permitan a las entidades de menores recursos, capacitarse y tener empleados con conocimientos idóneos, que permitan afrontar amenazas y mitigar sus efectos.

Por lo anterior se propone dos documentos el primero un Banco de Preguntas para identificar problemas asociados al factor humano y el segundo el Banco de Políticas aplicables para disminuir vulnerabilidades y amenazas debido al factor humano, ambos correlacionados siendo el primero el insumo para una mejor aplicabilidad del segundo**.**

### 5.4.1 Banco de Preguntas para identificar problemas asociados al factor humano.

Algo importante es la valoración del estado actual de la seguridad en las entidades enfocados al factor humano, porque es donde se pueden tomar medidas a menores costos, lo primero que se recomienda es la realización de un diagnostico esto se puede realizar a través de un banco de preguntas que permiten identificar problemas relacionados al personal, complementadas con las herramientas dadas

por el MinTic para encontrar los riesgos a los cuales darles soluciones a través de planes o estrategias, así como la mejora de los existentes o la implementación de nuevos.

Las preguntas pueden ser cerradas para tener mayor claridad, lo que no significa que estas preguntas puedan ser modificadas según la necesidad de cada entidad o lo que se requiera diagnosticar o verificar.

- **“Conoce el Plan Estratégico de Tecnologías de la Información de la alcaldía”**

Conocer el PETI el cual debe existir en cada una de las entidades según los lineamientos dados por el MinTic en sus guías así como la socialización a los diferentes actores que intervienen en él, por lo que conocer si los empleados saben de él es de importancia, entendiendo que existe muchos cargos o funcionarios que son de tipo OPS y otros de libre remoción, los cuales pueden estar cambiando de trabajos constantemente generando una rotación en dichos puesto lo que esto implica empalmes e inducciones .

Se entiende que al cambio de administraciones que por lo general son cada 4 años puede ser un problema, al entrar nuevo personal, lo que puede significar la perdida de continuidad, por lo que se deben tener políticas que garanticen un correcto empalme que conlleve a la continuidad de los procesos, principalmente en temas claves a largo plazo, por lo que de temas sensibles los encargados deberían ser de planta o las personas de libre remoción, que por lo general estos últimos permanecen más tiempo que los OPS.

- **“Usted ha asistido a capacitaciones en la protección de seguridad de la información o similares”**

Permite saber si se está cumplimiento con los lineamientos nacionales que busca que los empleados públicos tengan el conocimiento, que permita ser la primera barrera de seguridad ante diferentes amenazas, esta pregunta permitirá ser el insumo para tomar decisiones para estrategias de capacitaciones.

- **“En su manual de funciones tiene establecido las responsabilidades que tiene tanto con los equipos como con la información que radican en ellos.”**

Una de las herramientas de las administraciones es el manual de calidad que permite establecer las responsabilidades que cada uno de sus funcionarios tienen ante la entidad, el cual se deben estar actualizando ante los diferentes cambios que sufren debido a las leyes, normas o directrices que conlleven a ello, por lo que determinar que niveles de responsabilidad deben tener los diferentes empleados debe ser un proceso con retroalimentación constante.

- **“Conoce la política de seguridad de la información de la entidad “.**

Esta pregunta permite determinar que empleados pueden ser hasta cierto punto una vulnerabilidad para la entidad, lo que permitirá evaluar por qué no conocen la política en caso de la respuesta sea negativa, siendo lo pertinente realizar un test más detallado para mitigar dicha vulnerabilidad, como lo expresado del factor humano que sigue siendo uno de los eslabones más débiles de la seguridad de la información y una sola persona puede ser un agujero a explotar por los ciberdelincuentes, más en este tipo de entidades que es el **“**tercer sector que más recibe ataques cibernéticos cada día**”.**[53] Es probable que a través de los correos electrónicos estén recibiendo ataques en búsqueda de ingresar a las redes de las entidades, lo cual si no se tienen políticas establecidas para evitar este tipo de riesgo es un factor que puede llevar a situaciones no deseadas en las entidades.

También es importante verificar si la respuesta es afirmativa sea cierto ya que muchas personas pueden decir que si, aunque no sea la realidad, por lo que es bueno confirmarlo con una contra pregunta como, por ejemplo: Si la respuesta a la anterior pregunta fue si, escriba al menos una política, siendo una pregunta abierta que permite verificar la veracidad de la respuesta.

[53] Revista Dinero. Op. cit., p. 1

- **“Sabe quiénes son los responsables de la seguridad de la información en la entidad.”**

Conocer quiénes son los responsables de la seguridad es algo fundamental ya que permite saber a quién acudir ante cualquier incidente o para mejorar los procesos con retroalimentación en la implementación de las políticas y controles**.**

- **“Considera que la seguridad física (protección voltajes, robos, daños en la infraestructura etc.) de los equipos está garantizada”**

Con esta pregunta se puede conocer de los empleados su percepción en este aspecto, que también es fundamental para la pérdida o daño de la información, esto permite tomar medidas correctivas, formulando proyectos que permitan subsanar dichas falencias como por ejemplo la implementación de medidas de seguridad para los equipos si no cuentan con ello, arreglos locativos entre muchos aspectos.

- **“Utiliza dispositivos como USB, disco duro, DVD personales para guardar información de la entidad.”**

Esta pregunta permite identificar quienes están manejando información de la entidad en dispositivos que se pueden considerar como no seguros, permitiendo tomar las medidas de seguridad correspondiente para proteger el activo más importante de las entidades como es la información, que no debería estar almacena en cualquier dispositivo más cuanto tiene ciertos riesgos asociados al ser de una entidad.

- **“Usted puede navegar en los equipos y redes de la entidad sin ningún tipo de restricción, puede visitar cualquier página al igual que descargar.”**

El determinar si algunos controles que se pueden haber implementado, están en funcionamiento, en mal funcionamiento o por el contrario no se han establecido, es de importancia realizar el seguimiento a las diferentes estrategias que se llevan en

la entidad, estas deben tener un control como es en este caso, evitar que se instalen programas sin autorización a través de navegadores, que es uno de los mayores métodos de ataques y por ende de vulneración de los sistemas.

- **“Usted ha visto si algún compañero realiza alguna de las siguientes acciones frente a los equipos: Come frente a los equipos, navega en redes sociales, no apaga los dispositivos al irse, hace compras personales en dichos dispositivos, permiten el uso de dispositivos a terceros, entre otras acciones,”**

Muchas veces determinar quiénes no cumplen con normas básicas asociado por la cultura establecida en las sociedades, así como en las propias entidades, es importante para establecer las estrategias para mitigar los problemas que parten de ello, se puede fijar los planes para poder mitigar los riesgos que puedan nacer de esos comportamientos.

El tipo de respuesta es recomendado que sea de selección y también con la opción de escribir una respuesta en caso de que no se encuentre contemplada en la selección.

- **“Cuando apaga y desconecta usted los equipos”**

Preguntas relativamente sencillas que permiten identificar ciertos comportamientos que pueden dar por descontados y los cuales entendemos no ocurrirían, con esta se busca establecer si las personas que se encuestan cumplen o no con un procedimiento tan sencillo como apagar y desconectar los equipos al salir de las jornadas laborales.

Con este tipo de pregunta se abordan el tema de seguridad al igual que permite obtener otros beneficios como identificar falencias a niveles mínimos por lo que son una señal para la realización de diagnósticos que permitan tomar decisiones a corto plazo, salvaguardando la seguridad e integridad de los dispositivos e información que reside en ellos.

- **“Usted considera que la infraestructura tecnológica de la alcaldía es”**

Conocer la percepción de los empleados en cuanto a la infraestructura es importante, porque permite mejorarla utilizándola como retroalimentación, entendiendo que para un empleado no es lo mismo trabajar en un equipo obsoleto el cual no ofrece garantías de seguridad y fluidez para el desarrollo de los procesos que cada uno debe de llevar, ocasionando diferentes efectos entre estos el estrés siendo un problema no solo para el empleado sino para la entidad por lo que puede significar como indisposición del empleado.

- **“Tiene un cuadro comparativo o un historial de los diferentes autodiagnósticos realizados en la entidad que permita comparar la evolución año a año de estos”**

Tener un histórico de los diferentes autodiagnósticos o diagnósticos que se han realizado en los diferentes años es importante para saber cómo ha venido evolucionando los sistemas de información y seguridad en las entidades, si no existe seria recomendado su implementación, comprender que cambios y compromisos ha tenido la entidad permite una mejor autoevaluación y tomar decisiones basada en mejores datos.

