UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

# ESTRATEGIA PARA LA GESTIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN UNA MUNICIPALIDAD DE LA REGIÓN CHOROTEGA

Trabajo final de investigación aplicada, sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Tecnología de Tecnología de Información y Comunicación para la Gestión Organizacional, para optar al grado y título de Maestría Profesional en Tecnologías de la Información y Comunicación para la Gestión Organizacional

Marianella Villafuerte Guerrero

Ciudad Universitaria Rodrigo Facio, Costa Rica
2021

## Dedicatoria

El presente trabajo final de graduación lo dedico, principalmente, a Dios, por ser el inspirador y darme fuerza para continuar en este proceso de obtener uno de los anhelos más deseados.

A mis padres, por su amor, trabajo y sacrificio en todos estos años. Gracias a ustedes, he logrado llegar hasta aquí y convertirme en lo que soy. Especialmente, a mi madre, quien ha sido siempre un orgullo y el privilegio de ser su hija, gracias por ser mi cable a tierra y siempre sus palabras que llenan de amor mi corazón lo cual son mi gasolina para continuar cuando ya no daba más.

A mis hermanas y hermano por estar siempre presentes, acompañándome y por el apoyo moral, que me brindaron a lo largo de esta etapa de mi vida.

A todas las personas que me han apoyado y han hecho que el trabajo se realice con éxito, en especial a aquellos que nos abrieron las puertas y compartieron sus conocimientos.

## Agradecimientos

Agradezco a Dios por bendecirme la vida, por guiarme a lo largo de mi existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Gracias a mis padres: Eliette, Evaristo, Julio, por ser los principales promotores de mis sueños, por confiar y creer en mis expectativas, por los consejos, valores y principios que me han inculcado.

Agradezco a nuestros docentes de la Programa de Estudios de Posgrado en Computación e Informática de la Universidad de Costa Rica, por haber compartido sus conocimientos a lo largo de la preparación de mi profesión, de manera especial, a la profesora Vivian Murillo Méndez, tutora de este proyecto de investigación, quien me ha guiado con paciencia, dedicación, apoyo incondicional y rectitud.

Ha creado profesionales que se van a distinguir de los demás.

Este trabajo final de investigación aplicada fue aceptado por el Programa de Estudios de Posgrado en Computación e Informática de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Tecnologías de la Información y Comunicación para la Gestión Organizacional.

YEISON ANDRES GRANADOS BOLAÑOS (FIRMA)
PERSONA FISICA, CPF-02-0579-0590.
Fecha declarada: 04/11/2021 12:48:13 PM
Razón: Estoy aprobando este documento

M.Sc. Yeison Granados Bolaños
**Representante del Decano**
**Sistema de Estudios de Posgrado**

VIVIAN MARIELA MURILLO MENDEZ (FIRMA)
Firmado digitalmente por VIVIAN MARIELA MURILLO MENDEZ (FIRMA)
Fecha: 2021.11.01 14:22:06 -06'00'

MBA. Vivian Murillo Méndez
**Profesora Guía**

KENNETH SANCHEZ SANCHEZ (FIRMA)
Firmado digitalmente por KENNETH SANCHEZ SANCHEZ (FIRMA)
Fecha: 2021.11.01 22:32:40 -06'00'

M.Sc. Kenneth Sánchez Sánchez
**Lector**

RAFAEL ANTONIO MARTINEZ VILLARREAL (FIRMA)
PERSONA FISICA, CPF-05-0239-0868.
Fecha declarada: 05/11/2021 12:46:08 p. m.
Razón: Firmado digitalmente

M.Sc. Rafael Martínez Villareal
**Lector**

YORLENY SALAS ARAYA (FIRMA)
Firmado digitalmente por YORLENY SALAS ARAYA (FIRMA)
Fecha: 2021.11.08 10:51:38 -06'00'

M.Sc. Yorleny Salas Araya
**Directora Programa de Posgrado en Tecnología de Tecnología de Información y Comunicación para la Gestión Organizacional**

MARIANELLA VILLAFUERTE GUERRERO (FIRMA)
Firmado digitalmente por MARIANELLA VILLAFUERTE GUERRERO (FIRMA)
Fecha: 2021.11.05 14:07:41 -06'00'

Marianella Villafuerte Guerrero
**Sustentante**

Tabla de contenido

**Resumen**

El presente trabajo se realizó con el fin de brindar instrumentos de ayuda a la Municipalidad en estudio, en el desarrollo de sus procedimientos y manuales de operaciones para brindar un servicio más eficiente y seguro.

Se logró diseñar e implementar un cuestionario aplicado a los funcionarios de esa Municipalidad, lo cual permitió brindar un conocimiento más amplio del clima organizacional y comprender mejor la formar de interactuar con el Departamento de TI. Así mismo, se realizó una observación la cual se aplicó al Departamento de TI y brindó los cimientos del presente trabajo, al conocer de forma más cercana las fortalezas del departamento, así como sus debilidades y exponerlas de tal forma que sean tomadas como una forma de mejora continua dentro de la institución.

