CAPÍTULO V

ESTRATEGIA PARA LA ADOPCIÓN DE UNA CULTURA ORGANIZACIONAL DE CIBERSEGURIDAD EN LA ALCALDÍA DE NEIVA*

Yesica Tatiana Vanegas Silva

* Ponencia resultado del proyecto de investigación titulado *Gestión de riesgos en seguridad digital para la infraestructura crítica, de la Maestría en Ciberseguridad y Ciberdefensa*, de la línea de investigación *Seguridad Digital* del grupo de investigación *Masa crítica*, reconocido y categorizado en (B) por Minciencias, registrado con el código COL0123247, adscrito y financiado por la Escuela Superior de Guerra de la Republica de Colombia. Ponencia resultado de la investigación presentada como opción de grado para optar por el título de magíster en ciberseguridad y ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Resumen

Como consecuencia del aumento de los incidentes informáticos, la necesidad de proteger los activos de información y de cumplir con la legislación y la reglamentación nacional e internacional pertinentes, las organizaciones han tomado medidas técnicas y administrativas que permitan gestionar los riesgos cibernéticos. No obstante, diferentes estudios demuestran que no es suficiente establecer controles técnicos, pues quienes finalmente administran la información son personas. Por ello, el factor humano es fundamental en la ciberseguridad, pues es fuertemente influenciable por diferentes variables de su entorno, psicológicas, sociales y culturales, a escalas regional o nacional. Cualquier error humano, intencional o accidental, es una vulnerabilidad latente que puede ser explotada por diferentes amenazas. Por ello, este factor debe ser gestionado y cultivado dentro de la organización.

Para establecer una cultura organizacional no es suficiente un plan de concienciación y sensibilización. Así, este artículo contextualiza al lector en el concepto de *cultura organizacional*, desarrolla ocho factores que influyen en la construcción de una cultura organizacional de seguridad y propone una estrategia de cultura organizacional de ciberseguridad aplicable a la Alcaldía de Neiva. Para ello, toma como referencia investigación documental, trabajo de campo en la entidad, el esquema de cultura de seguridad de la empresa CLTRe AS de Oslo (Noruega), la investigación de cultura organizacional de la Agencia Europea de Seguridad de las Redes y de la Información y el kit de concienciación del Instituto Nacional de Ciberseguridad de España.

Palabras clave: cultura organizacional; ciberseguridad; apropiación; concienciación; cumplimiento; comportamiento.

Abstract

As a consequence of the increase in computer incidents, the need to protect information assets and to comply with relevant national and international legislation and regulations, organizations have taken technical and administrative measures that allow managing cyber risks. However, different studies show that it is not enough to establish technical controls, since those who ultimately manage the information are people. For this reason, the human factor is fundamental in cybersecurity, as it is strongly influenced by different variables of its environment, psychological, social and cultural, at regional or national scales. Any human error, intentional or accidental, is a latent vulnerability that can be exploited by different threats. Therefore, this factor must be managed and cultivated within the organization. To establish an organizational culture, an awareness and sensitization plan is not enough. Thus, this article contextualizes the reader in the concept of organizational culture, develops eight factors that influence the construction of an organizational culture of security and proposes a strategy of organizational culture of cybersecurity applicable to the Mayor's Office of Neiva. For this, it takes as a reference documentary research, field work in the entity, the security culture scheme of the CLTRe AS company in Oslo (Norway), the organizational culture research of the European Network Security Agency and the Information and awareness kit from the National Cybersecurity Institute of Spain.

Keywords: Organizational culture; cybersecurity; appropriation; awareness; fulfillment; behavior.

1. Introducción

La transformación digital ha implicado la evolución de las tecnologías tradicionales para dar paso a las disruptivas, es decir, aquellas que provocan un cambio en la forma de realizar y desarrollar ciertos procesos. Las más reconocidas son la impresión 3D, el *blockchain*, el internet de las cosas, la computación en la nube, la inteligencia artificial y el *big data*, pues han cambiado la forma de comunicamos, comprar, procesar y analizar la información. Sin embargo, esto ha traído consigo amenazas que atentan contra un nuevo activo organizacional: la información. Cuando su disponibilidad, confidencialidad e integridad quedan limitadas, dichas amenazas irrumpen las labores diarias, causan mala reputación y generan problemas económicos.

De acuerdo con un estudio sobre controles de seguridad mediante hackeo en empleados de Croacia, la seguridad de la información se basa en tres elementos básicos: personas (factor humano), procesos y tecnología (Lovrić Švehla et al., 2016, p. 1). Los riesgos de seguridad en el área técnica se pueden mitigar mediante controles definidos en *hardware* y *software*, gestión de riesgos, gestión de incidentes, políticas de seguridad, gestión de resiliencia y demás elementos descritos en la estrategia propuesta en cada organización. La pregunta es ¿cómo gestionar el factor humano haciendo que este sea consciente y cumpla con estas estrategias de seguridad establecidas por la entidad? El comportamiento humano no es consistente y puede estar fuertemente influenciado por las relaciones. Otra explicación es la creencia, general e ingenua, de que las cosas malas solo les suceden a otras personas (Johnston y Warkentin, 2010).

Según el estudio realizado en 2017 por Kaspersky Lab a más de 5000 empresas en todo el mundo, llamado "El factor humano en la seguridad de TI: cómo los empleados hacen que las empresas sean vulnerables desde dentro", el 52 % de las empresas admiten que los empleados son su mayor debilidad en seguridad de las tecnologías de la información (TI). El personal descuidado o desinformado, por ejemplo, es la segunda causa más probable de una infracción de seguridad grave, solo superada por el *malware*. Además, en el 46 % de los incidentes de seguridad cibernética en el último año, el personal descuidado o desinformado ha contribuido al ataque.

La principal conclusión de este estudio fue la siguiente:

> Las tendencias de movilidad significan que el personal descuidado o desinformado puede ser más propenso a cometer errores, y las amenazas como el *phishing* y la ingeniería social también ponen a las empresas en mayor riesgo por parte del personal que no sabe cómo diferenciar entre actividad legítima y maliciosa. (Kaspersky Lab, B2B International, 2017)

Para lograr que las personas de la Alcaldía de Neiva interioricen los conceptos, buenas prácticas, políticas, herramientas y demás avances establecidos en materia de seguridad y privacidad de la información, es necesario concientizarlas por medio de una cultura de ciberseguridad encaminada a los objetivos organizacionales y respaldada por la alta gerencia. Jo Malcolmson (2009) argumenta que la cultura de seguridad de la información está indicada por los supuestos, valores, actitudes, creencias y comportamientos de los empleados, pues estos pueden impactar la seguridad de la organización en la que trabajan.

El presente trabajo de investigación tiene como caso de estudio la Alcaldía Municipal de Neiva, encargada del tratamiento de datos personales y sensibles de la totalidad de la población del municipio, es decir, 345.806 habitantes, según las cifras del DANE. De ahí su importancia, además de salvaguardar la información, dar cumplimiento a lo establecido en la Ley 1581 de 2012, artículo 4.º denominado "Principios para el tratamiento de datos personales" y su principio de seguridad.

Así, se observan las motivaciones para abordar el concepto de *cultura organizacional de ciberseguridad*. Seguidamente, se abordan los ocho

factores clave que influyen y constituyen el éxito de una cultura de seguridad, como 1) el apoyo de la administración superior, 2) el establecimiento de una política eficaz, 3) la conciencia, 4) la capacitación y la educación, 5) el análisis y la evaluación de riesgos, 6) el cumplimiento, 7) las políticas de conducta ética y 8) la cultura organizacional.

En cuanto al caso de estudio de esta investigación, se analiza un contexto de la entidad en materia de procesos y normatividad aplicable a la misma; luego, se identifica su estado actual en lo referente a la ciberseguridad, seguridad de la información e informática, desde un enfoque documental y perceptivo, a través de encuestas realizadas a una muestra de la entidad. Este reconocimiento del contexto permitirá identificar riesgos de seguridad digital de cara al factor humano, los cuales son el insumo base para proponer la estrategia de cultura organizacional en esta entidad pública.

Por último, y teniendo en cuenta los conceptos identificados, se desarrolla la propuesta de una estrategia de cultura organizacional de ciberseguridad compuesta por cuatro etapas: 1) planeación, 2) métricas, 3) organización y 4) formación, teniendo como referencia el esquema de cultura de seguridad de la empresa CLTRe AS de Oslo, Noruega, la investigación de cultura organizacional de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y el kit de concienciación del Instituto Nacional de Ciberseguridad de España (INCIBE).

2. La cultura organizacional de ciberseguridad como un componente fundamental de una estrategia de ciberseguridad

Luego de analizar las encuestas realizadas durante 2015 en el Reino Unido, el artículo “El comportamiento humano como un aspecto de la garantía de ciberseguridad” revela que el error humano inadvertido causó la mitad de las peores violaciones de seguridad, debido a que es muy difícil controlar el talento humano en las organizaciones, por el

constante cambio en su comportamiento. Prueba de esto es el estudio que realizó Cisco en 2015, a través del cual identificó cuatro perfiles de comportamiento de los usuarios que usan y administran la información en una organización.

1) El consciente es aquella persona consciente de los riesgos de seguridad y de las políticas establecidas en la organización. Cree en la responsabilidad compartida en la protección de los datos. 2) El bienintencionado conoce la política de seguridad, la cumple de manera aleatoria, pero no comprende completamente el impacto de sus acciones. 3) El complaciente no cumple con la política ni con los controles establecidos. Esta persona tiende a pensar que la seguridad es un obstáculo para sus labores diarias. Por último, 4) el aburrido y cínico es aquel que cree que el costo de la información está sobrevalorado; ha oído hablar de las políticas de seguridad en la organización, pero intenta evadirlas (Cisco, 2015).