Esta pregunta está enfocada para un personal más específico, ya que dentro de la estrategia de gobierno digital la cual se reglamenta en: “El decreto 1078 de 2015 Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones que en su título 9 establece los lineamientos generales para la implementación de la estrategia”,[54] estable la aplicación de 4 planes estratégicos para esto los cuales se les debe estar realizando un seguimiento a estos, que por lo general son a 4 años pero que también se debe considerar el problema de la rotación de personal y la continuidad de estos un ejemplo de esto sería la

[54] República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. Decreto único reglamentario del sector de tecnologías de la información y las comunicaciones DECRETO 1078 DE 2015 (26 de mayo 2015) [En línea]. Bogotá: 2018. 172 p. Disponible en https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

implementación del PETI(Plan Estratégico de las Tecnologías de la Información y Comunicaciones).

- **“Usted utiliza un correo oficial para las comunicaciones de la entidad y que correspondan a sus funciones o utiliza uno personal para ello.”**

Es importante conocer los canales de comunicación que tienen los empleados, porque este es un método que frecuentemente es atacado y vulnerado por parte de los ciberdelincuentes, aprovechándose de las diferentes técnicas que existen para ello.

Entendiendo que la estrategia de gobierno digital así como de otras por mencionar una, la de cero papel que buscan el cuidado del medio ambiente y mejora de los procesos, lo que incentivan el uso de los correos electrónicos, que para el caso de las entidades tiene a disposición el que provee el MinTic bajo ciertas condiciones, como es tener un dominio en gov.co/territorial/, el cual también va acompañado de los correos electrónicos institucionales, los cuales deben cumplir ciertos requisitos al igual que los usos que se les pueden dar, algunos de estos son: “Las responsabilidades que tienen el propietario de la cuenta, la seguridad que debe tener el tipo de contraseña a establecer el periodo de cambios de estas, establece claramente que actividades no se puede utilizar las implicaciones que están trae entre muchas más”.[55]

Cumplir con las condiciones dadas por el MinTic es necesario para tenerlos, al igual de no tener riesgos de seguridad asociados a ellos, un ejemplo de un uso inadecuado seria que los empleados deban usar los correos personales para las comunicaciones oficiales por todo lo que esto implica, un factor de riesgo seria el cambio de cargos o abandonar el cargos esto podría traer consigo que las comunicaciones oficiales que llegan no sean leídas o correos archivados que se

[55] República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. TÉRMINOS Y CONDICIONES DE USO DEL CORREO ELECTRÓNICO[En línea]. Bogotá: 10 p. Disponible en https://estrategia.gobiernoenlinea.gov.co/623/articles-9410_politica_correo.pdf

llegasen a necesitar o peor aún que se utilicen esos correos para otros aspectos que vayan en contra de las actividades de la entidad.

- **“La entidad ha realizado un levantamiento de información evaluando los riesgos tanto físicos como lógicos, que puedan afectar el normal funcionamiento de los procesos de la entidad.”**

Esta pregunta es más específica para ciertos empleados ya que permite determinar si se tiene una base sobre la cual realizar las diferentes estrategias que conllevan a que la información está segura, como el plan de tratamiento de riesgos de la información el cual está establecido en el marco de estrategia de gobierno digital.

El cual está orientado a encontrar y mitigar cualquier riesgo que pueda existir para la información que reside en la entidad, ya sea en equipos que están dentro o no de esta, al igual que servicios contratados con terceros, los cuales deben tener sus respectivos contratos con los términos en que lo prestan como las condiciones y responsabilidades de ellos ante la información que poseen, a la cual deben garantizar su integridad y confidencialidad.

No se puede permitir un contrato con un tercero que permita el desentendimiento sobre la información, al igual la responsabilidad de la entidad debe ser permanente con esta así la tengan terceros, por lo que si se encuentra una respuesta negativa significa que la guía de gestión del riesgo, la numero 7 dada por el MinTic no existe en el peor de los casos o que en su desarrollo no se llevó a cabo correctamente, como lo establecen los puntos “10. IDENTIFICACIÓN DE RIESGOS y 11. ANÁLISIS DE RIESGOS”,[56] que son primordiales en la elaboración de un plan de tratamiento de riesgos, donde se pueden definir según los criterios de la información cuales pueden llegar a ser aceptables, cuales son críticos y se deben intervenir de manera inmediata.

[56] República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. Guía de gestión de riesgos SEGURIDAD Y PRIVACIDAD DE LA INFORMACION [En linea]. Bogotá: 39 p. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

- **“Tiene usted en su equipo o ha visto en algún equipo de la entidad software pirata instalado”**

Como se sabe la utilización de software pirata puede ser un gran agujero de seguridad, por lo que conocer esto permite tomar correctivos, que van desde la legalización de dicho software o la búsqueda de software opensource en caso de no contar con recursos para legalizarlos que se tienen de manera irregular, se deben remplazar por unos de licencia gratuita, los cuales deben cumplir con las mismas funciones, además de que se debería tener un control de esto y no ser permitido la utilización de software ilegal más cuando en Colombia existe una ley que regula este tema.

También a este banco de preguntas se pueden anexar las preguntas realizadas en los puntos 5.2 de este documento, las cuales permiten identificar los diferentes riesgos que existen en las entidades, dependiendo el propósito que tenga la recolección de la información se podrán aplicar dichas preguntas o ser la base para la formulación de preguntas más específicas.

### 5.4.2 Banco de Políticas aplicables para disminuir vulnerabilidades y amenazas debido al factor humano.

Entendiendo que “la formulación de políticas es un elemento imprescindible cuando se pretende gestionar la seguridad de la información en una empresa”,[57] de aquí la importancia de tenerlas en las entidades donde ayudan a mitigar los riesgos asociados al factor humano, más cuando establecen “Lo necesario para estar en apego con las leyes aplicables de acuerdo con el negocio de la organización, así como con las regulaciones y obligaciones contractuales directamente relacionadas

[57] MENDOZA, Miguel Ángel, Beneficios de la aplicación efectiva de políticas de seguridad [En línea]. 2014. 1 p. Disponible en https://www.welivesecurity.com/la-es/2014/07/25/beneficios-aplicacion-efectiva-politicas-de-seguridad/

con seguridad de la información",[58] por esto se coloca a consideración las siguientes políticas aplicables en las entidades, las cuales pueden servir de complemento a la guía que proporciona el MinTic para la elaboración de políticas.

Cada una de las políticas contiene el objetivo que se quiere lograr con cada una de ellas como el alcance que tendrá, esto siempre como sugerencia siempre puede acondicionarlas para lograr los objetivos que se deseen alcanzar.

#### 5.4.2.1 Políticas de la infraestructura Organizacional

**Objetivo:** Lograr una mayor eficiencia, así como una descripción clara y comprensible de la estructura de la entidad ante las personas que la componen, con una implementación segura de la información dentro de la organización.

**Alcance:** Todos los servidores públicos y la comunidad.

**Descripción de la política:**

- La entidad en cabeza del alcalde y funcionarios con responsabilidad en el manejo de la información, se comprometerán a difundir las políticas de la seguridad de la información a todo el personal y estar prestos a cualquier tipo de modificación y aclaración en caso de que hiciera falta.
- Se crearán canales seguros para trasmitir la información y garantizar que todo el personal este informado.
- Se fijará un comité de seguridad o asignará dichas funciones a uno ya existente, el cual tendrá la función de analizar los incidentes de seguridad y realizar el debido proceso con las áreas encargadas.
- El comité de Seguridad verificara y controlara que las políticas de seguridad se están implementando de manera adecuada.

[58] Ibíd, 1 P.

- El comité de seguridad o el que tome sus funciones deberá definir una metodología para realizar el análisis de Riesgo de la seguridad de la información y así mismo para clasificar la información.
- Se establecerá un esquema de seguridad de la información en donde se determinarán los Roles a los cuales se les asignarán funciones y responsabilidades.

#### 5.4.2.2 Política de limpieza del puesto de trabajo y pantalla limpia.

**Objetivo:** Prevenir la perdida, daño o acceso no autorizado a la información que se encuentra en los diferentes puestos de trabajo, cualquier dispositivo de almacenamientos, incluyendo la información que está en físico es decir en medios no electrónicos de cada uno de los servidores públicos.

**Alcance**: Todos los servidores públicos y terceros que tenga información de la entidad.

**Descripción de la política:**

- La entidad con el compromiso de los funcionarios y contratistas deben prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, tanto en los horarios laborales como fuera de estos, al igual que dentro y fuera de ella, mediante lineamientos establecidos para que sean aplicados.
- El funcionarios o contratista al levantarse del puesto de trabajo ya sea por diferentes factores sea por tiempos cortos, prolongados o al finalizar la jornada laboral, los escritorios deben permanecer libres de documentos físicos haciendo énfasis en medios extraíbles que contengan información pública ya sea clasificada o reservada, por lo que estos deben guardarse en lugares seguros y bajo medidas de seguridad evitando cualquier riesgo de pérdida de esta.

.