Se presenta un modelo para facilitar la obtención de un adecuado nivel de control de riesgos en Tecnologías de Información y Comunicación (TIC), que permita, entre otros, evitar y/o disminuir las fallas en los sistemas, redes, Internet y todo el patrimonio informático (hardware, software y datos) de ataques o desastres, antes que éstos ocurran.

**Abstract**

The present work was carried out in order to provide instruments to help the City Hall under study, in the development of its procedures and operations manuals to provide a more efficient and safe service.

It was possible to design and implement a questionnaire applied to the employees of the Municipality under study, which allowed to provide a broader knowledge of the organizational climate and better understand how to interact with the IT Department. Likewise, an observation was made which was applied to the IT Department and provided the foundations of this work, by knowing more closely the strengths of the department, as well as its weaknesses and exposing them in such a way that they are taken as a form of continuous improvement within the institution.

A model is presented to facilitate obtaining an adequate level of risk control in Information and Communication Technologies (ICT), which allows, among others, to avoid and / or reduce failures in systems, networks, Internet and all computer assets (hardware, software and data) from attacks or disasters, before they occur.

Tabla de Ilustraciones

UNIVERSIDAD DE COSTA RICA

SEP Sistema de Estudios de Posgrado

**Autorización para digitalización y comunicación pública de Trabajos Finales de Graduación del Sistema de Estudios de Posgrado en el Repositorio Institucional de la Universidad de Costa Rica.**

Yo, Marianella Villafuerte Guerrero, con cédula de identidad 503590149, en mi condición de autor del TFG titulado Estrategia para la Gestión de Políticas de Seguridad Informática en una Municipalidad de la Región Chorotega

Autorizo a la Universidad de Costa Rica para digitalizar y hacer divulgación pública de forma gratuita de dicho TFG a través del Repositorio Institucional u otro medio electrónico, para ser puesto a disposición del público según lo que establezca el Sistema de Estudios de Posgrado. **SI** [x] **NO** *[ ]

***En caso de la negativa favor indicar el tiempo de restricción: _____ año (s).**

Este Trabajo Final de Graduación será publicado en formato PDF, o en el formato que en el momento se establezca, de tal forma que el acceso al mismo sea libre, con el fin de permitir la consulta e impresión, pero no su modificación.

Manifiesto que mi Trabajo Final de Graduación fue debidamente subido al sistema digital Kerwá y su contenido corresponde al documento original que sirvió para la obtención de mi título, y que su información no infringe ni violenta ningún derecho a terceros. El TFG además cuenta con el visto bueno de mi Director (a) de Tesis o Tutor (a) y cumplió con lo establecido en la revisión del Formato por parte del Sistema de Estudios de Posgrado.

MARIANELLA VILLAFUERTE GUERRERO (FIRMA)
Firmado digitalmente por MARIANELLA VILLAFUERTE GUERRERO (FIRMA)
Fecha: 2021.11.05 14:08:23 -06'00'

**FIRMA ESTUDIANTE**

Nota: El presente documento constituye una declaración jurada, cuyos alcances aseguran a la Universidad, que su contenido sea tomado como cierto. Su importancia radica en que permite abreviar procedimientos administrativos, y al mismo tiempo genera una responsabilidad legal para que quien declare contrario a la verdad de lo que manifiesta, puede como consecuencia, enfrentar un proceso penal por delito de perjurio, tipificado en el artículo 318 de nuestro Código Penal. Lo anterior implica que el estudiante se vea forzado a realizar su mayor esfuerzo para que no sólo incluya información veraz en la Licencia de Publicación, sino que también realice diligentemente la gestión de subir el documento correcto en la plataforma digital Kerwá.

## i. Justificación

La constante digitalización de los documentos físicos y el uso de sistemas informáticos para las labores diarias son claros ejemplos de la forma en que, actualmente, se utilizan las tecnologías de información para infinidad de servicios. Esto ha traído consigo técnicas y medidas para contener los datos que se manejan dentro de una institución y asegurarse que la información no salga de los sistemas autorizados.

La gestión de la seguridad de la información se abre paso como un elemento fundamental en el desarrollo de los procesos informáticos dentro de una institución. Como menciona Ledo & Pérez (2012), las personas necesitan construir conocimientos que les permitan dar las respuestas más adecuadas ante las circunstancias que se presentan en cada momento, para lo cual se requiere disponer de una información adecuada.

Las políticas de seguridad son herramientas que permiten llevar un correcto control sobre los accesos a los sistemas y la información que se almacena en ellos, establecen los pasos a seguir al crear usuarios nuevos y el control que se debe establecer para el almacenamiento de respaldos o de la información que se extrae.

Las municipalidades no son ajenas a este contexto: tienen en su poder la gestión, mediante los sistemas de información, de los datos de sus contribuyentes, de sus funcionarios y, en general, de las personas a las que brindan un servicio. Esta información, en su mayoría, si bien es cierto es de acceso público, debe de almacenarse con los controles necesarios y la seguridad posible.

En esta municipalidad, existe una clasificación de los servicios, de acuerdo con su nivel de criticidad, políticas, procedimientos, manuales y matrices de control dentro de la institución; sin embargo, la gestión de toda esta información de seguridad informática puede que sea la más adecuada.