Lo anterior demuestra que el factor humano es una vulnerabilidad latente en una organización, y no gestionarla facilita la materialización de riesgos que exponen los activos de información. Es fácil pensar que la concienciación y la sensibilización son la solución para mitigar este riesgo, pero diferentes investigaciones académicas demuestran que el hecho de conocer estos riesgos y su rol en la protección de los activos no significa que se cumpla con las políticas dispuestas. Por ello, es necesario abarcar toda una cultura organizacional de ciberseguridad que incluya otros componentes mencionados en el presente documento, de manera que permita generar un cambio en el comportamiento de las personas.

Las definiciones de *cultura organizacional* son diversas y dependen del contexto y del sector donde se desarrolle dicha cultura. En la tesis titulada *Auditoría del clima y cultura de seguridad en la empresa*, se reúnen las características sobresalientes de estas definiciones: "la cultura es un conjunto de valores aprendidos que pueden tomar fuerza en una organización mediante prácticas interpretadas a través de reglas y normas de conducta" (Hernández, 2007). ENISA (2017) define la *cultura organizacional de ciberseguridad* como "los conocimientos, creencias, percepciones, actitudes, supuestos, normas y valores de las personas con respecto

a la ciberseguridad y cómo se manifiestan en el comportamiento con las tecnologías de la información" (p. 7).

Teniendo en cuenta las definiciones anteriores, se puede observar cómo el comportamiento desempeña un papel vital para establecer una cultura organizacional, siendo conscientes de esto o no. Furnell y Thomson (2009) establecen que la cultura es un conjunto de percepciones y actuaciones, en ocasiones inconscientes, que determinan el comportamiento de las personas —como individuos y como integrantes de una comunidad—.

Schein, en su libro *La guía de supervivencia de la cultura corporativa* (citado en Furnell y Thomson, 2009), establece que para comprender la cultura organizacional es necesario conocer los tres niveles de la cultura corporativa: 1) los artefactos, 2) los valores propuestos y 3) los supuestos tácitos compartidos. Los artefactos son los comportamientos concretos de una persona; lo que ha visto, escuchado y sentido en una organización. Los valores propuestos son aquellas directrices establecidas y defendidas por la alta gerencia. Los supuestos tácitos compartidos son los comportamientos y los valores compartidos por los miembros de la entidad, apostando por su veracidad (Furnell y Thomson, 2009).

Para Van Niekerk y Von Solms (2009), estos tres niveles aplican para establecer una cultura organizacional, pero consideran necesario agregar un cuarto nivel llamado "conocimiento de seguridad de la información", para establecer una cultura organizacional de seguridad de la información. La razón es que no se puede asumir que las personas cuentan con la formación y la preparación necesaria para interiorizar la cultura, y es aquí donde la concienciación y la sensibilización desempeñan un papel importante.

2.1. Factores que constituyen e influyen en una cultura de seguridad de la información

En 2012, mediante su tesis doctoral titulada *Comprensión y medición de la cultura de seguridad de la información en países en desarrollo: caso de Arabia Saudita*, Mohammed A. Alnatheer realizó una investigación a

partir de una muestra de veinte altos directivos de compañías que administraran infraestructura de seguridad de la información y usaran prácticas de gestión de seguridad de la información con frecuencia.

En este estudio, el autor identificó tres factores que constituyen una cultura de seguridad de la información: el primer factor es la *apropiación*, que permite a los integrantes de la organización entender sus roles y sus responsabilidades frente a la seguridad, así como los riesgos asociados a sus acciones. Así, busca aumentar los niveles de conciencia de seguridad de las personas y el cumplimiento de la política de seguridad de la organización. El segundo factor es la *concienciación*, que es el grado en que los miembros de la organización comprenden la importancia de la seguridad de la información, el nivel de seguridad requerido por la organización y sus responsabilidades de seguridad individuales para actuar en consecuencia. El tercer factor es el *cumplimiento*, que se refiere al seguimiento de las políticas, prácticas y procedimientos de seguridad establecidos en la organización.

Según la Academia Real de la Lengua Española, *constituir* es "Formar, componer, ser" e *influir* es "Dicho de una cosa: producir sobre otra ciertos efectos". Por ser conceptos diferentes, Alnatheer, en 2015, identificó ocho factores de éxito que influyen en la construcción de una cultura organizacional de seguridad:

1. *El apoyo de la administración superior:* teniendo en cuenta que el cambio en el comportamiento del factor humano en la organización se logra con el respaldo de la alta dirección —la cual debe incluir dentro de su objetivo de negocio la protección de los activos de información y tecnológicos, ratificar su importancia asignando presupuesto para tal fin, siguiendo a Fourie (2003, citado en Alnatheer et al., 2012)—, esta debe establecer roles y responsabilidades y contar con el recurso necesario para establecer el monitoreo continúo del cumplimiento de las directrices propuestas.
2. *La creación* —por parte de la alta gerencia— *de una política eficaz de Seguridad de la información y ciberseguridad*, que establezca las estrategias, los responsables y los derroteros

que deben cumplir los empleados para alcanzar el objetivo propuesto.

3. *La conciencia*, factor que constituye e influye en la construcción de una cultura de seguridad. Sin este grado de interiorización y cumplimiento de las políticas establecidas en la organización, no sería posible establecer una cultura. La norma ISO/IEC TR 13335-1 (citada en Alnatheer, 2015) establece que la conciencia de seguridad de todos los empleados es un elemento esencial de la seguridad efectiva y contribuye positivamente a una cultura de seguridad mejorada. Para abordarla, es necesario establecer un plan de concienciación, que se articula perfectamente con el siguiente factor.
4. *Capacitación y educación*, sin este factor, es muy difícil ser consciente de los riesgos en el ciberespacio. Por tal razón, una estrategia de ciberseguridad en la empresa debe incluir un plan de "sensibilización, capacitación y educación", reconociendo que el ser humano, debido a que este es fuertemente influenciable, es el eslabón más débil de la cadena de seguridad.

   Howell (1982, citado en Thomson et al., 2006), consciente de que el conocimiento impartido a las personas mediante la sensibilización, la capacitación y la educación no garantiza el cumplimiento de las políticas y de los controles establecidos, y de que es necesario que las personas interioricen estos conocimientos para poder aplicarlos en su día a día de una manera inconsciente, desarrolló el modelo de aprendizaje de competencia consciente, dividido en cuatro etapas.

   En la primera etapa, *incompetencia inconsciente*, el empleado no cuenta con el conocimiento necesario para realizar una actividad específica ni conoce la importancia de esta. En la segunda, *incompetencia consciente*, el empleado es consciente de la importancia de su rol en la organización y puede discernir si su comportamiento es correcto o incorrecto, de acuerdo con las directrices establecidas; sin embargo, aún no cuenta con el conocimiento necesario para cumplir las funciones en su rol.

En la tercera, *competencia consciente*, ha recibido capacitación y cuenta con el conocimiento necesario, pero debe pensar en la forma y los pasos para poder realizar la acción. En la cuarta, *competencia inconsciente*, el empleado alcanza la habilidad de realizar las actividades a su cargo sin pensar en la manera de ejecutarlo. Según este modelo, se debe avanzar por cada una de las etapas mediante capacitación, cumplimiento y práctica, para lograr así un nivel óptimo de concienciación e interiorización de las políticas, valores o directrices dispuestas por la dirección.

5. *Análisis y evaluación de riesgos*: el riesgo es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o un daño en un activo de información (Organización Internacional de Normalización, 2005).
   La gestión de riesgos es un factor que influye en la construcción de ciberseguridad, debido a que la evaluación de este brinda conciencia sobre el valor de los activos, sus pérdidas y sus daños. Asimismo, identifica que la falta de una cultura consciente de seguridad se debe a la carencia de conocimiento sobre seguridad y el incumplimiento de las políticas y buenas prácticas establecidas por la alta dirección (Alnatheer, 2015).
   Según la *Cartilla de administración de riesgos* del Departamento Administrativo de la Función Pública de Colombia (DAFP), el proceso para la administración del riesgo inicia con su identificación, análisis (determinación de su probabilidad, consecuencias y nivel) y valoración (controles, efectividad de controles y tratamiento), todo dentro de un monitoreo y una revisión continúa (Ministerio de Tecnologías de la Información y Comunicaciones, 2016).
6. *El cumplimiento*: no es suficiente establecer políticas, directrices y concienciación en la organización si las personas no cumplen con lo dispuesto. Así, Furnell y Thomson (2009) establecieron los *Niveles de cumplimiento de seguridad basados en comportamientos individuales*, en los que describen el nivel

de cumplimiento e incumplimiento de la seguridad, basados en los comportamientos de los empleados. En la tabla 5.1 se identifica una línea delgada entre el nivel de cumplimiento consciente y el incumplimiento ignorante, debido a que establecer una conciencia a través de un plan de concienciación o cualquier otro mecanismo no es suficiente para alcanzar una cultura. Para esto son necesarios, según ese estudio, la obediencia y el compromiso.

Tabla 5.1. Niveles de cumplimiento de seguridad basados en comportamientos individuales

Cumplimiento	Cultura	El estado ideal en el que la seguridad es parte implícita del comportamiento natural del usuario.
	Compromiso	La seguridad no es una parte natural del comportamiento, pero sí se proporciona una guía adecuada. Los usuarios aceptan la necesidad y realizan un esfuerzo asociado.
	Obediencia	Los usuarios no pueden aceptar los principios, pero se les puede hacer cumplir a través de la autoridad apropiada.
	Conciencia	Los usuarios son conscientes de su papel en la seguridad de la información, pero todavía no están cumpliendo completamente con las prácticas o los comportamientos asociados.
Incumplimiento	Ignorancia	Los usuarios no son conscientes de los problemas de seguridad y, por lo tanto, pueden presentar efectos adversos involuntarios.
	Apatía	Los usuarios son conscientes de su papel en la protección de los activos de información, pero no están motivados para adherirse a las buenas prácticas de seguridad de la información.