- Cada puesto de trabajo debe permanecer limpio y ordenado siendo los primeros responsables cada uno de los funcionarios asignados a los puestos de trabajo.
- En los procesos de impresiones, copias o digitalización de información pública independientemente del carácter que tenga no deben permanecer en dichos dispositivos por lo que se deben retirar al terminar el proceso realizado.
- Los diferentes dispositivos como impresoras, escáner y cualquier otro que se encuentre en la estación de trabajo debe permanecer limpios de cualquier documento.
- Los gabinetes, cajones, gavetas o archivadores donde se guarden documentos o los diferentes medios extraíbles que contienen la información pública ya sea pública o de índole reservado deben estar guardadas con llave durante los recesos prolongados al igual que al finalizar las jornadas de trabajo.
- En el escritorio del computador (pantalla de inicio) no debe guardarse ningún tipo de archivo más que los accesos directos a las aplicaciones que se necesiten por quien opera u operen el equipo en caso de ser más de una persona la autorizada para usar el dispositivo.
- Los documentos electrónicos que se generen ya sean por funcionarios o contratistas de la entidad según sea clasificación de la información y si se dispone deberán realizar el guardado exclusivamente en los dispositivos de almacenamiento autorizados para ellos, como en un servidor local o servicio en la nube, por lo que debe garantizar que solo en estos sea guardada.
- Todo equipo igual que impresoras, escáner, fotocopiadoras entre otros que en caso de no ser usado por un tiempo prolongado deben apagarse.

#### 5.4.2.3 Políticas protección de datos y manejo de la información.

**Objetivo:** Garantizar de manera eficiente los niveles de seguridad para evitar la alteración, consultas o usos inapropiados de la información.

**Alcance:** Todos los servidores públicos y terceros que manejen información de la entidad.

**Descripción de la política:**

- Se debe garantizar que los ciudadanos y servidores públicos tengan acceso a la información a través de procesos seguros y solo a la que tienen permitido acceder ajustado al artículo 21 del Decreto Reglamentario 1377 de 2013.
- La información y datos suministrados por los ciudadanos ya sea de manera digital o en físico debe tener copias seguridad que garanticen su confidencialidad e integridad.
- Los ciudadanos tienen el derecho a rectificar sus datos personales que residen en la entidad, así como limitar la divulgación de dicha información bajo la normativa legal vigente.
- La información que reside en la entidad podrá ser usada para minería de datos siempre que se garantice su integridad, seguridad y disponibilidad, solo se usaran para efectos de mejora de servicios como análisis estadísticos, focalización de sectores entre otros, siempre que no tenga un carácter de confidencial, para tal caso esta información solo podrá usarse en los estrictamente necesario.
- El tratamiento de datos personales que se dan en el ejercicio propio de las funciones legales no se requerirá la autorización previa de las personas, no obstante cuando dichos datos no correspondan a sus funciones se deberá obtener autorización en un documento donde el titular da el consentimiento claro para el manejo de sus datos, ya sea en medio físico o electrónicos, este último a través diferentes canales de comunicaciones que existen, en caso de respuesta negativo o no tenerla nunca se podrá almacenar o utilizar su información, salvo los que permite la ley Colombia.

- La entidad debe garantizar el derecho a la consulta, eliminación de datos personales que residen en ella acordes a la ley, para lo cual debe habilitar los medios de comunicación físicos o electrónicos o el que se considere, siempre que garantice la seguridad e integridad en estos canales, para la pertinente entrega de la información de los titulares de la información.
- En los equipos, dispositivos, plataformas u otros elementos que maneje información que utilice la entidad, no deberá haber información de carácter personal que no tenga relación con las funciones o procesos de la entidad, en caso de tener dicha información será responsabilidad de los servidores públicos lo que ocurra con ella.
- Se debe garantizar que la información que reside en la entidad o en terceros, que son utilizadas en el marco de sus asignaciones no sufran ningún tipo de alteración, pérdida, consulta, uso o acceso no autorizado, que termine afectando a los titulares de la información o la entidad.
- La entidad debe garantizar a plenitud los derechos de los titulares de los datos personales establecidos la ley 1581 de 2012.

#### 5.4.2.4 Política de copias de seguridad.

**Objetivó:** Realizar y comprobar la integridad de las copias de seguridad garantizando la disponibilidad, integridad y seguridad de la información, como la continuidad de los procesos.

**Alcance:** Todos los servidores públicos que tengan información confidencial y esencial para la entidad en cada uno de los procesos que se llevan a cabo en ella.

**Descripción de la política:**

- La entidad debe establecer el procedimiento para realizar la copia de seguridad, así como el cronograma según el activo de información, permitiendo siempre ante cualquier incidente que se pueda presentar una continuidad del negocio.

- La entidad debe definir el tipo de Backups que requiera la información según sea el activo, para lo cual debe determinar el periodo de caducidad de las copias de seguridad, el borrado de las mismas, la ubicación de ellas, quienes son los responsables de realizarlas, quienes tienen acceso y debe garantizar la fiabilidad y consistencia de estas.
- Según el nivel de la información la copia de seguridad se debe garantizar su cifrado más cuando sea en dispositivos extraíbles como USB, discos duros, DVD u otro medio extraíble, si la copia de seguridad es en la nube se debe revisar el nivel de cifrado de las copias tengan un alto grado de confidencialidad, así como la disponibilidad y su integridad.

#### 5.4.2.4 Política de Autenticación de los Usuarios

**Objetivo**: Garantizar que todos los servidores públicos, contratistas o terceros que requieran por sus funciones ingresar a las instalaciones físicas o lógicas de la entidad tengan responsabilidades, como acceso a la información que solo le competen junto a la responsabilidad que conlleva el correcto uso de los usuarios y contraseñas, del personal debidamente autorizado.

**Alcance**: La política de autenticación de usuarios será aplicada a las diferentes áreas que manejan la información, tienen la responsabilidad de guardar y procesarla, así como del profesional encargado de la seguridad de la información de la entidad o quien tenga sus funciones.

**Descripción de la política:**

- La entidad debe establecer los perfiles de acceso a los diferentes activos de información de los Servidores públicos y contratistas, garantizando que solo accedan a la información autorizada.
- Se debe establecer accesos según las capacidades de los equipos y aplicaciones implementando autenticaciones de doble factor dando mayor seguridad, así como el establecimiento bitácoras de acceso ya sea físicas o

digitales a través de los logs de los sistemas o lo que estén acorde a los recursos de las entidades.

- Se debe garantizar la aplicabilidad de la política de contraseña o similar.
- El acceso a la red de la entidad debe realizarse con medidas de seguridad, tales como ingreso por MAC, contraseña y usuario o cualquier otro mecanismo de seguridad que evite el ingreso de intrusos a la red de la entidad.
- Se debe realizar un cronograma de auditoria para establecer falencia en cualquier tipo de autenticación desde usuario, equipos, ingreso a plataformas, software u cualquier otra actividad que se requiera de métodos de seguridad para su ingreso.

#### 5.4.2.5 Política De Uso Software y derechos de autor.

**Objetivo**: Garantizar el cumplimiento de las obligaciones legales, reglamentarias y morales de la sociedad, relacionadas con los derechos de autor que poseen los diferentes elementos que intervienen en los procesos de la entidad.

**Alcance**: Se encargará de su aplicabilidad los responsables del área de informática, así como control interno junto con todos los servidores públicos que deben garantizar el cumplimiento de ella.

**Descripción de la política:**

- La entidad debe tener un inventario de software con los diferentes tipos de licencia que se tienen, así como el registro de ellas, las cuales se debe garantizar también su seguridad, para que no sean reutilizadas en otros equipos salvo si su licencia lo permite.
- La entidad utilizara software acorde a las necesidades de esta, bajo la disponibilidad de los recursos que se tengan, por eso se debe priorizara el software freeware y tenga el mismo beneficio o similar al de licencia shareware.

- El software donado se debe establecer su uso y condiciones en que se puedan dar, sin que esto implique cedérselo a terceros salvo casos específicos.
- Los Servidores públicos o terceros que tengan licencia de un software, que por cuestiones de sus labores necesiten instalarlo en equipos de la entidad deberán notificar y solicitar la instalación, dejando claro el objetivo, así como las actividades a desarrollar con él, se determinara que poseen las licencias para su uso.
- Todo software utilizado en la entidad se debe verificar su procedencia y que cuente con las respectivas licencias garantizando los derechos de autor.
- Siempre que un funcionario o contratista autorizado instale un software en un equipo institucional o en un equipo personal para atender funciones de la entidad debe revisar que posee la autorización para su uso de acuerdo a la licencia que tiene.
- La disposición final de las licencias del software debe considerarse acorde a su tipo, evaluando el procedimiento a desarrollar como almacenamiento, destrucción o en caso que lo permita cederla a terceros para su utilización.
- Determinar las sanciones disciplinarias que conlleve el incumplimiento en la instalación de software no autorizado principalmente pirata.
- Establecer mecanismos de seguridad que evite la instalación de software no autorizado.
- La entidad debe realizar y establecer un cronograma de auditorías de software instalado, para tener control y aplicar las respectivas sanciones a los funcionarios que incumplan, así como las respectivas correcciones para evitar que se repita.
- La instalación de software con licencia freeware debe cumplir con un proceso que garantice que este no trae ningún tipo de código malicioso o genere una vulnerabilidad en el sistema.