Es fundamental establecer una estrategia de gestión de políticas de seguridad informática que mejorará la gestión de los recursos tecnológicos dentro de la

Municipalidad, como menciona Ledo & Pérez (2012). Los daños, producto de falta de seguridad informática, pueden producir falta de credibilidad y pérdidas económicas para la institución.

En síntesis, establecer una estrategia para la gestión de las políticas de seguridad en esta municipalidad podrá mejorar la implementación de los sistemas y su uso dentro de la institución. Se controlará de mejor forma los accesos a información crítica y una mejor administración de los datos.

## ii. Objetivo General:

Elaborar una estrategia para la gestión de políticas de seguridad informática en una Municipalidad de la Región Chorotega con el fin de minimizar el riesgo y la integridad del software y la información.

## iii. Objetivos Específicos:

- Analizar vulnerabilidades dentro de la infraestructura tecnológica, para establecer lineamientos que permitan elaborar las políticas de seguridad.
- Evaluar las políticas de monitoreo de recursos actuales en la Municipalidad en estudio, para identificar debilidades y fortalezas.
- Proponer políticas de seguridad informática en la Municipalidad estudiada, para la minimización del riesgo y la integridad del software y la información.

## Capítulo I. Fundamentación Teórica Contextual

La finalidad de este capítulo es brindar una orientación de la investigación y definir aspectos importantes para la mejor comprensión de los capítulos.

### *1.1 Definición de TIC*

Las tecnologías de la información y la comunicación (TIC) son todas aquellas herramientas y programas que tratan, administran, transmitan y comparten la información, mediante soportes tecnológicos (Biblioteca Médica Nacional 2020).
Las TIC son las tecnologías que se necesitan para la gestión y transformación de la información, muy en particular el uso de ordenadores y programas que permiten crear, modificar, almacenar, proteger y recuperar esa información (Sánchez, 2008).
Las TIC se reconocen como productos innovadores, donde la ciencia y la ingeniería trabajan en conjunto para desarrollar aparatos o sistemas que resuelvan los problemas del día a día. Ellas sintetizan elementos de las llamadas tecnologías de la comunicación o TC (radio, prensa, TV) con las tecnologías de la información (Significados.com, 2020).
En este caso, las computadoras son fundamentales para la selección y el registro de la información, la digitalización para disponer de los recursos en cualquier momento.

### *1.2 Importancia de la TIC como Herramienta Estratégica*

Para la gestión empresarial, se cuenta con recursos informáticos que ayudan en el ahorro de costos y facilitan las tareas diarias.
Es necesario que las TIC se inserten en prácticas sociales ya existentes de personas, grupos u organizaciones; de este modo, servirán como herramientas que potenciarán el trabajo en un mundo real y concreto, y no a la inversa, no se trata de promover y forzar la realización de acciones con el fin de utilizar las TIC (Sánchez, 2008).
En la sociedad actual, se reconoce el papel desempeñado por las tecnologías de la información como núcleo central de una transformación multidimensional que

experimenta la economía y la sociedad, de aquí lo importante que es el estudio y dominio de las influencias que tal transformación impone al ser humano como ente social, ya que tiende a modificar no sólo sus hábitos y patrones de conducta, sino, incluso, su forma de pensar, trabajar y educarse (Ecured.cu, 2020).

### *1.3 Conceptualización de Seguridad Informática*

La seguridad informática es parte fundamental en el desarrollo de las transacciones diarias, a continuación, se brinda su definición, tipos y principios:

#### *1.3.1 Definición*

Se puede definir la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad. (Vieites,2007)

Una política de seguridad es un conjunto de directrices, normas, procedimientos instrucciones que guía las instrucciones de trabajo y definen los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico (Clavillo, 2006).

#### *1.3.2 Tipos de Seguridad Informática*

En este trabajo, se van a tomar como referencia los siguientes tipos de seguridad informática, para una mejor comprensión de la información brindada:

**Seguridad de Hardware.** La seguridad del hardware va relacionada con dispositivos utilizados para monitorear el tráfico de red, de esta manera se detectan intromisiones causadas por el uso del hardware.

**Seguridad de Software.** A través de la seguridad, el software se protege de ataques maliciosos, virus, hackers, de forma tal, que el software utilizado siga funcionando correctamente aún con este tipo de riesgos.

**Virus.** Los virus, una de las amenazas informáticas más antiguas, son un desagradable tipo de malware que secuestra los recursos del equipo para replicarse, propagarse y sembrar el caos.
Los virus informáticos se han ganado su denominación debido a su capacidad para "infectar" varios archivos en un ordenador. Se extienden a otras máquinas, cuando los archivos infectados se envían por correo electrónico o cuando los usuarios los llevan incluidos en medios físicos, como unidades USB o (hace ya tiempo) en los disquetes. Según el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), el primer virus informático, llamado "Brain", se desarrolló en 1986. Cansados de que los clientes piratearan software de su tienda, dos hermanos afirman haber diseñado el virus para infectar el sector de arranque de los disquetes de los ladrones de software. Cuando los discos se copiaban, el virus se transmitía (Kaspersky.es 2020).