Resistencia	Los usuarios trabajan pasivamente contra la seguridad, oponiéndose a aquellas prácticas con las que no están de acuerdo.
Desobediencia	Los usuarios trabajan activamente contra la seguridad, con abusadores internos que infringen intencionalmente las reglas y eluden controles.

Fuente: Furnell y Thomson (2009).

7. *Políticas de conducta ética y cultura organizacional*: Hellriegel et al. (citados en Veiga, 2008) definen la *ética* como los valores y las reglas que distinguen el bien del mal. El comportamiento ético difiere dependiendo del contexto en que se encuentren las personas, pues una acción que se considere ética dentro de un territorio u organización no lo es en un contexto diferente. Por esto, la alta gerencia debe establecer parámetros aceptables de comportamiento entre los empleados, alineados con los objetivos estratégicos, con el fin de minimizar el riesgo de acciones que reduzcan la seguridad en la organización.

La conducta ética y la cultura organizacional van de la mano, teniendo en cuenta que se articulan para lograr un cambio en el comportamiento de las personas. La ética, dictamina las reglas y los valores, en cuanto a la cultura, se centra en el cumplimiento y adopción de estas reglas en una comunidad en el ámbito organizacional. En el artículo "Una aproximación al concepto de cultura organizacional", Álvarez (2005) establece que la *cultura organizacional* son las conductas de las personas dentro de un contexto, y que para lograr el éxito en la organización es necesario crear estrategias gerenciales que permitan que las personas interioricen los valores y las políticas establecidas para contribuir así al compromiso e identidad en los empleados (Álvarez, 2005).

2.2. El factor humano como amenaza interna para la ciberseguridad en una organización

Según el Informe de investigaciones de violación de datos de Verizon del 2019, el *phishing*, el *misdelivery* y *pretexting* se encuentran en el *ranking* de las principales amenazas, fuertemente relacionadas con el factor humano (Verizon, 2019). Diferentes autores de todo el mundo han concluido en sus investigaciones que un porcentaje muy alto de incidentes de seguridad son causados por errores humanos. Un ejemplo es un estudio de 2019 que analizó 7202 incidentes publicados por la Oficina del Comisionado de Información del Reino Unido. Según esta investigación, el 64.44 % de los incidentes tienen la "probabilidad"; el 35.14 %, la "posibilidad", y el 0.41 %, la "improbabilidad" de ocurrir por errores humanos (Evans et al., 2019). Asimismo, el 50 % de las organizaciones encuestadas en el estudio sobre incumplimientos de seguridad de la información, realizado en 2015 en el Reino Unido, respondió que el peor incidente sufrido fue por un error humano inadvertido (HM Government, 2015).

Las empresas líderes en ciberseguridad día a día desarrollan productos y servicios para salvaguardar los activos de *hardware*, *software* y redes de las constantes amenazas cibernéticas. Sin embargo, las amenazas internas (maliciosas o accidentales) cada año logran posicionarse en el top de las principales amenazas del mundo, según el *Informe del panorama de amenazas 2018* de Agencia Europea de Seguridad de las Redes y de la Información (2019). En 2017 y en 2018, se encuentran en el número 9 dentro del *ranking* (tabla 5.2).

Uchenna et al. (2015) afirman que para obtener eficiencia en la ciberseguridad no basta con disponer de "antivirus, *firewalls* y sistemas de detección/prevención de intrusos (ID/PS)" o de "procedimientos de seguridad estrictos" ni de "expertos en seguridad de TI altamente calificados", si el factor humano no se apropia de la seguridad establecida en la organización (p. 170). Por esta razón, describen que para contar con éxito en la protección de los activos, la ciberseguridad debe estar compuesta por la tríada "personas, procesos y tecnología" (figura 5.1).

Así, los autores definen a la ciberseguridad como "la armonización de capacidades en personas, procesos y tecnologías para asegurar y controlar tanto el acceso autorizado o ilegal como la interrupción o destrucción de los sistemas informáticos electrónicos (*hardware*, *software* y redes), los datos y la información que poseen".

Tabla 5.2. Descripción general y comparación de los panoramas de amenazas (2017-2018)

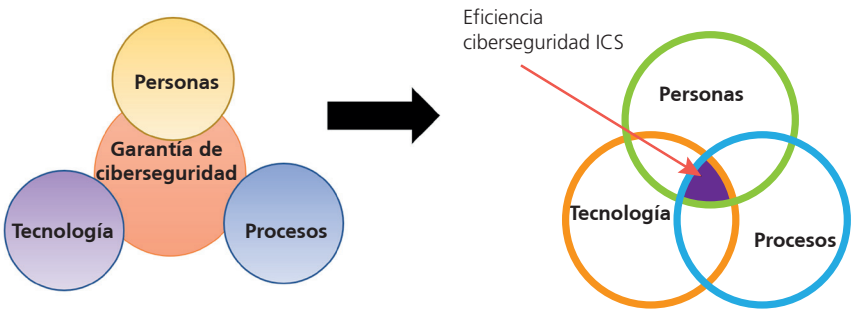
Top de amenazas en 2017	Top de amenazas en 2018	Cambio en el *ranking*
1. *Malware*	1. *Malware*	
2. Ataques basados en la web	2. Ataques basados en la web	
3. Ataques a aplicaciones web	3. Ataques a aplicaciones web	
4. *Phishing*	4. *Phishing*	
5. *Spam*	5. Denegación de servicios	
6. Denegación de servicios	6. *Spam*	
7. *Ransomware*	7. *Botnets*	
8. *Botnets*	8. Violaciones de datos	
9. Amenazas internas	9. Amenazas internas	
10. Manipulación física, daño, robo o pérdida	10. Manipulación física, daño, robo o pérdida	
11. Violaciones de datos	11. Fuga de información	

Top de amenazas en 2017	Top de amenazas en 2018	Cambio en el *ranking*
12. Robo de identidad	12. Robo de identidad	→
13. Fuga de información	13. *Cryptojacking*	NUEVA
14. Kits de explotación	14. *Ransomware*	↓
15. Espionaje cibernético	15. Espionaje cibernético	→

↑ Subiendo → Igual ↓ Bajando

Fuente: Elaboración propia con base en la información de la ENISA (2019).

Figura 5.1. Entidades colaborativas para una seguridad cibernética efectiva



Fuente: Adaptación propia con base en Uchenna et al. (2015, p. 170).

Las personas son trascendentales en la implementación de toda estrategia, pues son estas las que finalmente administran y desarrollan los procesos y los procedimientos de las organizaciones, y quienes permiten cumplir los objetivos estratégicos diseñados por la alta gerencia.

Es tan importante el factor humano, que el Gobierno de Colombia desarrolló el Modelo Integrado de Planeación y Gestión (MIPG), que en su dimensión n.º 1 desarrolla la Política de Gestión Estratégica de Talento Humano, en la que el factor humano aparece definido como "el

activo más importante con el que cuentan las entidades y […] el gran factor crítico de éxito que les facilita la gestión y el logro de los objetivos y los resultados" (Departamento Administrativo de la Función Pública, 2018, p. 4).

No obstante, si no se gestiona ni evalúa el comportamiento de las personas, estas pueden convertirse en una amenaza interna para la ciberseguridad en la organización. Para el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon (2015), una *amenaza interna maliciosa* para una organización es

> … un empleado, contratista u otro socio comercial actual o anterior que tiene o ha tenido acceso autorizado a la red, al sistema o a los datos de una organización, e intencionalmente excedió o usó mal ese acceso de una manera que afectó negativamente la confidencialidad, integridad o disponibilidad de la información o los sistemas de información de la organización. Además, las amenazas internas también pueden ser involuntarias (no maliciosas). (p. 2)

Debido al cumplimiento de sus funciones y obligaciones laborales, las personas cuentan con perfiles de autoridad y confianza cuyo alcance se incrementa a medida que lo hacen la responsabilidad y el mando. Una persona que desee realizar alguna actividad maliciosa en la organización cuenta con mayores posibilidades de obtener su cometido, pues posee acceso sin restricción y privilegios al *hardware*, *software*, redes, información y demás activos de la organización. Además, debido a su experticia en el manejo de las herramientas y los procesos a su cargo, conoce el cómo, el cuándo y el dónde atacar. Por su parte, las amenazas externas deben realizar todo un procedimiento de reconocimiento de la víctima para lograr su meta.

Teniendo en cuenta las cifras anteriores e investigaciones realizadas, es necesario gestionar al factor humano en una organización, pues este es quien "diseña, implementa, opera, usa y abusa de los sistemas de información" abriendo paso a errores voluntarios e involuntarios, no obstante, este además es quien puede evitar que estos riesgos se materialicen (Lacey, 2009, pág. 1). Sin embargo, se debe tener en cuenta que no solo el mal comportamiento es un factor asociado al incremento de

incidentes informáticos, factores como el estrés, falta de conocimiento, falta de supervisión, fallos en las herramientas tecnológicas o procesos, es decir errores involuntarios causan estos incidentes, por esta razón se debe identificar el origen de estos errores para tomar las medidas pertinentes (Lacey, 2009).

3. Alcaldía de Neiva: contexto de la entidad

Como lo afirmó la Oficina de Tecnologías de la Alcaldía de Neiva en el PETI, Resolución 279 de 2017 (Alcaldía de Neiva, 2017), esta es una entidad pública cuyo principal objetivo es usar de manera adecuada los recursos económicos asignados al municipio desde las diferentes dependencias, en busca del bienestar físico, económico, social y cultural de todos sus habitantes para que gocen de una mejor calidad de vida. Así, la Alcaldía de Neiva realiza el tratamiento de la información personal, financiera, educativa y social de los 347.501 habitantes de la ciudad, según proyección censal del Departamento Administrativo Nacional de Estadística (DANE).