- Tener establecido los procedimientos operacionales y responsabilidades garantizando la operación correcta de la información bajo el estándar ISO 27001 que garantice las restricciones en la instalación de software.
- Establecer un marco de sanciones disciplinarias que se deriven por el uso de software ilegal o no autorizado, con el establecimiento de las diferentes responsabilidades que conllevan desde las pecuniarias hasta las penales.
- La entidad debe garantizar que toda la producción de información que se de en ella para uso propio o de la comunidad en general cumpla con las condiciones de derechos de autor.
- Los Servidores públicos, contratistas o terceros se deben capacitar para que tengan conocimiento en los derechos de autor garantizando el cumplimiento de la ley.
- La violación de los derechos de autor a causa de terceros en la entidad será responsabilidad de ellos, el cual responderá por todas implicaciones económicas y legales que puedan darse por su mal proceder.
- La utilización de información por parte de los Servidores públicos, contratistas u otros en el desarrollo de sus actividades debe estar en el marco de la legalidad, por lo que la utilización de imágenes, música, videos, citas de autores, software entre otros debe estar bajo el marco de uso libre o tener expreso los derechos de autor para su utilización.
- La entidad no se hace responsable por lo contenidos, datos e informaciones que puedan producir sin el debido consentimiento de los responsables de la alcaldía tales como los Servidores públicos, contratistas u otros designados para ello.
- Ante cualquier inquietud sobre la utilización de información se debe consultar sus derechos de autor y si no se pueden establecer se deberá abstener de usarla.
- La entidad debe realizar los diferentes procesos que se requieran en caso de tener producciones propias para que estas estén bajo la protección de los derechos de autor.

- La explotación o utilización de manera legítima de cualquier tipo de obra, software u cualquier objeto que esté dispuesto a derechos de autor y aunque estos no estén registrados se debe tener autorización de sus autores para la utilización.
- Todo lo relacionado con el uso de TIC dentro de la entidad u en cualquier proceso que con lleve a las actividades debe estar en el marco de derechos de autor.

#### 5.4.2.6 Política De Controles Criptográficos

**Objetivo**: Garantizar que la información se encuentre debidamente protegida, en especial la catalogada como confidencial, que permita ser trabajada de manera segura en los diferentes procesos donde se necesite garantizando su confidencialidad, integridad y su disponibilidad.

**Alcance:** La Política de Controles Criptográficos será aplicada por el área de Informática en colaboración con todas las áreas donde se requiera su implementación, así como de contratistas y terceros que manejen la información de la entidad y que tenga carácter de confidencial.

**Descripción de la política:**

- Implementar los estándares que permitan el uso de sistemas y técnicas criptográficas para la protección de la información, que garanticen proteger la confidencialidad, su autenticidad e integridad de la información de la entidad.
- La entidad implementara y diseñara un marco que regule el uso de controles criptográficos, que permita tener la información protegida en los diferentes procesos que se llevan a cabo dentro de la entidad al igual que fuera de ella, garantizando a través de mecanismos de encriptación estos den seguridad en el resguardo, almacenamiento y transporte, esto complementado con la política de control de acceso.

- En caso de que se requiera guardado de contraseñas, claves o similares se debe garantizar que dicha información este encriptada.
- Los contratistas o terceros que manejen información de la entidad deben garantizar su confidencialidad, integridad y disponibilidad a través de mecanismos criptográficos, los cuales deberán implementar según las capacidades, en caso de no tener dicha capacidad deben solicitar al área en cargada de la entidad asesoría, el desconocimiento no lo excluye de la responsabilidad legales y penales por la pérdida o acceso indebido de la información por terceros.
- El área encargada de la informática de la entidad implementara estándares para los controles criptográficos que cumplan con la normativa legal vigente.

#### 5.4.2.7 Política de teletrabajo y/o trabajo remoto.

**Objetivo:** Garantizar la aplicación de esta modalidad de trabajo en marcada en la ley, garantizando la protección de la información que se maneja por medio de esta modalidad.

**Alcance:** Todo servidor público o tercero que permita la ley para aplicar a esta modalidad de trabajo.

**Descripción de la política:**

- La entidad debe garantizar que las personas que vayan a realizar teletrabajo y/o se encuentren certificadas para realizar sus funciones.
- La entidad debe verificar y garantizar que los equipos donde se van a realizar actividades relacionadas con procesos de la alcaldía cuenten con mínimos de seguridad, como protección de antivirus el cual debe ofrecer una seguridad contra la mayoría de amenazas de la red, así como una conexión segura y estable para la realización de dichas actividades.
- Debe garantizar que el entorno laboral desde donde se realiza el teletrabajo y/o cumpla con las condiciones de seguridad laboral, así como de presentar

un cronograma de las actividades a desarrollar, el cual permita evaluar su actuar.

- Nunca utilizar los espacios dados para teletrabajo por la entidad, para otras actividades sobre todo comerciales que no tengan relación con las funciones a cumplir, menos si es en equipos de la entidad.
- El tele trabajador y la alcaldía debe cumplir con todo lo que la Ley 1221 de 2008 que regula esta actividad y cualquier otra ley, norma o resolución que lo regule.

#### 5.4.2.8 Política de Dispositivos Móviles

**Objetivo:** Garantizar las condiciones para el adecuado manejo de dispositivos móviles que no permitan la materialización de riesgos de seguridad para la información que reside en la entidad.

**Alcance:** Esta política aplica para todos los servidores públicos y terceros que utilicen dispositivos móviles en la entidad o realicen funciones que tienen que ver con ella.

**Descripción de la política:**

- Los equipos pertenecientes a la alcaldía municipal, para salir de las instalaciones deben ser autorizados por el responsable del área tecnológica o el respectivo responsable y su salida se da una vez se verifique que:
    - Tiene instalado antivirus actualizado y activado.
    - Configuración de permisos de conexión USB.
    - Restricción para la ejecución de aplicaciones
- Si posee información sensible este debe tener un sistema de autenticación ya sea contraseña, patrón, código de desbloque u otro método.
- Dentro de las instalaciones podrán hacer uso de los dispositivos personales tanto la comunidad en general como de servidores públicos, los cuales lo podrán hacer en las zonas comunes de las instalaciones de la entidad, queda

prohibido el uso de dispositivos móviles en zonas que estén marcadas con restricción incluyendo servidores públicos que no tengan autorización para ello.

- La conexión de los dispositivos móviles de la comunidad en general a la red de la entidad está totalmente prohibida salvo emergencias o con autorización de la secretaria general junto con el encargado de las Tics de la entidad.
- La conexión de los dispositivos móviles de los servidores públicos y contratistas de la entidad será aprobada por secretaria Tics o secretaria que tenga las funciones Tics, los cuales estén acorde a las funciones designadas dentro de la entidad y que no tenga otro dispositivo asignado para ello o que desde este no se pueda realizar dichas funciones.

#### 5.4.2.9 Política de contraseña

**Objetivo:** Garantizar que todos los equipos, dispositivos, aplicaciones y plataformas solo sean usados por las personas autorizados manteniendo segura la información que reside en ellos.

**Alcance:** Esta política está estructurada por los encargados de control interno junto con el área de informática, es aplicable a todos los servidores públicos, contratistas o terceros que participen en los procesos de la entidad.

**Descripción de la política:**

- Debe garantizar que las claves u contraseñas que se implementen en los diferentes sistemas tengan un mínimo de seguridad, donde se establezcan combinaciones que no permita contraseñas débiles, que presenten un mínimo de caracteres que las haga robustas y no sean fáciles de adivinar con técnicas como ingeniería social.
- Establecer el ingreso a los sistemas con factor de autenticación de doble factor en los dispositivos siempre que esto sea posible.

- Establecimiento de vencimiento de las contraseñas que obligue su cambio.
- Los servidores públicos y terceros que tengan usuarios y contraseñas de equipos, aplicaciones, plataforma entre otros, no deben transferir ni prestarlos, en caso de fuerza mayor solo en los que sea para fines de la entidad, en la brevedad se deberá cambiar la contraseña y cambios de configuraciones de seguridad si así se requiere.
- Las contraseñas de las cuentas se deben cambiar aproximadamente cada tres meses como máximo cada 3 meses cumpliendo con las características de una contraseña fuerte, teniendo mínimo 8 caracteres alfanuméricos.

#### 5.4.2.10 Política de uso de Internet.

**Objetivo:** Garantizar el correcto y buen uso del internet que vaya acorde de los procesos misionales sin poner en riesgo la información que reside en la entidad, así como ser una herramienta de mejora.