***Firewall.*** Las instituciones deben asegurar sus sistemas mediante muros de fuego o “firewall” según Molina (2019) este es un: “programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.”

***Antivirus.*** Para evitar que los activos sean vulnerables ante ataque cibernéticos, se debe instalar software para prevenir intrusiones, mediante antivirus informático, este según Molina (2019): “es un conjunto de programas que protegen nuestra computadora del daño que pueda causar cualquier software o programa maligno.”

***Malware.*** Malware es un término general para referirse a cualquier tipo de “malicious software” (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento. Hay muchos tipos de malware y cada uno busca sus

objetivos de un modo diferente. Sin embargo, todas las variantes comparten dos rasgos definitorios: son subrepticios y trabajan activamente en contra de los intereses de la persona atacada.

***Seguridad de Red.*** Mediante la seguridad de red se establecen formas de acceso, que permitirán ingresos y salidas confiables dentro de la red. Si actualmente los usuarios tienen acceso sin restricciones, debe delimitarse mediante políticas de seguridad.

***Principios de la Seguridad Informática***

La seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático (Salazar, 2009):

Confidencialidad: se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados.

Integridad: es la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático.

Disponibilidad:  continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Importancia de la seguridad informática

## 1.4 Conceptualización de Políticas de Seguridad

Dentro de toda organización que trabaje con sistemas de información, siempre debería ser importante mantener lineamiento en el marco de la seguridad informática.

***Definición***

Las políticas son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro y en algunos casos fuera de la organización.

La implementación de Políticas de Seguridad de la Información es un proceso técnico y administrativo que debe abarcar a toda la organización, por ende, debe estar avalado y contar con un fuerte apoyo de la dirección y/o máxima gerencia, ya que, sin este apoyo, su implementación será más compleja e incluso puede fracasar (Salazar, 2009).

### *Importancia de las Políticas de Seguridad*

Las políticas de seguridad constituyen una herramienta para poder hacer frente a futuros problemas, fallos del sistema, imprevistos y posibles ataques informáticos, (Vieites,2007).

Una política de seguridad para que sea efectiva necesita contar con elementos indispensables que apoyen este proceso: La cultura organizacional, las herramientas y el monitoreo. Esto involucra la participación directa y comprometida de las personas, el diseño de planes de capacitación constante a los usuarios. La disponibilidad de recursos financieros, técnicos y tecnológicos es fundamental y sobre todo actividades de control y retroalimentación que diagnostiquen e identifiquen puntos débiles para fortalecerlos siguiendo las mejores prácticas (Clavijo, 2006).

### *Características de las Políticas de Seguridad*

De acuerdo con Vieites (2007), las políticas de seguridad deberían contar con los siguientes aspectos:

- Alcance
- Objetivos
- Análisis y gestión de riesgos
- Asignación de responsabilidades
- Identificar las medidas, normas y procedimientos a aplicar.
- Gestión de incidentes

- Cumplimiento de la legislación vigente

***Marco de Control***

Existen diferentes marcos de control. Para efectos de este trabajo se analizarán los siguientes:

- Control Objectives for Information and related Technology (COBIT), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC. Actualmente tiene más de 60.000 miembros en alrededor de 100 países.
- Information Technology Infrastructure Library (ITIL), es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial.

***Manuales de Seguridad***

Los procedimientos e instrucciones de trabajo son un conjunto de orientaciones para realizar las actividades operativas, que representa las relaciones interpersonales e interdepartamentales y sus respectivas etapas de trabajo para su implementación y mantenimiento de la seguridad de la información.

***Protocolos de Seguridad***

Los protocolos de seguridad son un conjunto de reglas para ejercer confidencialidad, integridad y autenticación en el transporte de la información, diseñadas para que el sistema pueda soportar ataques maliciosos.

Con el propósito de enfrentar correctamente los procesos de auditoria y a la vez para satisfacer un adecuado nivel de control interno en las actividades de TIC, se deben diseñar controles, de manera que ellos abarquen a todos los procesos que se manejan por medio de las TIC en una organización (Salazar, 2009).

# Capitulo II. Reseña Histórica, Contexto Estratégico y Legal de las Municipalidades

En este capítulo, se presentan los antecedentes históricos de las municipalidades en Costa Rica, los aspectos legales por los cuales se rigen las mismas, una descripción de la reseña histórica de los municipios y su contexto estratégico y estructural.

## 2.1 Antecedentes Históricos de las Municipalidades en Costa Rica

Mediante Decreto Ejecutivo Nº 7248-E del 19 de julio de 1977, se estableció el 31 de agosto de cada año, “Día de Régimen Municipal” como un reconocimiento a la presencia de la municipalidad como institución consustancial al régimen democrático costarricense.