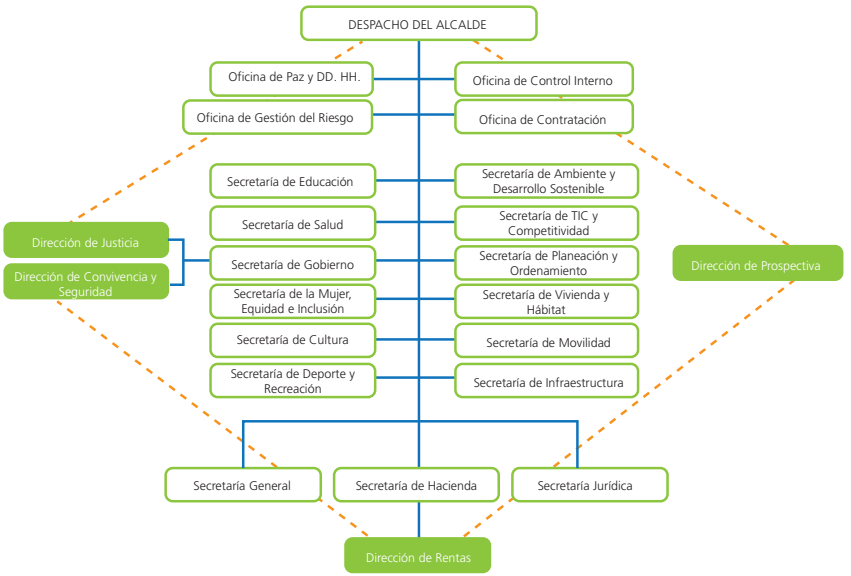
La figura 5.2 presenta la estructura administrativa de la Alcaldía de Neiva, según el Decreto Municipal 590 de 2016.

La entidad cuenta con veinte procesos, divididos en cuatro líneas principales: 1) estratégicos, 2) misionales, 3) apoyo y de evaluación y 4) control. Estos procesos son la columna vertebral de la administración, cumpliendo así con su misión, visión y objetivos estratégicos (figura 5.3).

Un aspecto importante por resaltar es que en este mismo Decreto Municipal 590 de 2016, por el cual se estableció la estructura de la alcaldía del municipio de Neiva y se creó la Secretaría TIC y Competitividad, se definió para esta Secretaría la función n.º 15, cuyo objetivo es

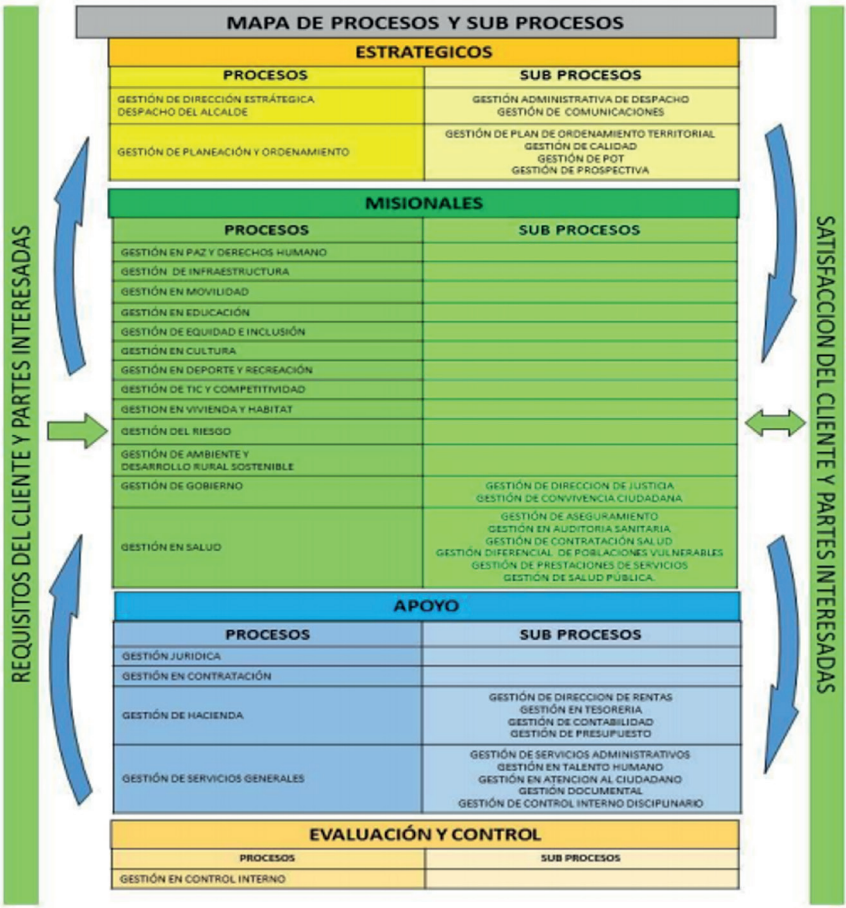
> Definir y desarrollar estrategias de gestión de información de la entidad territorial para garantizar la seguridad informática, ciberseguridad y ciberdefensa con el fin de lograr un flujo eficiente y disponible para el uso de ella en la gestión y toma de decisiones. (Alcaldía de Neiva, 2016)

Figura 5.2. Organigrama de la Alcaldía de Neiva



Fuente: Alcaldía de Neiva (2016).

Figura 5.3. Procesos y subprocesos de la Alcaldía de Neiva



Fuente: Resolución 279 de 2017.

3.1. Ciberseguridad en la entidad

Con el objetivo de utilizar la tecnología como articulador transversal en la prestación de servicios a los ciudadanos del municipio, la Alcaldía de Neiva, desde 2015, ha avanzado, según los plazos establecidos, con la implementación del Decreto 1078 de 2015: "Estrategia de Gobierno en línea" en las entidades públicas a escala nacional. Esta estrategia desarrolló cuatro componentes: 1) TIC para servicios, 2) TIC para Gobierno

abierto, 3) Tic para la gestión y la seguridad, y 4) privacidad de la información.

En el mismo decreto, se establecen los plazos para el cumplimiento de estos cuatro componentes. Así, se define que para los municipios de categoría 3 —es decir, el municipio de Neiva—, para 2019, se debe cumplir con el 100 % del componente TIC para servicios; mantener el 100 % para Gobierno abierto; el 80 %, para la gestión, y el otro 80 % para seguridad y privacidad de la información. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015)

La implementación de la Estrategia Gobierno en Línea permitió a la Alcaldía de Neiva posicionar la tecnología como un dinamizador y articulador de procesos y procedimientos, de cara a brindar un servicio óptimo a los ciudadanos. Por esto, para abordar el componente de Seguridad y Privacidad de la Información de esta estrategia nacional, así como para garantizar la confidencialidad, integridad y disponibilidad de la información en las entidades, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) diseñó el Modelo de Seguridad y Privacidad de la Información (MSPI).

Este modelo tomó como base la norma ISO/IEC de 2013, el esquema de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST), los fundamentos de la arquitectura empresarial, algunas mejoras prácticas de ITIL y la Ley 1581 de 2012 de privacidad de la información y tratamiento de datos personales. Cuenta con un instrumento de diagnóstico basado en los dominios establecidos en la norma ISO 27002, con un avance en el ciclo PHVA y con un nivel de madurez y una calificación en mejores prácticas en ciberseguridad, de acuerdo con el esquema NIST. Adicionalmente, para su implementación, cuenta con 21 guías (cuadro 5.1).

Cuadro 5.1. Guías del Modelo de Seguridad y Privacidad de la Información

Guía 1	Metodología de pruebas de efectividad
Guía 2	Política General MSPI v1
Guía 3	Procedimiento de seguridad de la información
Guía 4	Roles y responsabilidades
Guía 5	Gestión de la clasificación de los activos
Guía 6	Gestión documental
Guía 7	Gestión de riesgos
Guía 8	Controles de seguridad de la información
Guía 9	Indicadores de gestión de seguridad de la información
Guía 10	Continuidad del negocio
Guía 11	Análisis de impacto del negocio
Guía 12	Seguridad en la nube
Guía 13	Evidencia digital
Guía 14	Plan de comunicación, sensibilización y capacitación
Guía 15	Auditoría
Guía 16	Evaluación de desempeño
Guía 17	Mejora continua
Guía 18	Lineamientos terminales de las áreas financieras de las entidades públicas
Guía 19	Aseguramiento del Protocolo IPv4_IPv6
Guía 20	Transición IPv4_IPv6
Guía 21	Gestión de incidentes

Fuente: Biblioteca de seguridad dispuesta por el MINTIC (2016).

Según el autodiagnóstico concertado en el MSPI, la Alcaldía de Neiva, en la evaluación de efectividad de controles, dispuestos en el Anexo A de la norma ISO 27001:2013, cuenta con un promedio de 18 sobre 100 puntos. Esta calificación la ubica en el nivel 1 o inicial, según la brecha entre el estado actual de la entidad y el nivel optimizado. La tabla 5.3 y la figura 5.4 presentan los dominios evaluados.