**Alcance:** Todos los servidores públicos de la entidad.

**Descripción de la política:**

- El uso del internet dentro de la entidad es exclusivamente para las actividades asignadas y no debe utilizarse para otro fin que no tenga relación con ella.
- Al usar el internet se da por entendido que son responsables de buenas prácticas en su uso, que son responsables y no puedan comprometer la seguridad de la información.
- Para enviar, descargar o visualizar información que vaya contra la moral de las personas u de la entidad está totalmente prohibido y acarreara sanciones según la afectación que se genere.
- El funcionario no deberá descargar ningún tipo de programa sin que este no tenga su debida licencia, si son archivos de imagen, música, video deben ser

de libre uso, no se pueden ningún tipo de archivo que vaya en contra de los derechos de autor.

- Los funcionarios o contratistas no deberán realizar transmisiones vía internet por los canales de comunicación oficiales, que no tengan una relación a sus funciones o en pro de la entidad debidamente justificada.
- La conexión de Internet de la entidad no puede usarse para ningún propósito con carácter comercial y menos de índole político.
- La conexión de internet de la entidad no puede ser usado para actividades privadas que no vayan acorde a la función de entidad.
- El internet puede ser usado con fines educativos o investigativos sin que coloque en riesgo la información que reside en la entidad.
- Los funcionarios o contratistas no intentaran evadir ni modificar las medidas de seguridad de la red de la entidad, así como con cualquier otro sistema que permite el acceso a internet.
- Ninguna persona que esté conectado a la red podrá interceptar su tráfico, salvo en casos aprobado para una auditoria informática y solo con fines de encontrar fallas, mas no con un interés personal o comercial, se debe garantizar que se subsanen las fallas encontradas.

#### 5.4.2.11 Política de concientización y capacitación

**Objetivo:** Capacitar y concientizar constantemente a los servidores públicos y terceros en temas de seguridad de la información.

**Alcance:** Según las disposiciones legales, así como de los requerimientos que se presenten para servidores públicos.

**Descripción de la política:**

- Implementación de estrategias y planes que permitan la concientización, la capacitación diferenciada entre el personal existente como del nuevo, que

permitan que el empleado tenga las herramientas dado un mínimo de seguridad en el diario de sus actividades, con conocimiento en la identificación de amenazas y comportamientos no deseables, entendiendo que la seguridad informática es una responsabilidad compartida y que cada uno es importante para ello.

- La entidad garantizara los espacios y tiempos para que el personal sea capacitado sin que esto signifique más carga laboral, sea para el crecimiento personal y en pro de la seguridad de la información que reside en la entidad.
- En la contratación de personal se debe tener en cuenta su perfil profesional que sea acorde a las funciones que va a cumplir, en lo posible que no requiere de nuevas capacitaciones para no incurrir en demora en la ejecución de los procesos, así como evitar el gasto y demás asociadas a este factor.

#### 5.4.2.12 Política de uso de correo electrónico

**Objetivo:** Garantizar la seguridad integridad y confidencialidad de la información que reside en los correos electrónicos.

**alcance**: Todo servidor público que tenga asignado un correo institucional o utilice uno personal para usos de la entidad.

**Descripción de la política:**

- El uso de correo electrónico perteneciente a la alcaldía municipal debe prestarse por un canal cifrado.
- Los usuarios son responsables de todas las actividades que se realicen con sus respectivas cuentas, por lo que todo contenido u información que distribuya será responsabilidad exclusiva del usuario.
- Es responsabilidad de los usuarios informar al área encargada, cuando reciba correos de tipo SPAM, correo no deseado o de dudosa procedencia.

- Está prohibido utilizar el correo electrónico con propósitos no acordes a las funciones en la entidad, la utilización para la propagación y difusión de mensajes de índole político, religioso, ofensivo o contenido inapropiado o cualquier otro tema que no tenga que ver con sus funciones.
- Para los casos en que se pierda los datos para el ingreso a la cuenta de correo debe dirigirse por escrito al área encargada para su restablecimiento.
- Las cuentas que no se utilicen en un lapso de tiempo mayor a 90 días se notificara, se debe evitar que se desactivan temporalmente en caso de que esto ocurra se debe realizar el procedimiento por el área encargada ante el ente que es el responsable del manejo del correo institucional, en caso de reincidir se estudiara la posibilidad de reasignación del correo a una dependencia que lo requiera.
- La asignación y eliminación de cuentas del sistema se realizará solo por el personal encargado.
- Los funcionarios son completamente responsables de todas las actividades realizadas con las cuentas de correo electrónico asignado.
- Las cuentas de correo son exclusivamente para el uso del personal asignado y no se pueden transferir sin aprobación del área encargada, el mal uso de estas puede ocasionar la eliminación de la cuenta por parte del administrador, siendo responsabilidad del funcionario las consecuencias de ello.
- El personal que tiene asignado correo electrónico institucional debe utilizar solo para las comunicaciones oficiales, en caso de no tener asignado uno y no existir la disponibilidad, se autoriza el uso de un correo personal.

#### 5.4.2.13 Política de Roles y responsabilidades

**Objetivo**: Garantizar que todo los servidores públicos y terceros conozca y aplique los roles y responsabilidades relacionados con la seguridad de la información.

**Alcance:** Todos los servidores públicos y terceros que tienen funciones con la entidad.

**Descripción de la política:**

- Los activos de información de la alcaldía municipal deben tener claramente identificado su propietario y su responsable, los cuales deben saber las medidas para protegerlo, siendo responsables de garantizar su confidencialidad, integridad y disponibilidad.
- La toma de decisiones sobre los activos de información de la entidad debe ser avalados por el responsable del área, ante cualquier suceso que los involucre se debe contar con autorización sea escrita o verbal según sea el caso.
- Los usuarios deben de informar en el momento que tengan acceso a contenidos o servicios dentro de la entidad para los cuales no están autorizados.

#### 5.4.2.14 Política seguridad de la información en el talento humano.

**Objetivo:** Garantizar la seguridad de la información antes, durante y después de la relación contractual que tienen los servidores públicos o terceros con la entidad.

**Alcance:** La política será aplicada a todos los servidores públicos como terceros que por sus funciones tengan acceso a información de la entidad.

**Descripción de la política:**

- La entidad debe verificar todos los antecedentes del personal a contratar, que cumpla con todos los requisitos de ley que se requieren para el cargo.
- Se establecerán actas de entrega y devolución con los dispositivos a si como plataformas que tengan en relación con el cargo a desempeñar permitiendo tener un seguimiento desde la entrega hasta la devolución al finalizar el contrato.

- En caso de que un servidor público, efectúe un cambio de posición dentro de la entidad, se debe revisar el manual de funciones para el nuevo cargo y modificar o mantener los privilegios de acceso a los sistemas de información en los que esto ocurra.
- El área encargada de talento humano debe realizar los diferentes procesos de desvinculación de los servidores públicos, contratistas o terceros, así como de las licencias, vacaciones o cambios en los puestos de trabajo que realizan al interior a través de mecanismos como paz y salvo o el que permita un control, con aprobaciones de áreas como la encargada de la informática o el encargado de inventario de la entidad.

#### 5.4.2.15 Políticas De Seguridad Física.

**Objetivo:** Garantizar que las instalaciones donde residen los recursos tecnológicos y demás elementos que resguardan o tienen información, tenga una protección adecuada, logrando la preservación de la confidencialidad, integridad y disponibilidad de la información que reside en la entidad.

**Alcance:** El área tecnológica, los encargados de la seguridad de la entidad, así como todo los Servidores públicos, contratistas y comunidad en general.

**Descripción de la política:**

- La entidad debe garantizar los espacios para que los servidores públicos o cualquiera persona que necesite utilizar las instalaciones puedan realizar los ingresos y salidas de manera adecuada y con seguridad.
- Los Servidores públicos o contratistas deben identificarse dentro de la entidad a través de carnets o cualquier otro distintivo que permita a los ciudadanos y los demás Servidores públicos identificar quienes pertenecen a la entidad o realizan funciones en ella.
- La entidad debe identificar las limitaciones de acceso a los Servidores públicos según sus funciones, así como a los visitantes, garantizando que

solo el personal autorizado tenga acceso a los equipos e información según sea su función.

- La entidad debe garantizar las condiciones físicas y medioambientales que garanticen la protección y operación correcta del personal, así como de los dispositivos bajo las normas que lo regulan.
- Debe garantizar la seguridad de los equipos y elementos que en esta residen a través de diferentes herramientas como circuitos cerrados de televisión, controles de acceso a través de diferentes medios electrónicos o con talento humano como celadores o cualquier otro mecanismo, que garantice mayores niveles de seguridad protegiendo la información y equipos que en ella están.
- Todas las actividades de mantenimiento se deben garantizar que sean realizadas por el personal idóneo, el cual debe ser autorizado y debidamente identificado, se debe establecer un control que sirvan como herramienta de información y seguimiento.
- Se debe señalizar las áreas donde solo pueda ingresar personal de la entidad o contratistas con los respectivos permisos, llevando anotaciones de personas en sitios no autorizados, por lo que los ciudadanos y servidores públicos sin autorización no deben intentar ingresar a estas áreas.
- La entidad debe revisar periódicamente y tomar medidas en los diferentes tipos de accesos con los que cuenta, en búsqueda de accesos físicos que permitan el ingreso a ella de manera irregular.
- La entidad debe restringir el acceso físico del personal a los equipos de cómputos más en las dependencias donde se procesa información sensible o contenga información en otros medios como archivo donde radican todos los documentos oficiales.