Nuestros municipios tienen sus orígenes en los cabildos establecidos por los españoles durante la Colonia, sobre el que recaían importantes responsabilidades en la vida social, política y económica de nuestra austera vida colonial. (Seminario Universidad, 2012)

El espíritu localista y la necesidad de forjar el estado nacional llevaron a don Braulio Carrillo a eliminar a las municipalidades (mediante Ley de Bases y Garantías). Fueron restablecidos posteriormente a su caída. La Constitución de 1847 establece municipalidades solo en las cabeceras de Departamento. Las ordenanzas municipales, promulgadas en 1867, con reformas y adiciones posteriores, establecieron la organización básica de las municipalidades, cuya vigencia se extenderá en el siglo XX hasta la promulgación del primer Código Municipal en 1970. (www.ifamgo.cr, 2020)

### *2.1.1 Aparición de los Ayuntamientos en Costa Rica*

En Costa Rica, el proceso electoral de los ayuntamientos se inició hacia el 12 de octubre de 1812, cuando el gobernador Juan de Dios Ayala dio instrucciones a las

autoridades de los diferentes pueblos para que, de inmediato, levantaran los padrones respectivos.

La labor de empadronamiento era importante para definir la composición del ayuntamiento de cada pueblo, y para determinar la población total de la provincia pues, de acuerdo con la Constitución de Cádiz, se nombraba un diputado a las Cortes por cada 70.000 habitantes. Cabía también la posibilidad de unir electoralmente a dos jurisdicciones, como ocurrió con el caso de Costa Rica y el partido de Nicoya. (La Nación, 2013)

### 2.2 Aspectos Legales que Rigen las Municipalidades en Costa Rica

La Reforma Económica o Financiera constituyó el primer paso que se dio con el objeto de fortalecer al régimen municipal y fue de carácter eminentemente económico-hacendario. Se estimó que una de las principales debilidades de nuestras municipalidades la constituía la falta de recursos económicos con los cuales hacer frente a los requerimientos de sus comunidades. El impuesto territorial, que normalmente es un tributo de carácter local, en Costa Rica era de carácter nacional y servía para financiar diversas actividades. Con esta reforma de tipo económico, por medio de la Ley Nº 4340 del 30 de mayo de 1969, se trasladaron los ingresos derivados del Impuesto Territorial a las municipalidades del país, aunque su administración continuó en el ámbito central. Este tributo desde entonces ha sido una de las principales fuentes de financiamiento de las municipalidades (www.ifamgo.cr, 2020).

Las leyes que regían la organización y funcionamiento de las municipalidades databan del siglo XIX. Eran anticuadas y no respondían a las necesidades de la época moderna. Se encontraban dispersas y habían sido dictadas sin sentido orgánico ni sistémico. A fines de los años sesenta, se integró una comisión de juristas con el objeto de redactar un Código Municipal, el primero en nuestro país. Así, además de mayores recursos por medio del Impuesto Territorial, se pretendía dotarlas de instrumentos jurídicos y organizativos más modernos que les

permitiera cumplir mejor con su papel que culminó con el Código Municipal (www.ifamgo.cr, 2020)

## 2.4 Contexto Estratégico de las Municipalidad en Estudio

A continuación, se exponen la misión, visión y los valores organizacionales de la municipalidad en estudio. Seguidamente, la estructura organizacional, donde se podrá visualizar de una mejor manera el organigrama del municipio.

### *2.4.1 Misión*

Promover el desarrollo integral del cantón, con una administración activa que mejora la calidad de vida.

### *2.4.2 Visión*

Ser una Municipalidad líder en la gestión, que promueva el desarrollo integral para el bienestar común.

### *2.4.3 Estructura Organizacional*

La estructura jerárquica de la municipalidad en estudio, en términos generales, se divide en 2 grandes subprocesos: la política y la administrativa, siendo el concejo el ente político de la organización, y la alcaldía la parte administrativa, brindando de esta forma mejor gestión y control, de las diferentes acciones que se realizan en estos procesos, divididos en subprocesos y actividades generales.

En la Ilustración 1, se muestran los niveles administrativos que componen la organización en la municipalidad.