Tabla 5.3. Evaluación de efectividad de controles

Dominio	Calificación actual	Calificación objetivo	Evaluación de la efectividad del control
Políticas de seguridad de la información	60	100	Efectivo
Organización de la seguridad de la información	18	100	Inicial
Seguridad de los recursos humanos	31	100	Repetible
Gestión de activos	37	100	Repetible
Control de acceso	6	100	Inicial
Criptografía	0	100	Inexistente
Seguridad física y del entorno	13	100	Inicial
Seguridad de las operaciones	16	100	Inicial
Seguridad de las comunicaciones	16	100	Inicial
Adquisición, desarrollo y mantenimiento de sistemas	3	100	Inicial

Dominio	Calificación actual	Calificación objetivo	Evaluación de la efectividad del control
Relaciones con los proveedores	0	100	Inexistente
Gestión de incidentes de seguridad de la información	9	100	Inicial
Aspectos de seguridad de la información de la gestión de la continuidad del negocio	7	100	Inicial
Cumplimiento	33,5	100	Repetible
Promedio de la evaluación de controles	**18**	**100**	**Inicial**

Fuente: Alcaldía de Neiva, Comité Institucional de Gestión y Desempeño (2018).

Figura 5.4. Diagnóstico de seguridad y privacidad de la información de acuerdo con el Anexo A ISO 27001:2013

Fuente: Alcaldía de Neiva, Comité Institucional de Gestión y Desempeño (2018).

En cuanto al avance del ciclo de funcionamiento del modelo de operación (PHVA), en el componente de *planificación* se cuenta con un porcentaje de avance actual de la entidad del 12 % sobre un total deseado del 40 %; en el componente de *implementación*, del 1 % sobre el 20 %; en el componente de *evaluación de desempeño*, del 5 % sobre el 20 %, y en el componente de *mejora continua*, del 8 % sobre el 20 %. Estas cifras promedian el 26 % del avance actual de la entidad sobre el 100 % esperado (tabla 5.4).

Tabla 5.4. Avance en el ciclo de funcionamiento del modelo de operación

Componente	Avance actual (%)	Avance esperado (%)
Planificación	12	40
Implementación	1	20
Evaluación de desempeño	5	20
Mejora continua	8	20
Total	**26**	**100**

Fuente: Alcaldía de Neiva, Comité Institucional de Gestión y Desempeño (2018).

Luego de la puesta en vigencia del Decreto 1499 de 2017, el cual desarrolla la estructura del Modelo Integrado de Planeación y Gestión (MIPG), se establece una articulación y complementariedad con otros sistemas de gestión, como el Sistema Nacional de Servicio al Ciudadano, Gestión de la Seguridad y la Salud en el Trabajo, Gestión Ambiental y Seguridad de la Información. Asimismo, con 16 políticas de gestión y desempeño institucional (Departamento Administrativo de la Función Pública, 2017), entre las cuales figura la de Seguridad Digital y Gobierno Digital (antes, Gobierno en Línea).

Entre otras disposiciones, el Decreto 1499 de 2017 establece que la medición de la gestión y el desempeño institucional se debe realizar a

través del Formulario Único de Reporte y Avance de Gestión (FURAG). Este formulario se encuentra a disposición de las entidades obligadas a aplicar el MIPG. En la figura 5.5 se puede observar que, según lo reportado por la entidad, esta se encuentra en el rango *medio alto* en el avance de la implementación de la política de Gobierno Digital.

Figura 5.5. Avance en la implementación de la política de Gobierno Digital

Nivel de avance en la implementación de la Política de Gobierno Digital		Escala de 0 - 100
	Bajo	Menor a 20
	Medio bajo	Igual o mayor a 20 y menor a 40
	Medio	Igual o mayor a 40 y menor a 60
	Medio alto	Igual o mayor a 60 y menor a 80
	Alto	Igual o mayor a 80 y menor o igual a 100

Fuente: Alcaldía de Neiva (2019).

Teniendo en cuenta que la política de Gobierno Digital desarrolla tres habilitadores transversales (seguridad de la información, arquitectura empresarial y servicios ciudadanos digitales) (tabla 5.5), la herramienta evalúa el habilitador de seguridad de la información, que, según lo reportado por la entidad, se encuentra en un nivel *alto*. A continuación, se presenta el porcentaje de cumplimiento de los indicadores que pertenecen al habilitador de seguridad de la información establecido en el FURAG.

Tabla 5.5. Indicadores de cumplimiento para el habilitador en la seguridad de la información

Fase	Indicadores de cumplimiento	Porcentaje de cumplimiento (%)
Evaluación y planificación de la seguridad de la información	Diagnóstico de seguridad y privacidad de la información	100
	Política del MSPI	100
	Roles y responsabilidades del MSPI	100

Fase	Indicadores de cumplimiento	Porcentaje de cumplimiento (%)
	Procedimientos del MSPI	100
	Gestión de activos de seguridad de la información	100
	Gestión de riesgos de seguridad y privacidad de la información	100
	Plan de comunicación, sensibilización y capacitación en seguridad de la información	100
Implementación de seguridad de la Información	Implementación del plan de tratamiento de riesgos de seguridad de la información	100
	Plan de control operacional	100
	Indicadores de gestión de seguridad de la información	100
Seguimiento, evaluación y mejora de seguridad de la información	Seguimiento y evaluación del desempeño de la seguridad de la información	50
	Plan de mejoramiento continuo de seguridad de la información	0

Nota: Modelo de seguridad y privacidad de la información (MSPI).
Fuente: Elaboración propia con base en Alcaldía de Neiva (2019).

En cuanto a la sensibilización y concienciación en seguridad de la información y la ciberseguridad establecida en la entidad, la oficina de Tecnologías de la Información y las Comunicaciones estableció el documento titulado *Plan de sensibilización de seguridad y privacidad de la información, Alcaldía de Neiva*. El alcance de este es "maximizar la interiorización de los conceptos y su aplicación en la cotidianidad institucional y personal". Este documento cuenta con una serie de preguntas que, según el autor, permiten analizar la visión personal de cada encuestado

sobre el conocimiento y el compromiso en temas de seguridad y privacidad de la información, la definición del grupo profesional necesario para la implementación del plan y el despliegue de los elementos de sensibilización, como carteles, correos electrónicos y otros (Alcaldía de Neiva, 2018).

Según el enfoque metodológico de la presente investigación, para desarrollar la estrategia propuesta se realizó, en enero de 2020, una encuesta compuesta por trece preguntas, a través de la herramienta Formularios de Google. Fue aplicada a catorce dependencias de la entidad, con dos a tres funcionarios de cada dependencia seleccionada (una muestra de veintinueve personas que laboran de la Alcaldía de Neiva).

Los participantes de este estudio fueron auxiliares administrativos, abogados, ingenieros de sistemas, administradores y economistas. La encuesta se llevó a cabo con el fin de identificar la conciencia y la apropiación de la ciberseguridad y la seguridad de la información en la entidad, a través de preguntas centradas en el conocimiento de la política de seguridad y privacidad de la información y el plan de sensibilización y concientización propuesto por la oficina de tecnología de la entidad pública.

La Política de Seguridad y Privacidad de la Información es la directriz superior en cuanto a esa materia en la entidad, pues establece el compromiso para la protección de los activos de la organización. Sin embargo, el 58,6 % de las personas encuestadas manifiestan no conocer esta política, y el 34,5 % indica solo haberla leído. Así las cosas, es poco posible que dicha política se cumpla y se mitiguen los riesgos de seguridad en la entidad.

Por su parte, el 58,6 % de los encuestados indica no conocer la política de copias de seguridad; el 41,4 % indica que nunca realiza copias de seguridad, y el 31 % indica que las realiza una vez al mes. Esta mala práctica es un riesgo para los activos de información, pues al estar expuestos a su pérdida, imposibilitan la continuidad efectiva de la prestación de los servicios a los ciudadanos.

Por otro lado, el 41,4 % de las personas actualiza el sistema operativo de sus equipos de cómputo al menos una vez al mes, y el 39,9 % nunca lo hace. Asimismo, el 51,7 % de las personas señala contar

con *software* antivirus, pero no realiza actualizaciones periódicas. Esto demuestra niveles de conciencia reducidos en cuanto a la gestión de la actualización de los sistemas operativos y sus antivirus, por lo que los equipos de cómputo quedan vulnerables a posibles ataques cibernéticos.

Del total de los participantes, el 65,5 % indica que no conoce el plan de sensibilización y concienciación adoptado por la entidad, y el 34,5 % señala que solo lo ha leído. Estos datos demuestran que si bien la oficina de tecnologías ha generado y publicado en la página web institucional este documento, los funcionarios no lo han socializado. Este alto nivel de desconocimiento se debe al incumplimiento de las actividades propuestas en el plan, pues, según el documento, estas debieron llevarse a cabo durante cuatro meses, entre febrero y junio de 2019 (Alcaldía de Neiva, 2018).

A la pregunta ¿con qué frecuencia ha recibido capacitación, por parte de la entidad, en temáticas como seguridad de la información, informática o ciberseguridad?, el 89,7 % de las personas respondió que nunca ha recibido capacitación, y el 10,3 %, que al menos una vez al mes la ha recibido.

Es importante mencionar que en el plan de capacitación con vigencia de 2020 se identifica una formación llamada "Seguridad en el acceso de la información", aunque se encuentra pendiente por definir el tipo de capacitación, la fecha y la entidad que realizará la misma (Alcaldía de Neiva, 2020, p. 25).

Esta falta de concientización y capacitación por parte de la entidad se ve reflejada en el desconocimiento de los protocolos por seguir al ocurrir un incidente de seguridad de la información, pues el 72,4 % de las personas indica que no los conocen. Asimismo, el 75,9 % de los encuestados dice no conocer el significado de ataques informáticos tan comunes como *malware*, *phishing* y robo de información.

Es importante mencionar que en la evaluación de indicadores de cumplimiento del habilitador de seguridad de la información, según lo reportado por la entidad en el FURAG, la Política del MSPI y el Plan de comunicación, sensibilización y capacitación en seguridad de la información tienen el 100 % de cumplimiento (tabla 5.5). Sin embargo,

la mayoría de las personas encuestadas indica no tener conocimiento de estas temáticas, lo cual expone la necesidad de no solo aprobar y publicar en la página web institucional estos documentos, sino además de socializarlos con los funcionarios y velar por el cumplimiento de estos.