#### 5.4.2.16 Política de cumplimiento de disposiciones legales.

**Objetivo:** Asegurar que la entidad cumpla con el marco normativo, regulaciones y demás requisitos legales que corresponda a la actividad que se realiza en ella.

**Alcance:** La política será aplicada a todos los servidores públicos y terceros.

**Descripción de la política:**

- La entidad deberá identificar los requisitos legales, los contractuales y los reglamentarios en los que tenga obligación por su función, a los cuales debe garantizar que no se de incumplimiento a ninguno de ellos.
- La entidad debe evaluar los riesgos que existen y la gravedad que estos tiene junto a la probabilidad de que estos se produzcan.
- Debe garantizar la protección de los datos personales, en el manejo como en la cesión a terceros bajo criterios que garanticen que los derechos de las personas no sean perjudicados.
- La entidad debe garantizar el cumplimiento legal en la compra de equipos y software que requiera la entidad o compras realizadas con disposición final a terceros.
- La entidad establecerá un marco para asegurar que no suceda incumplimientos y en eventos de presentarse deberá garantizar el registro de ello para la toma de decisiones que permitan la no repetición de estos.

### 5.4.3 Guías del MinTic para mejor los sistemas de seguridad de la información.

El saber en qué estado están implementadas las guías es recomendable como control interno si es que este no existe, que por funcionamiento debería tener dicha oficina, la cual debería tener un proceso estipulado para ello, en caso de no existir se debería implementar, para estar en una constate retroalimentación de los propósitos de las guías.

La importancia de conocerlas se puede observar en cada una de ellas las cuales se encuentran en la página oficial del Ministerio de Tecnologías de la Información y las Comunicaciones, en la sección Modelo de Seguridad el cual busca según el MinTic “A nivel metodológico es importante tener presente que el Modelo de Seguridad y Privacidad de la Información – (MSPI) cuenta con una serie de guías anexas que

ayudarán a las entidades a cumplir lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo",[59] donde se pueden encontrar, y que se pueden descargar en el siguiente enlace https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/ para el entendimiento se relacionan las guías en la siguiente tabla.

Tabla 6 Guías del MinTic para la implementación de MSPI

| No de guía | Nombre |
|---|---|
| 1 | Metodología de pruebas de efectividad |
| 2 | Política General MSPI v1 |
| 3 | Procedimiento de Seguridad de la Información |
| 4 | Roles y responsabilidades |
| 5 | Gestión Clasificación de Activos |
| 6 | Gestión Documental |
| 7 | Gestión de Riesgos |
| 8 | Controles de Seguridad de la Información |
| 9 | Indicadores Gestión de Seguridad de la Información |
| 10 | Continuidad de Negocio |
| 11 | Análisis de Impacto de Negocio |
| 12 | Seguridad en la Nube |
| 13 | Evidencia Digital (En actualización) |
| 14 | Plan de comunicación, sensibilización, capacitación |
| 15 | Auditoria |
| 16 | Evaluación de Desempeño |
| 17 | Mejora continua |
| 18 | Lineamientos terminales de áreas financieras de entidades públicas |
| 19 | Aseguramiento de protocolo IPv4_IPv6 |
| 20 | Transición IPv4_IPv6 |
| 21 | Gestión de Incidentes |
| | Modelo de Seguridad y Privacidad |
| | Instrumento de Evaluación MSPI |

Fuente: República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. Modelo de Seguridad [En línea]. Bogotá: 2019. 1 p. [Consultado: 4 de marzo de 2020] Disponible en https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

[59] República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. Modelo de Seguridad [En línea]. Bogotá: 2019. 1 p. Disponible en https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Las anteriores guías y documentos, así como el instrumento de evaluación que aporta el MinTic son herramientas que permiten subsanar riesgos no solo a los asociados al factor humano, por lo que la aplicación de estas en las entidades debe ser de manera efectiva, donde se permite tener lineamientos de buenas prácticas en pro de mejorar la seguridad de la información, que aporta cada una de ellas desde técnicos hasta procedimentales, por lo que la existencia de estas deberían verse reflejadas en la seguridad que existen en las diferentes entidades.

Se deberían estar aplicando bajo la directriz del Ministerio de Tecnologías de la Información y Comunicación el cual tiene un equipo dispuesto para esto, por lo que el que no estén en aplicabilidad es un alto riesgo más cuando en la guía de Instrumento de Evaluación MSPI sobre la aplicabilidad de los controles del Anexo A, indica que para 2020 se debe llegar al 100% como se ve en la figura 42 lo cual no corresponde a la realidad más con los problemas encontrados en la recolección

de información, los resultados ante auditorias y realización de pentesting podría dar más luces de la realidad de la seguridad de la información en este tipo de entidad.

Figura 41 Implementación del Anexo A.

| TIPO DE ENTIDAD | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|
| De Orden Nacional | 40% | 60% | 80% | 100% | Mantener 100% | Mantener 100% |
| De Orden Territorial A | 35% | 50% | 80% | 100% | Mantener 100% | Mantener 100% |
| De Orden Territorial B y C | 10% | 30% | 50% | 65% | 80% | 100% |

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. Gráfica 4 - Avance PHVA. Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información versión 1.0 2017

La anterior figura indica que las entidades del estado deberían de estar preparadas en todo sentido para enfrentar los riesgos de seguridad a través de los controles implementados, lo cual se debería demostrar en el próximo informe del Centro Cibernético Policial con la disminución de la perdida de dinero de las entidades.

## RECOMENDACIONES

- ✓ Realizar capacitaciones específicas y efectivas segregadas para los diferentes empleados que componen dichas entidades, implementaciones de las políticas con compromiso en su aplicabilidad, teniendo un capítulo muy especial en el tema de la ingeniería social, que es la mayor amenaza que se tiene, entre otros temas propios de cada entidad.

- ✓ Se debe establecer los perfiles a los cuales se les pueden asignar funciones acordes a su preparación, para que no se tengan eslabones débiles en los procesos a implementar, mantener o mejorar, en la seguridad de la información como en cualquier proceso que tenga interacción.

- ✓ Debe cambiar la mentalidad en los temas de tecnología, ya que este es transversal a la mayoría de los procesos que se realizan en las entidades y que van en pro de su desarrollo, haciéndolos más eficientes por lo que se debe ver que el presupuesto que se destina a esto es una inversión más que un gasto.

- ✓ Atender y aplicar los lineamientos que da el ministerio de las tecnologías para su implementación tanto desde el factor humano como el de infraestructura, para ser unas entidades inteligentes al servicio de las comunidades, como su fin garantizando procesos transparentes que no es más que procesos confiables y seguros.

- ✓ Establecer un proceso de inversión a corto, mediano y largo plazo que permita la adquisición de equipos que permitan garantizar desde la parte

física un mínimo de seguridad, ofreciendo un margen a la seguridad del sistema con la mitigación de errores debidos al factor humano.

- ✓ Realizar pruebas para demostrarle a los empleados que estos pueden ser víctimas de robo de información a través de diferentes herramientas, como ingeniería social o ataques Phishing, las cuales se deben realizar en entornos controlados y bajo parámetros de seguridad identificables y seguros para la entidad y los propios empleados.

- ✓ Realizar retroalimentaciones de los diferentes controles que se implementen que permita evaluar si aportan o no a la seguridad de la información, sin que estos terminen siendo una carga más para las actividades de las entidades.

- ✓ Establecer programas de inducción para los nuevos empleados o contratistas que permitan concientizarlos sobre sus responsabilidades y compromisos con las entidades.

- ✓ Establecer los canales de comunicación con los diferentes organismos colombianos encargados de la ciberseguridad, para establecer estrategias que mejoren la seguridad de cada una de las entidades.

# CONCLUSIONES

La mejor manera de prevenir riesgos y encontrar vulnerabilidades es tener un SGSI para lo cual el Mintic tiene una estrategia que permite a las diferentes entidades llegar a esto, a través de las diferentes guías que han diseñado aplicando metodologías como son la ISO 27001 y marcos como COBIT e ITIL que si se aplicaran según dichas guías los riesgos asociados a las personas se mitigarían en gran medida, teniendo como obstáculo para su aplicabilidad la falta de personal capacitado o con conocimientos en el área, siendo esto el mayor riesgo de seguridad, por lo que la aplicabilidad de otra metodología es muy difícil que se de en este tipo de entidad.