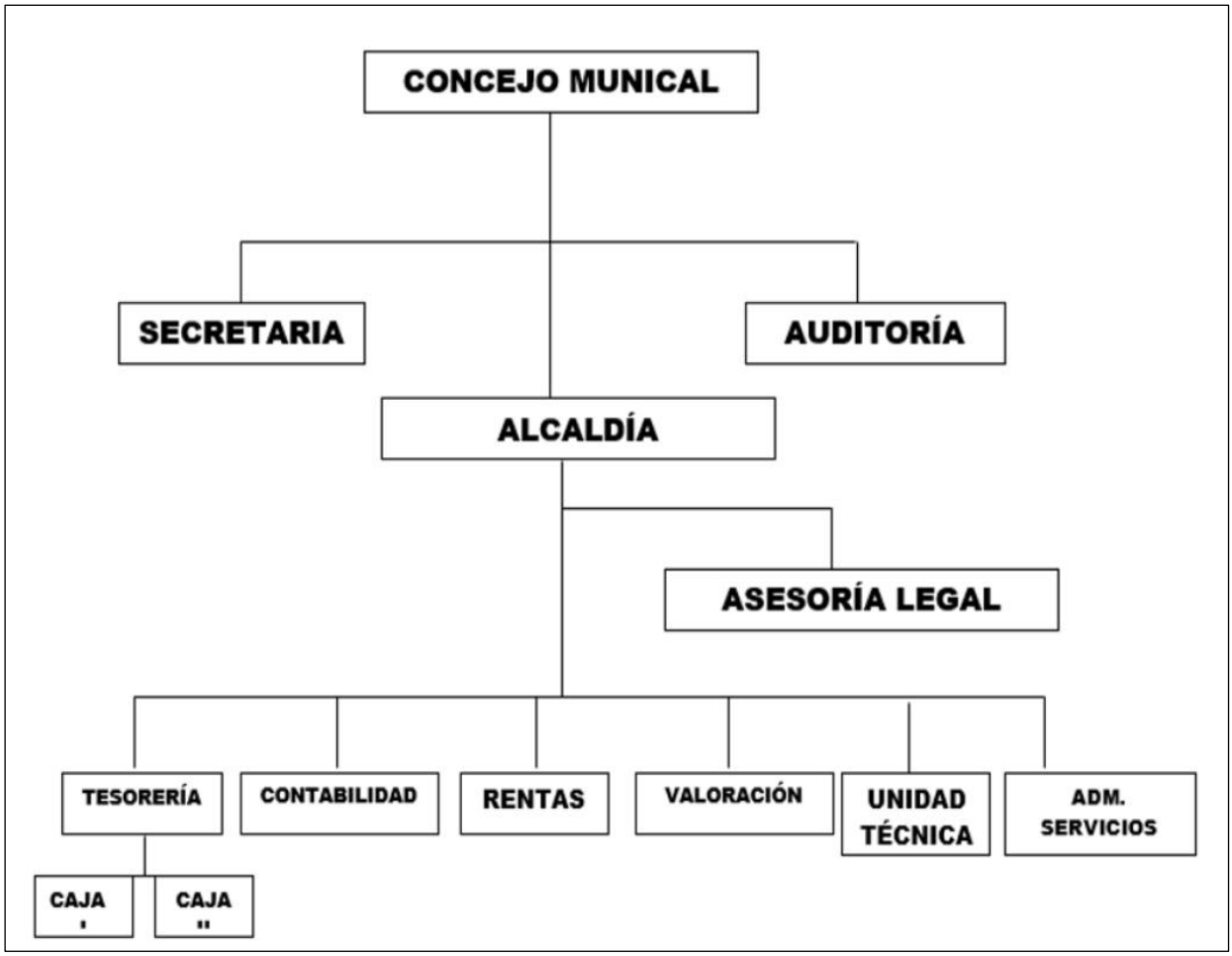


*Ilustración 1: Corresponde a la estructura de la Municipalidad en estudio*

Fuente: Elaboración propia, 2021

# Capitulo III. Metodología

En este apartado, se define la manera en que se llevó a cabo la estrategia para la gestión de políticas de seguridad informática en una municipalidad de la Región Chorotega, detallando el tipo de investigación, las fuentes que fueron consultadas, así como instrumentos de la recolección de datos.

## 3.1 Tipo de Investigación

El tipo de investigación que se utilizó fue la descriptiva, la cual es: “una forma de estudio para saber quién, dónde, cómo y porqué del sujeto o razón de estudio. En otras palabras, la información obtenida en un estudio descriptivo explica perfectamente a la organización, el consumidor, objetos, conceptos y cuentas” Naghi, M. (2000).

Además, el enfoque utilizado fue mixto. Los métodos mixtos representan según Hernández-Sampieri y Mendoza (2008):

> un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (meta inferencias) y lograr un mayor entendimiento del fenómeno bajo estudio (pág. 534)

## 3.2 Fuentes

Las fuentes son “todos los recursos que contienen datos formales, informales, escritos, orales o multimedia” (Silvestrini Ruiz & Vargas Jorge, 2008, pág. 1). Estas fuentes permiten obtener información de gran valor para las investigaciones, puesto que tienen datos que le permiten sustentar los trabajos.

Por esa razón, se procedió a utilizar tanto fuentes primarias como secundarias, para la recopilación de datos importantes, los cuales permitieron la realización con éxito del presente trabajo. A continuación, se detallan:

### 3.3 Fuentes Primarias

Las fuentes primarias “contienen información original, que no ha sido publicada por primera vez y que no ha sido filtrada, interpretada o evaluada por nadie más. Son producto de una investigación o de una actividad eminentemente creativa” (Silvestrini Ruiz & Vargas Jorge, 2008, pág. 2). En otras palabras, es la información recopilada por los investigadores del trabajo.

La fuente primaria utilizada para efectuar esta estrategia es la evaluación del estado actual de manuales y documentación previamente elaborada relacionada a seguridad informática. (manuales, procedimientos, políticas, personas encuestadas, etc.)

La encuesta se aplicó 13 personas de puestos de jefatura dentro de la institución, que por su perfil académico brindan más conocimiento y experiencia a la investigación. La observación, por su parte, se realizó con personas inmersas en el proceso de solicitud de accesos (jefatura y encargado de TI).

### 3.4 Fuentes Secundarias

Las fuentes secundarias, como su palabra lo indica, “permiten conocer hechos o fenómenos a partir de documentos o datos recopilados por otros” (Guzmán Stein, 1982, pág. 1). Estas consisten en material bibliográfico como libros, revistas, reglamentos, trabajos finales de graduación e internet, que posean algún tipo de relación con el tema en estudio.