3.2. El factor humano como amenaza interna en la identificación de riesgos de ciberseguridad en la Alcaldía de Neiva

Dando cumplimiento al objetivo E1.2 del documento CONPES 3854 del 2016, que indica que se debe "Implementar en el Gobierno nacional un modelo de gestión de riesgos de seguridad digital" (Departamento Nacional de Planeación , 2016, p. 48), MINTIC elaboró el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD). Este modelo tomó como referencia las buenas prácticas nacionales e internacionales de gestión del riesgo, con el fin de realizar guías para identificar, analizar, evaluar y tratar los riesgos de seguridad digital en sectores estratégicos como el sector público y de Gobierno, el sector mixto y privado, el sector de la fuerza pública y la ciudadanía (MinTIC, 2018).

Con base en lo anterior, y teniendo en cuenta que la Alcaldía de Neiva es una entidad pública de orden territorial, para identificar los riesgos de ciberseguridad de cara al factor humano, la presente investigación ha consultado la *Guía de orientación de aplicación de la gestión de riesgos de seguridad digital en el sector público, territoriales y Gobierno nacional*.

Para identificar los riesgos, se toma como insumo la información recopilada en la etapa de conocimiento del estado actual de la entidad, a través de información documental y encuestas realizadas a los funcionarios en materia de seguridad de la información y ciberseguridad, para posteriormente convertirla en una matriz de riesgos que sirva como base para construir la Estrategia de Cultura Organizacional por proponer.

Se identifican once riesgos en los cuales el factor humano actúe como amenaza y vulnerabilidad para la materialización de aquellos. Luego, se identifican las consecuencias, el tipo de activo, el responsable y el tipo y clasificación del riesgo. Tres de estos riesgos se encuentran catalogados

en la zona de riesgo *alta* —denegación del servicio, fuga de información y descarga, instalación o uso de *software* no autorizado—, y ocho, en la zona de riesgo *moderada* —alteración de la información sin autorización, fraude y robo de información, daño o mal funcionamiento, acceso no autorizado a los activos de información, uso indebido o inadecuado de los sistemas de información e información, fuga de conocimiento a través de talento humano, alto nivel de dependencia de proveedores externos a la entidad, incumplimientos legales (anexo 5.1).

4. Estrategia de cultura de ciberseguridad propuesta

La estrategia de cultura organizacional de ciberseguridad propuesta nace para atender la necesidad latente en Colombia —específicamente en la Alcaldía de Neiva— de minimizar los riesgos de ciberseguridad provocados intencional o accidentalmente por el factor humano en las organizaciones. Toma como marco de referencia la investigación documental presentada en este artículo, enfocada en la identificación de los factores que constituyen —e influyen en— una cultura organizacional de seguridad, así como en la identificación y el conocimiento del estado actual en materia de seguridad cibernética —en términos de documentación y conciencia de los funcionarios— y en el esquema de cultura de seguridad desarrollado por la empresa CLTRe AS de Oslo, Noruega, bajo una licencia "Creative Commons Share Alike" —que indica que es libre de uso y modificación, con la condición de citar la fuente y compartir los aportes realizados a la comunidad creada por esta empresa.

Luego de una revisión de literatura, se identifica que este esquema reúne componentes importantes, como el establecimiento de metas, la medición de estas y elementos organizacionales y formativos para la construcción de una cultura organizacional de ciberseguridad

Este esquema tiene cuatro etapas: en la primera, *medición*, se identifica el estado actual por medio de un autodiagnóstico denominado As-is. También se deben definir las metas deseadas To-Be. En la segunda,

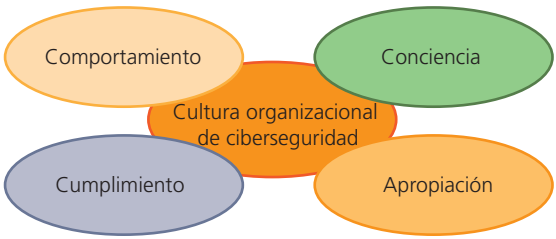
organización, se identifican los roles y las responsabilidades de los actores en la estrategia. En la tercera, *temas*, se describe el contenido de las temáticas que serán desarrolladas en las campañas de capacitación, a través de folletos y correos, entre otros. En la cuarta, *planear*, se identifican los objetivos, las metas y las actividades que deben incluirse en el desarrollo de este esquema de cultura de seguridad (CLTRe, 2019).

Esta propuesta de estrategia contribuye en el desarrollo de un plan de acción, actividades, métricas, roles en el contexto organizacional y contenido de formación, teniendo como referencia aportes propios, así como elementos importantes de la norma ISO 27001, la investigación sobre cultura organizacional de seguridad cibernética de ENISA y el kit de concienciación del INCIBE, enmarcado en cada una de las cuatro etapas del esquema descrito. El resultado es una estrategia que permea la cultura organizacional en su componente de ciberseguridad.

4.1. Objetivo de la estrategia

El objetivo de la estrategia de cultura organizacional de ciberseguridad para la Alcaldía de Neiva es gestionar el talento humano por medio de la articulación de factores como la conciencia, la apropiación, el cumplimiento y el comportamiento (figura 5.6), de manera que permita la mitigación de riesgos de ciberseguridad en la organización.

Figura 5.6. Objetivo de la cultura organizacional de ciberseguridad



Fuente: Elaboración propia.

La estrategia propuesta se compone de cuatro etapas que trabajan en pro del fortalecimiento de cuatro capacidades que garantizan la integralidad de la organización: tecnología, información, personas y procesos.

En la primera etapa, *planeación*, se define un plan de acción, con la descripción de las actividades necesarias para su cumplimiento. En la segunda, *métricas*, se define la medición que se realizará para evaluar el cumplimiento del plan de acción identificado en la primera etapa. En la tercera, *organización*, se definen los roles y las actividades que facilitan la implementación de la estrategia. En la cuarta, *formación*, se lista el contenido en materia de capacitación, formación y educación para lograr su concienciación y apropiación. Estas etapas se encuentran enmarcadas por un proceso de mejora continua. La figura 5.7 representa la estrategia propuesta.

Figura 5.7. Estrategia de la cultura organizacional de ciberseguridad

Fuente: Elaboración propia con base en el Security Culture Framework (2019).

4.2. Etapa de planeación y métricas

Teniendo como referencia que para establecer una cultura de ciberseguridad es necesario articular y abordar las capacidades tecnológicas, de información, personas y procesos en una organización, se establece la tabla 5.6, en donde se identifican las actividades y la medición para fortalecer cada una de estas capacidades, pues esta será la hoja de ruta para realizar la implementación de la estrategia que se propone en el presente estudio.

Tabla 5.6. Plan de acción y métricas para la estrategia de cultura organizacional de ciberseguridad propuesta

Capacidad	Plan de acción	Actividades	Métrica
Tecnología	Identificar la infraestructura tecnológica dispuesta en la organización para el cumplimiento de la misión.	Realizar un inventario de la infraestructura tecnológica de la organización, determinando su ubicación, responsables, valor estratégico y criticidad ante una interrupción no autorizada del servicio.	Inventario de infraestructura tecnológica realizado.
		Inventariar los sistemas de información, determinando su ubicación, roles a cargo de la administración, valor estratégico y criticidad ante una interrupción no autorizada del servicio.	Inventario de sistemas de información realizado.
Información	Gestionar los riesgos de seguridad de la información y la ciberseguridad.	Realizar el levantamiento de activos de información de la organización, en el cual se especifique el proceso al que pertenece cada uno, el tipo de activo, el custodio, la clasificación, la criticidad, las amenazas y las vulnerabilidades.	Inventario y clasificación de activos de información realizados.

Capacidad	Plan de acción	Actividades	Métrica
Información		Revisar periódicamente el plan de tratamiento de riesgos de seguridad de la información y la ciberseguridad, con el objetivo de controlar cambios planificados, no planificados y la consecuencia de estos.	Revisiones documentadas.
	Mantener una comunicación constante con entidades públicas y privadas para establecer una cooperación para la prevención y la atención de incidentes cibernéticos.	Recopilar información sobre ataques, vulnerabilidades y exposiciones, normatividad brindada por compañías de seguridad informática y centros de cooperación —como Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), el Comando Conjunto Cibernético (CCOC), el Centro Cibernético Policial (CCP), el CSIRT de la Policía Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)—.	Información recopilada y documentada.
Personas	Formar al factor humano en el conocimiento de los riesgos de seguridad por medio de programas de sensibilización, concienciación y educación en ciberseguridad.	Publicar consejos y buenas prácticas en ciberseguridad (a través de medios *online*, *offline* e híbridos), con miras a informar al personal operativo y técnico y la alta gerencia..	Resultado de las pruebas de conocimiento antes y después de implementar el programa de sensibilización.
		Realizar simulacros por medio de ataques dirigidos con el fin de identificar la conducta de la persona y probar su conocimiento en el procedimiento de resolución de incidentes y presentación de informes.	Número de empleados que siguen los protocolos de reporte de incidentes después de que los detectan.
		Entrenar al personal encargado de administrar la seguridad de la organización por medio de escenarios y juegos de guerra.	Número de empleados que pueden prevenir y detectar un ciberataque.
		Encuestar y entrevistar a los empleados con el fin de evaluar su percepción y conciencia en materia de ciberseguridad.	Encuestas y entrevistas realizadas.