En la recolección de información se determinó que el conocimiento de los empleados de las entidades de categoría 6 es mínimo y por lo tanto es un riesgo para la seguridad de la información de reside en sus sistemas, lo que implicaría posible pérdida de su recurso más valioso como es la información y también la perdida de recurso presupuestal, lo que afecta no solo procesos internos de las entidades sino a terceros con posibles implicaciones legales y económicas, por lo que debe ser una prioridad mejorar los conocimientos de su personal.

Existen diferentes causas en la generación de los riesgos y vulnerabilidades en la seguridad de la información asociados al factor humano, entre las principales se encuentra la falta de compromiso de la alta dirección y personal en general, ya que muchas entidades no cuentan con personal con conocimientos en el área, los cuales puedan aplicar las guías del MinTIC así como las diferentes estrategias que formulan, permitiendo la eliminación y mitigación de riesgos y vulnerabilidades no solo a las asociadas al factor humano, por lo que este tipo de entidad debe contemplar en su personal un equipo que esté a cargo en liderar y gestionar la estrategia de gobierno digital.

El factor humano es uno de los mayores riesgos de la seguridad de la información esto debido a diferentes razones que van desde culturales, educativas,

organizacionales, entre otras, por lo que la aplicación de políticas de seguridad de la información debe contemplar diferentes aspectos para que sean de fácil entendimiento e implementación, y logren mitigar los riesgos.

La falta de capacitaciones efectivas en los empleados es un factor decisivo en una entidad para que ellos no sean una vulnerabilidad y por ende un factor de riesgos para los sistemas de información, el propósito de estas debe ser en caminarlos a ser un ítem más en los sistemas de protección de la información.

# 6. BIBLIOGRAFÍA


Alemán, Helena,. Rodríguez Claudia Metodologías Para el Análisis de Riesgos en los SGSI [En línea] 2015. Disponible http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1754

Ashford, Warwick. La gente puede ser el eslabón más fuerte en la ciberseguridad, dice NCSC. [En línea] searchdatacenter. 2017, Disponible en https://searchdatacenter.techtarget.com/es/cronica/La-gente-puede-ser-el-eslabon-mas-fuerte-en-la-ciberseguridad-dice-NCSC

Borrero, Cortés, Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia [En línea:] Revista de Derecho Comunicaciones y Nuevas Tecnologías Universidad de los Andes. 2015. Disponible en https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics227.pdf

Cancino, Héctor. Factor humano: ¿cómo combatir al eslabón más débil en la cadena de la ciberseguridad? Citado por Cecilia Pastorino [En línea] Revista AméricaEconomía 2019 Disponible en https://tecno.americaeconomia.com/articulos/factor-humano-como-combatir-al-eslabon-mas-debil-en-la-cadena-de-la-ciberseguridad

Ccn-cert El 95 por ciento de las incidencias de seguridad se deben a errores humanos internet [En línea] CCN-CERT2014 Disponible en https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/1152-el-95-por-ciento-de-las-incidencias-de-seguridad-se-deben-a-errores-humanos.html

Ccn-cert MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de InformaciónLibro I - Método[En línea] Ministerio de Hacienda y Administraciones Públicas Gobierno de España. 2019. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Centro cibernético Policial, Policía Nacional, DIJIN. costos del cibercrimen en Colombia 2016-2017 [En línea] Policía nacional Direccion de investigación criminal e INTERPOL. 2017. Disponible en https://caivirtual.policia.gov.co/sites/default/files/costos_del_cibercrimen_v4.pdf

Centro cibernético Policial, Policía Nacional, DIJIN. costos del cibercrimen en Colombia 2016-2017 [En línea] Policía nacional Dirección de investigación criminal e INTERPOL. 2017. Disponible en

https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf

CONGRESO DE COLOMBIA, LEY 1273 DE 2009 (Enero, 05, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. El Congreso. Bogotá D.C., 2009.

CONGRESO DE COLOMBIA, LEY 136 DE 1994(junio, 02, 1994). Por la cual se dictan normas tendientes a modernizar la organización y el funcionamiento de los municipios. El Congreso. Bogotá D.C., 1994.

CONGRESO DE COLOMBIA, LEY 1551 DE 2012 (Julio, 06, 2012). Por la cual se dictan normas para modernizar la organización y el funcionamiento de los municipios. El Congreso. Bogotá D.C., 2012.

Departamento Administrativo Nacional de Estadística. Boletín técnico FORMACIÓN PARA EL TRABAJ O[En línea]. 2016. Disponible en https://www.dane.gov.co/files/investigaciones/boletines/ech/formacion/GEIH_FormacionTrabajo_abr_jun15.pdf

EL CONGRESO DE COLOMBIA, LEY 1955 DE 2019 (25 de mayo de 2019). Plan Nacional de Desarrollo 2018-2022. “Pacto por Colombia, Pacto por la Equidad”. Congreso.

Erhardt, Wolfgang. Identifica los diferentes tipos de phishing [En línea] 2017. Disponible en https://www.forbes.com.mx/identifica-los-diferentes-tipos-de-phishing/

Eset , Eset security report Latinoamérica [En línea]. 2018. 16 p. Disponible en https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

ESET, LLC y ESET, spol. s.r.o. Compare la seguridad de su empresa con las de su país [En línea] ESET 2019 1 p. Disponible en https://security-report.eset-la.com/

Función Pública. Concepto 20101 de 2016 Departamento Administrativo de la Función Pública [En línea]. El mundo. 2015 Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=68295

Gobierno de España, Normas ISO sobre gestión de seguridad de la información [En línea] 2014. Disponible en http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

González, Cristián. citado por AméricaEConomía.com. 4 tips para elaborar estrategias de ciberseguridad [En línea]. 2019 Disponible en https://mba.americaeconomia.com/articulos/notas/4-tips-para-elaborar-estrategias-de-ciberseguridad

Gonzalez, Hugo. GESTION DEL RIESGO – ISO 31000 [En línea] 2016. Disponible en https://calidadgestion.wordpress.com/2016/10/28/gestion-del-riesgo-iso-31000/

Grupo Bancolombia. El eslabón suelto de la ciberseguridad: el empleado [En línea]. Grupo Bancolombia. 2018. Disponible en https://www.grupobancolombia.com/wps/portal/empresas/capital-inteligente/tendencias/innovacion/el-eslabon-suelto-ciberseguridad

IBM Security X-Force Threat Intelligence Index2019 [En línea] IBM 2019 Disponible en https://www.ibm.com/downloads/cas/ZGB3ERYD

Iso27000.es ¿Qué es un SGSI? [En línea] 2005 Disponible en http://www.iso27000.es/sgsi.html

Isotools. COSO como metodología de gestión de riesgo [En línea] Isotools 2015 Disponible en https://www.isotools.org/2015/01/12/iso-90012015-coso-como-metodologia-gestion-riesgo/

Ministerio de defensa, colCERT, Acerca de colCERT [En linea] Ministerio de defensa. 2017, 1 disponible en http://www.colcert.gov.co/?q=acerca-de

Ministerio de Tecnologías de la Información y las Comunicaciones. Despacho de la Ministra Seguridad y Privacidad de la Información. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Versión 1.0 [En línea]. Grupo Bancolombia. 2018 Disponible en https://www.mintic.gov.co/portal/604/articles-100251_plan_seguridad_privacidad_informacion_2019.pdf

Nee, Lee 2017 Threat Landscape Survey:Users on the Front Line[En línea] SANS Institute 2017. Disponible en https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910

Pacheco, Federico. La importancia de un SGSI[En línea]. 2010. Disponible en https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

Panda Security. ruityArmor: ciberdelincuentes que aprovechan las vulnerabilidades de Windows [En línea]. 2019 2p. disponible en https://www.pandasecurity.com/spain/mediacenter/seguridad/ciberdelincuentes-aprovechan-vulnerabilidades-windows/

Performia Colombia. La rotación de personal perjudica significativamente a las empresas [En línea] 2016 Disponible en http://www.performia.com.co/la-rotacion-

de-personal-perjudica-significativamente-a-las-empresas

Periódico digital El mundo. Facebook reconoce la filtración de datos de más de 120 millones de usuarios [En línea]. El mundo. 2018 Disponible en https://www.elmundo.es/tecnologia/2018/06/30/5b35f2f4468aeb22438b457d.html

Prieto,José Luis ingeniería social En línea] Disponible en http://www.tugurium.com/gti/termino.php?Tr=social%20engineering&Tp=T&Or=0

Real Academia Española, conocimiento [En línea] Disponible en https://dle.rae.es/conocimiento

República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. MANUAL DE GOBIERNO DIGITAL Implementación de la Política de Gobierno Digital Decreto 1008 de 2018 [En línea]. Bogotá: 2018. Disponible en https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. AGENDA ESTRATÉGICA DE INNOVACIÓN:CIBERSEGURIDAD [En línea]. Bogotá: 2014. Disponible en https://mintic.gov.co/portal/604/articles-6120_recurso_2.pdf