Capacidad	Plan de acción	Actividades	Métrica
Procesos	Buscar el compromiso de las directivas con la estrategia de cultura organizacional.	Garantizar los recursos necesarios para implementar las actividades propuestas para fortalecer y mejorar continuamente la estrategia de cultura organizacional.	Recursos para la estrategia de cultura organizacional incluidos dentro del presupuesto anual.
		Crear un plan de incentivos laborales (económicos o morales) que sirva para motivar a los funcionarios a cumplir la estrategia propuesta y a adoptarla en su día a día.	Porcentaje de cumplimiento del plan anual de incentivos.
		Crear un equipo de cultura organizacional dispuesto a seguir la estrategia propuesta y a generar espacios propicios para la discusión con el personal.	Equipo de cultura organizacional de ciberseguridad creado.
		Crear una política de cultura organizacional que incluya el componente de ciberseguridad y no dependa del cambio de administración.	Política de cultura organizacional creada.
		Crear un código de conducta y de ética aceptables y de obligatorio cumplimiento.	Evaluación del cumplimiento del código por medio de procesos de control interno y control interno disciplinario.
		Crear el procedimiento de gestión del conocimiento y la cultura de la documentación.	Conocimiento documentado.

Capacidad	Plan de acción	Actividades	Métrica
Procesos	Generar los espacios para la participación.	Promover la participación del personal por medio de foros dispuestos en la intranet de la organización, los cuales sirvan para resolver inquietudes, brindar aportes, entre otros.	Inquietudes, sugerencias y aportes gestionados.
	Seguir y mejorar continuamente la implementación de la estrategia de cultura organizacional de ciberseguridad.	Diagnosticar el estado actual de la cultura organizacional de ciberseguridad de la audiencia objetivo.	Diagnóstico realizado.
		Realizar auditorías internas para verificar el cumplimiento de las métricas propuestas en la estrategia de cultura organizacional de ciberseguridad.	Número de auditorías realizadas.

Fuente: Elaboración propia con base en información de la ENISA y el INCIBE (2020).

4.3. Organización

Para implementar la estrategia de cultura organizacional de ciberseguridad, es necesario contar con un grupo interdisciplinario dispuesto a realizar seguimiento a la misma, desde su etapa inicial hasta de su mejora continua. Según la ENISA (2017), los roles que se deben identificar para la construcción de una cultura organizacional de ciberseguridad en la organización se describen en la tabla 5.7.

Tabla 5.7. Roles necesarios para una cultura de ciberseguridad

Rol	Papel
Alta gerencia	Aprobar las políticas, brindar respaldo económico, incluir la estrategia de ciberseguridad en la cultura organizacional y establecer la importancia de la gestión de riesgos de seguridad para el cumplimiento de la misión.
Grupo de TI	Aportar conocimiento y experiencia en la infraestructura tecnológica y los sistemas de información; intermediar el grupo de seguridad de la información y la alta gerencia.
Grupo de seguridad de la información	Articular los objetivos estratégicos del grupo de TI con los principios de seguridad de la información, con énfasis en la gestión del riesgo.
Recursos humanos	Acompañar al factor humano, por medio de un plan de incentivos o sanciones, para ejercer el cumplimiento de políticas y buenas prácticas dispuestas en la organización.
Comunicaciones	Promover la divulgación del programa de sensibilización en materia de ciberseguridad, por medio del uso de canales efectivos de comunicación.

Fuente: Elaboración propia con base en información de la ENISA (2017).

4.4. Formación

Teniendo en cuenta la identificación de riesgos de cara al factor humano detallados en el anexo 1 del presente documento y los resultados de la encuesta realizada en materia de conciencia y en ciberseguridad y seguridad de la información en la Alcaldía de Neiva (anexo 5.2), en esta etapa se tienen en cuenta temáticas dispuestas en el kit de concienciación de INCIBE, pues a través de estas se busca fortalecer el conocimiento y

la conciencia de los funcionarios de la entidad y, así, mitigar los riesgos de ciberseguridad identificados (INCIBE, 2020).

Tabla 5.8. Propuesta para una estrategia de cultura de ciberseguridad

Tema	Medio	Recurso	Receptor
Escritorio de equipo limpio y bloqueo de equipo en periodos de inactividad.	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.
Creación de contraseñas seguras.	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.
Control en el uso de dispositivos extraíbles (memorias USB, DVD).	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.
Conexión remota con dispositivos de la entidad por medio de una red privada virtual (VPN).	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Todo el personal
Consejos como evitar las amenazas informáticas: ramsonware, phishing, robo de identidad, ingeniería social.	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.
Divulgación de la política de seguridad de la información y la ciberseguridad.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Todo el personal.

Tema	Medio	Recurso	Receptor
Cifrado de información sensible.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Todo el personal.
Legislación en materia de protección de datos, seguridad y privacidad de la información.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Todo el personal.
Control del acceso a sistemas de información y de la ubicación de infraestructura crítica.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Administradores de sistemas de información.
Realización de copias de seguridad.	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.
Seguridad en la red. Segmentación de red, *firewall*.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Administradores de sistemas de información.
Actualizaciones de los sistemas operativos, sistemas de información y antivirus.	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.
Conexión de dispositivos personales en la organización.	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.

Tema	Medio	Recurso	Receptor
Amenazas y vulnerabilidades de ciberseguridad.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Todo el personal.
Procedimiento para el reporte de incidentes de seguridad.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Todo el personal.
Continuidad del negocio.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Grupo de TI.

Fuente: Elaboración propia con base en información del INCIBE (2020).

Las actividades propuestas en la tabla 5.6, así como los contenidos de formación descritos en la tabla 5.8, forman parte del plan de tratamiento de riesgos propuesto en la matriz de riesgos del anexo 1. La entidad deberá implementarlos, realizar una segunda valoración e identificar el riesgo residual. Será importante un monitoreo y un seguimiento para verificar la efectividad de las acciones en la mitigación de los riesgos identificados.

En cada una de las cuatro etapas descritas se observan las actividades, contenidos, roles y responsabilidades necesarios para implementar la Estrategia de Cultura Organizacional en la Alcaldía de Neiva. Con el objetivo de alcanzar la madurez en materia de cultura, es necesario involucrar un proceso de mejora continua, teniendo como insumo las auditorías internas descritas en el plan de acción (tabla 5.6).

5. Conclusiones

Con base en los referentes teóricos revisados en el desarrollo del presente artículo, se puede observar que el éxito de la seguridad cibernética se basa en establecer una visión estratégica que articule la construcción de capacidades en tecnología, información, procesos y personas, teniendo en cuenta que las amenazas pueden ser de diversa naturaleza, y una de estas es el factor humano. No es suficiente establecer controles técnicos si no se cuenta con una cultura organizacional que permita a las personas adoptar e interiorizar estos controles, conceptos y buenas prácticas, para cumplir con lo establecido de una manera inconsciente.

Este documento desarrolló los ocho factores que, según el autor consultado, influyen en la construcción de una cultura organizacional de ciberseguridad. Su desarrollo permitió comprender que no es suficiente crear un plan de concienciación pretendiendo cambiar el comportamiento de las personas. Por esto, debe existir un apoyo de la alta gerencia para que cree políticas de seguridad, promueva conductas éticas aceptables e incentive el cumplimiento.

Luego de identificar los riesgos de cara al factor humano, revisar la documentación referente al cumplimiento de las directrices establecidas por el Gobierno nacional en materia de seguridad digital y evaluar la conciencia y la percepción en la Alcaldía de Neiva al respecto, la entidad reporta un cumplimiento del 100 % en el establecimiento de la política MSPI y del plan de concienciación y capacitación. Sin embargo, esta cifra no se refleja en el comportamiento, cumplimiento, conciencia y percepción de los funcionarios de la entidad. La encuesta realizada demuestra que la conciencia en ciberseguridad es baja.

Con base en la investigación documental teórica y práctica desarrollada en el presente documento, se identifica la necesidad de gestionar el factor humano, considerado una amenaza interna de la organización. Para ello, se propone una estrategia de cultura organizacional de ciberseguridad, basada en el trabajo anterior de CLTRe, pero enriquecida con el aporte de los autores referenciados en el presente documento y

enfocada en la construcción y fortalecimiento de cuatro capacidades: tecnología, información, personas y procesos.

En la primera etapa de la estrategia propuesta, hay un plan de acción encaminado a generar conciencia en las personas, a partir de sesiones de capacitación y educación; un plan de incentivos; participación de los funcionarios en foros y actividades grupales; códigos de conducta ética y de cultura organizacional, y otras actividades complementarias.

En la segunda etapa, se establece la forma de medir el cumplimiento de las actividades del plan de acción. En la tercera, se desarrollan roles necesarios para la implementación, auditoría y mejora continua de la estrategia.

Por último, teniendo en cuenta los resultados de la encuesta realizada en materia de conocimiento en ciberseguridad y la identificación de riesgos de ciberseguridad de cara al factor humano en la Alcaldía de Neiva, se proponen los temas de formación, los recursos necesarios y las personas que serán receptoras de esta formación. Con la implementación de esta estrategia, se pretende facilitar la mitigación de los riesgos de ciberseguridad de cara al factor humano, para así cumplir con los objetivos estratégicos de la Alcaldía de Neiva.

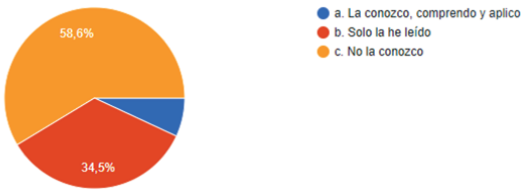
Se recomienda en un trabajo futuro implementar la estrategia aquí propuesta, con el fin de realizar un ejercicio de mejora continua que fortalezca los componentes aquí descritos.

Anexo 1: Matriz de niveles de riesgos de ciberseguridad de cara al factor humano de la alcaldía de Neiva

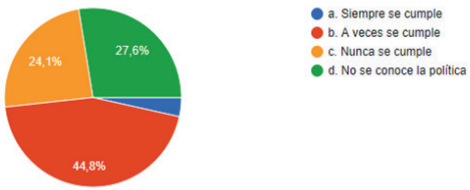
N.°	Riesgo	Definición y descripción del riesgo	Amenazas	Vulnerabilidad	Definición de los efectos de materialización del riesgo identificado	Activos de información asociados	Dueño o propietario del riesgo	Tipo de riesgo	Riesgo asociado			Clasificación del riesgo	Factores		Riesgo inherente						¿Se acepta?	Actividades, estrategia cultura organizacional a implementar
									Confidencialidad	Integridad	Disponibilidad				Posibilidad de ocurrencia		Impacto		Zona de riesgo			
1	Denegación del servicio	Indisponibilidad en los servicios como la página web, internet y software a causa de ataques contra el sistema, entrenamiento insuficiente en seguridad y ausencia de personal calificado	1. Ataques contra el sistema (por ejemplo, negación distribuida del servicio) 2. Intrusión en el sistema 3. Interceptación y espionaje 4. Código malicioso (por ejemplo, virus bomba lógica, troyano) 5. Incumplimiento en el mantenimiento del sistema de información	1. Entrenamiento insuficiente en seguridad 2. Mantenimiento insuficiente 3. Ausencia de personal calificado 4. Desconocimiento de política de copias de seguridad 5. Falta de conciencia acerca de la seguridad 6. Sistemas desactualizados	1. Pérdida de la imagen institucional 2. Incumplimiento de la misionalidad de la entidad 3. Costo financiero de las habilidades específicas para reparar el daño	Servicios/ software	Oficina de Tecnologías	Seguridad digital			X	Tecnológico	5	Recurso humano	3	Posible	3	Moderado	9	Alta	No	1. Crear programas de sensibilización por medios *online, offline* e híbridos en donde se dé a conocer consejos, buenas prácticas en materia de ciberseguridad 2. Realizar sesiones de entrenamiento con el personal encargado de administrar la seguridad de la organización por medio de escenarios y juegos de guerra 3. Crear un plan de incentivos laborales para el personal, económicos o Morales el cual motive a los funcionarios a cumplir la estrategia propuesta, así como adoptarla en su día a día 4. Recopilar información sobre ataques, vulnerabilidades y exposiciones, normatividad brindada por compañías de seguridad informática y centros de cooperación
2	Alteración sin autorización de la información	La falta de políticas de control de acceso, contraseñas de bases de datos no seguras, pueden facilitar una alteración no autorizada causando la pérdida de la integridad de la base de datos	1. Error en el uso 2. Manipulación no autorizada 3. Uso no autorizado del equipo	1. Uso incorrecto del *software* y *hardware* 2. Falta de conciencia acerca de la seguridad 3. Contraseñas de bases de datos no seguras 4. Falta de políticas de control de acceso	1. Divulgación ilegal de información 2. Destrucción de información 3. Investigaciones y sanciones	Datos/ bases de datos	Todos	Seguridad digital	X			Tecnológico	5	Recurso humano	2	Improbable	3	Moderado	6	Moderada	Sí	1. Implementar plan de formación descrito en la etapa 4 de la Estrategia de Cultura Oganizacional 2. Crear un código de conducta ética aceptable y de obligatorio cumplimiento
3	Fuga de información	La falta de conciencia en materia de seguridad, así como amenazas como la ingeniería social permiten que empleados con conocimiento deficiente, intencional o accidentalmente brinden información confidencial de la entidad	1. Ingeniería social 2. Intrusos (empleados con entrenamiento deficiente, descontentos, mal intencionados, negligentes, deshonestos o despedidos)	1. Línea de comunicación sin protección adecuada 2. Ausencia de terminación de la sesión cuando se abandona la estación de trabajo 3. Falta de conciencia acerca de la seguridad	1. Venta de información personal 2. Pérdida de datos de la información privada y con carácter de reservada	Información	Oficina de Tecnologías/ Planeación	Seguridad digital	X			Operativo	5	Recurso humano	3	Posible	3	Moderado	9	Alta	No	1. Realizar simulacros por medio de ataques dirigidos con el fin de identificar la conducta de la persona y probar su conocimiento en el procedimiento de resolución de incidentes y presentación de informes 2. Crear una política de Cultura organizacional en la cual se encuentra incluido el componente de ciberseguridad la cual no dependa del cambio de administración 3. Implementar plan de formación

Anexo 2

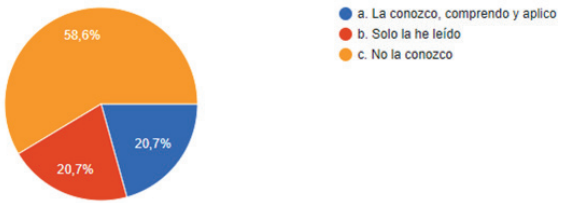
1. ¿Qué tanto conoce la política general de seguridad y privacidad de la información adoptada por la entidad?



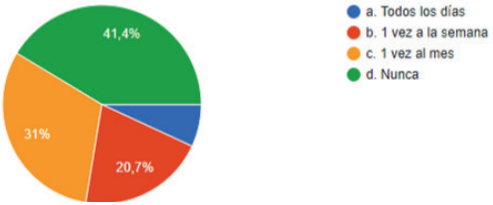
2. Según su percepción, ¿qué tanto se cumple con la política de seguridad y privacidad de la información dispuesta por la entidad?



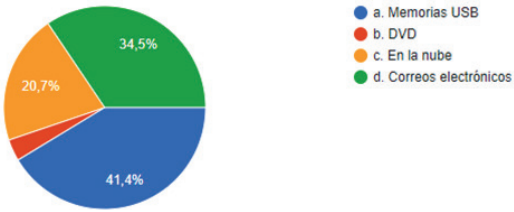
3. ¿Conoce la política de copia de seguridad o respaldo de la información?



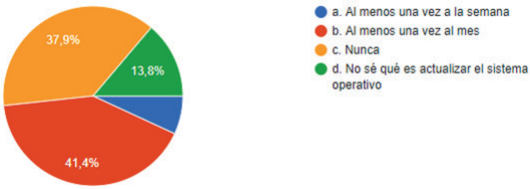
4. ¿Con qué periodicidad realiza copias de seguridad de su información?



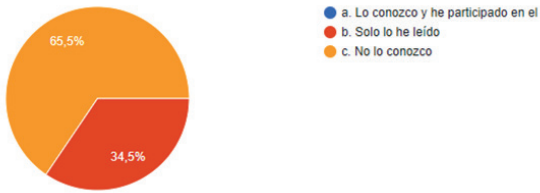
5. ¿Qué medio utiliza para almacenar información en la entidad?



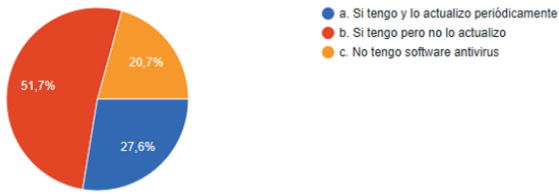
6. ¿Qué tanto conoce el plan de sensibilización y concienciación generado por la Oficina de Tecnologías de la Entidad?



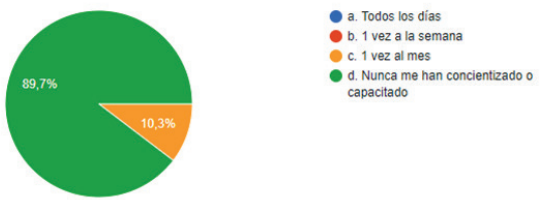
7. ¿Con qué frecuencia actualiza el sistema operativo de su equipo de cómputo?



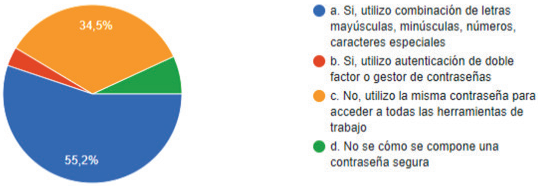
8. ¿Tiene instalado en su equipo de cómputo software antivirus?



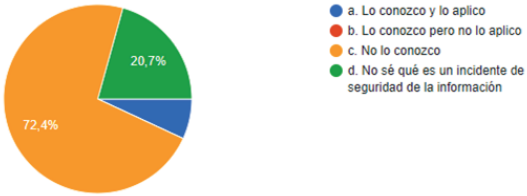
9. ¿Con qué frecuencia usted ha recibido capacitación, por parte de la entidad, en seguridad de la información, informática o ciberseguridad?



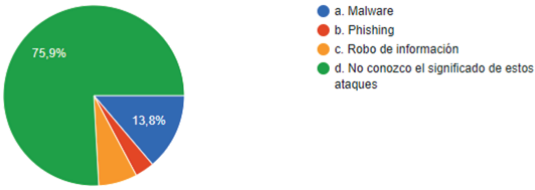
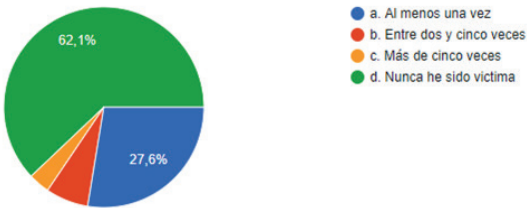
10. ¿Considera que su contraseña de acceso al equipo de cómputo, correo electrónico, páginas web y sistemas de información es segura?



11. ¿Conoce el protocolo que se debe realizar en caso de un incidente de seguridad de la información en la entidad?



12. ¿Reconoce ser víctima de alguno de los siguientes ataques informáticos?



13. ¿Con qué frecuencia ha sido víctima de ataques informáticos?