República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. MANUAL DE GOBIERNO DIGITAL Implementación de la Política de Gobierno Digital Decreto 1008 de 2018 (14 de junio de 2014) [En línea]. Bogotá: 2018. Disponible en https://www.mintic.gov.co/portal/604/articles-5271_Peti.pdf

República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. Decreto único reglamentario del sector de tecnologías de la información y las comunicaciones DECRETO 1078 DE 2015 (26 de mayo 2015) [En línea]. Bogotá: 2018. Disponible en https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. TÉRMINOS Y CONDICIONES DE USO DEL CORREO ELECTRÓNICO[En línea]. Bogotá: Disponible en https://estrategia.gobiernoenlinea.gov.co/623/articles-9410_politica_correo.pdf

Revista Dinero. Los sectores económicos más impactados por el cibercrimen en Colombia Citado por La firma de seguridad informática Digiware. [En línea] Revista Dinero. 2017, 1 p. Disponible en https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321

Sun ,Tzu. El arte de la guerra, siglo V a. C. antigua china

Terrill, Christie. What You Need To Know Now About Cybersecurity And Social Media, [En linea]. Forbes Media LLC. 2017, 2p. Disponible en https://www.forbes.com/sites/christieterrill/2017/04/28/what-you-need-to-know-now-about-cybersecurity-and-social-media/#6c98b6793a16

Tomáš, Foltýn. 773 millones de direcciones de correo y 21 millones de contraseñas fueron filtradas [En línea]. 2019. disponible en https://www.welivesecurity.com/la-es/2019/01/17/millones-direcciones-correo-contrasenas-filtradas/

# Anexos

## Formato de encuesta.

*Anexo encuesta tipo 1*

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA - UNAD
Escuela De Ciencias Básicas, Tecnología E Ingeniería (Ecbti)
Especialización En Seguridad Informática
Proyecto De Seguridad Informática I

Encuesta tipo 1

*Fecha:* _____/_____/_____
*Entidad:* _____
*Nombre:* _____
*Cargo:* _____

**Objetivo de la encuesta.**

Analizar el grado de conocimiento que tienen los empleados de una entidad de categoría 6 en cuanto a la seguridad de la información.

Su vinculación con la entidad es de

Planta. ___ Contrato___ otro ____

1. **¿Ha escuchado hablar de las siguientes entidades?**
   - CSIRT-PONAL
     SI __ NO ___
   - Centro Cibernético Policial (CCP)
     SI __ NO ___
   - Comando Conjunto Cibernético de las Fuerzas Militares CCOC
     SI __ NO ___
   - colCERT Grupo de respuesta a emergencias cibernéticas de Colombia
     SI __ NO ___

2. **¿Sabe que es una norma o política de *seguridad informática?***

   SI __ NO ___

3. **¿Cuál cree que es la mayor amenaza que se presenta en internet?**
   - ☐ Robo de información personal
   - ☐ Correo basura
   - ☐ Programas espías
   - ☐ Estafas, ingresar a sitios que cree son legítimos.
   - ☐ Virus
   - ☐ Ingresar a sitios nocivos
   - ☐ Otros

4. **¿Sabe que es?**
   - Un Virus. SI __ NO __
   - Malware. SI __ NO __
   - Spyware. SI __ NO __
   - Ransomware. SI __ NO __

Página **1** de **3**

- Gusano. SI __ NO __
- Troyano. SI __ NO __
- Antivirus. SI __ NO __

5. **¿De los que selecciono en la pregunta anterior sabe cómo funcionan?**
   SI __ NO ___

6. **¿Usted cree que los virus se pueden propagar a través de?**
   - ☐ Correo electrónico
   - ☐ Redes sociales
   - ☐ Skype
   - ☐ Servicios de la nube
   - ☐ Memorias USB

7. **¿Conoce de los controles implementando en la entidad sobre los diferentes procesos de la seguridad de la información?**
   SI __ NO ___

8. **¿Sabe qué hacer ante cualquier incidente informático que se presente?**
   SI __ NO ___

9. **¿Sabe qué pasos debe seguir ante incidentes informáticos en sus equipos de trabajo?**
   SI __ NO ___

10. **¿Utiliza redes sociales personales en las instalaciones de la entidad?**
    SI __ NO ___

11. **¿Quién es el responsable de la seguridad tanto física como lógica de los equipos donde realiza su trabajo?**
    RTA _____

12. **¿Sabe que es una contraseña fuerte?**
    SI __ NO ___

13. **¿Realiza periódicamente una copia de seguridad de los datos más importantes que tienen los dispositivos sobre los que trabaja?**
    SI __ NO ___
    - Si la respuesta fue sí en que medio realiza la copia de seguridad

    RTA _____

**14. ¿Sabe reconocer un email sospechoso?**
SI __ NO ___

**15. ¿Sabe identificar cuando una dirección URL es legitima?**
SI __ NO ___

**16. ¿Cada cuanto cambia las contraseñas de sus correos electrónicos o de los diferentes usuarios que tiene en redes sociales y otras plataformas.?**
RTA _____

**17. ¿Su equipo tiene contraseña para poder usarlo?**
SI __ NO ___

**18. ¿Con qué frecuencia utiliza Windows Update?**
- ☐ Todos los días
- ☐ 1 ves a la semana
- ☐ 1 ves al mes
- ☐ No sabe que es Windows update
- ☐ Nunca

**19. ¿Qué navegador usa normalmente?**
- ☐ Google Chrome
- ☐ Mozilla Firefox
- ☐ Internet Explorer
- ☐ Opera
- ☐ Safari

**20. ¿Actualiza el navegador o verifica que se encuentre actualizado?**
SI __ NO ___

**21. ¿Tiene software antivirus instalado en los dispositivos que utiliza en su trabajo?**
SI __ NO ___

**22. ¿Conoce la ley 1273 de 2009?**
SI __ NO ___

Gracias por su colaboración.

*Anexo encuesta tipo 2*

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA - UNAD
Escuela De Ciencias Básicas, Tecnología E Ingeniería (Ecbti)
Especialización En Seguridad Informática
Proyecto De Seguridad Informática I

Encuesta tipo 2

*Fecha:* _____/_____/_____
*Entidad:* _____
*Nombre:* _____
*Cargo:* _____

**Objetivo de la encuesta.**

Analizar el grado de conocimiento que tienen los empleados de una entidad de categoría 6 en cuanto a la seguridad de la información.

Su vinculación con la entidad es de: Planta. ___ Contrato___ otros____

1. **¿Existe personal especializado responsable de la seguridad de los equipos de la entidad?**
   SI __ NO ___
2. **¿Tiene implementado algún programa para incidentes de seguridad de la información?**
   SI __ NO ___
3. **¿Tienen programa de monitoreo de las estaciones de trabajo y red de la entidad?**
   SI __ NO ___
4. **¿Qué tipo de antivirus utilizan?**
   ☐ Licencia free
   ☐ Licencia paga
   ☐ No sabe
5. **¿Sabe que es un SGSI?**
   SI __ NO ___
6. **¿Manejan un marco de buenas prácticas para la gestión de seguridad de la información?**
   SI __ NO ___
   **¿Cuál? _____**
7. **¿Existe un programa de Ciberseguridad en la entidad?**
   SI __ NO ___
8. **¿Existe un manual de responsabilidad en la entidad sobre los incidentes Informáticos que se puedan presentar?**
   SI __ NO ___

1

9. **¿Sabe cuál es el nivel de protección de la entidad?**
   SI __ NO ___

10. **¿Utilizan sistemas de autenticación de doble factor?**
    SI __ NO ___

11. **¿La conexión a la red interna de la entidad ya sea física o inalámbrica tiene limitantes, controles para la conexión?**
    SI __ NO ___

12. **¿Los empleados tienen conectados los teléfonos a la red la entidad.?**
    SI __ NO ___

13. **¿Usted cree que Los empleados tienen la capacidad para reconocer un email sospechoso?**
    SI __ NO ___

14. **¿Tienen servidores para los diferentes servicios que se llevan a cabo en la entidad?**
    SI __ NO ___

15. **¿Tienen personal encargado para instalar o desinstalar los programas y aplicaciones informáticas en su empresa?**
    SI __ NO ___

16. **¿Conoce la ley 1273 de 2009?**
    SI __ NO ___

17. **¿Existe en la entidad un inventario de activos de información en la entidad?**
    SI __ NO ___

18. **¿Ha escuchado hablar de las siguientes entidades?**
    - CSIRT-PONAL
      SI __ NO ___
    - Centro Cibernético Policial (CCP)
      SI __ NO ___
    - Comando Conjunto Cibernético de las Fuerzas Militares CCOC
      SI __ NO ___
    - colCERT Grupo de respuesta a emergencias cibernéticas de Colombia
      SI __ NO ___

Gracias por su colaboración.