En el caso de las fuentes secundarias consultadas, fueron las siguientes:

- Sitios de Internet, donde se recopiló los antecedentes históricos de las instituciones públicas en Costa Rica. También, documentos que contienen información relevante para las perspectivas teóricas.

- El Código Municipal, debido a que en este se establecen aspectos importantes para la elaboración de los manuales

- Documentación de la Unión Nacional de Gobiernos Locales (UNGL) y de la Dirección General del Servicio Civil (DGSC).

- Documentación de la Contraloría General de la República de Costa Rica.

### 3.5 Técnicas e Instrumentos de Recolección de Datos

Para obtener la información relacionada al conocimiento de los funcionarios municipales, en relación con la aplicación de políticas de seguridad y ciberseguridad, se utilizó la técnica de encuesta.

Por medio de ella, se conocerá el grado de importancia que tienen las TIC para los funcionarios municipales y su nivel de conocimiento en cuanto a los procedimientos de seguridad que deben de aplicar. La encuesta se ha convertido en una herramienta fundamental para el estudio de las relaciones sociales. Las organizaciones contemporáneas, políticas, económicas o sociales, utilizan esta técnica como un instrumento indispensable para conocer el comportamiento de sus grupos de interés y tomar decisiones sobre ellos. (Romo, 1998)

Así mismo, se utilizó la observación participante, la cual es empleada para aquellas investigaciones que involucran la interacción social entre el investigador y los informantes, y durante la cual se recogen datos de modo sistemático y no intrusivo. (Taylor y Bogdan, 1987)

Es decir, en la observación participante no existe una relación directa con los sujetos de estudio, el investigador se limita a la recolección de datos e información para alcanzar los objetivos del proyecto; el registro de información no implica interacción alguna con el objeto de estudio. En este caso, la observación consistirá lograr recabar información pertinente sobre seguridad informática y la aplicación de procedimientos.

Los instrumentos utilizados fueron el cuestionario (ver Anexo 1) y una guía de observación (ver Anexo 2) para la obtención de los resultados. El valor del muestreo radica en la posibilidad de conocer el comportamiento de una población infinita, a partir de un subconjunto. Este procedimiento aporta una valiosa solución: sin necesidad de realizar un censo, es decir la observación o medición de todos

los individuos de una población, podemos conocer las características que nos interesan. (Romo, 1998)

### 3.6 Alcances

La población de estudio comprende los funcionarios de la municipalidad pertinente, que actualmente hacen uso de, al menos, un sistema de información dentro de la institución.

Estos funcionarios serán abordados iniciando por las jefaturas y coordinaciones, para luego abarcar los funcionarios que tienen contacto directo con los contribuyentes y que llegan a ser usuarios expertos de los sistemas.

### 3.7 Limitaciones

La información expuesta en este trabajo de investigación queda a completa discreción de los lectores. Los datos obtenidos corresponden a una empresa de servicios públicos, por lo que la aplicación de dicha propuesta queda a discreción de cada institución.

# Capitulo IV. Tabulación y Análisis de la Aplicación de Instrumentos

El siguiente análisis se basa en las respuestas brindadas por funcionarios municipales que actualmente hacen uso de, al menos, un sistema de información dentro de la institución.

Es importante mencionar que la información fue obtenida de manera anónima y confidencial, mediante técnicas de entrevistas y encuestas, sin mantener el registro de nombres, ni correos electrónicos en las respuestas, que permitieran revelar la identidad de los emisores.

## 4.1 Encuesta Aplicada a Funcionarios Municipales

El fin de la encuesta dirigida a funcionarios municipales fue identificar el grado de importancia que tienen las TIC para ellos y su nivel de conocimiento en cuanto a los procedimientos de seguridad que deben de aplicar o que ya están estandarizados dentro de la institución en estudio.

Se envió a 13 funcionarios, mediante correo electrónico, un enlace a un formulario creado en la plataforma Google Forms. Esta técnica es utilizada, actualmente, para aumentar la posibilidad de respuesta y reducir los tiempos de respuesta a la encuesta.

En relación con el género de los encuestados, la Ilustración N°2 expone los resultados:

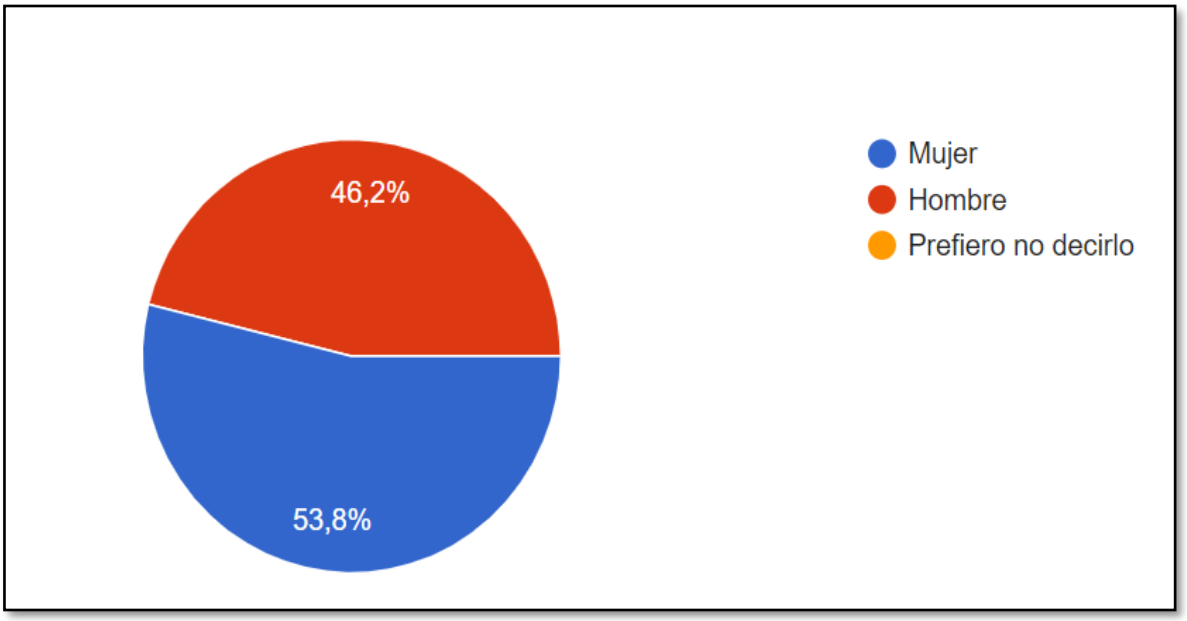


*Ilustración 2: Género de los encuestados.*

Fuente: Encuesta aplicada, año 2021

Se puede observar que la mayoría de los empleados que aplicaron la encuesta son mujeres (53,8%) y un número menor de los encuestados fueron hombres (46.2%), considerando la jefaturas son en su mayoría masculinas, la tendencia a la colaboración en este sentido fue mejor aceptada por las mujeres. En relación con la cantidad de años laborando en la institución que tienen los encuestados, la información se muestra en la Ilustración N°3:

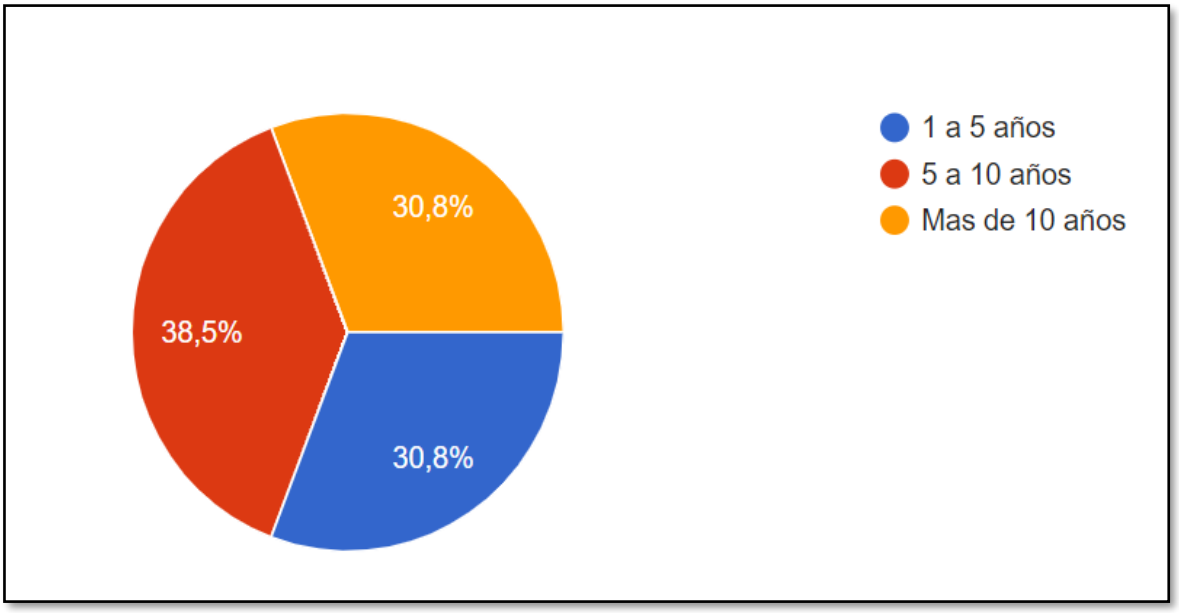


*Ilustración 3: Años laborando para la institución*

Fuente: Encuesta aplicada, año 2021

Se observa que la cantidad de personas que laboran en cada uno de los segmentos proporcionados son similares, mostrándonos de esta forma que la cantidad de años de los encuestados es bastante proporcional.

En relación con la división de los encuestados en las áreas que laboran dentro de la institución, se puede observar la Imagen N°4, la cual es de gran importancia debido que, al tener participantes de la encuesta de diferentes áreas de la organización, se puede obtener un panorama más amplio de los diferentes conocimientos de los participantes, así como su nivel de educación es variado por lo que las respuestas van a ser más reales.

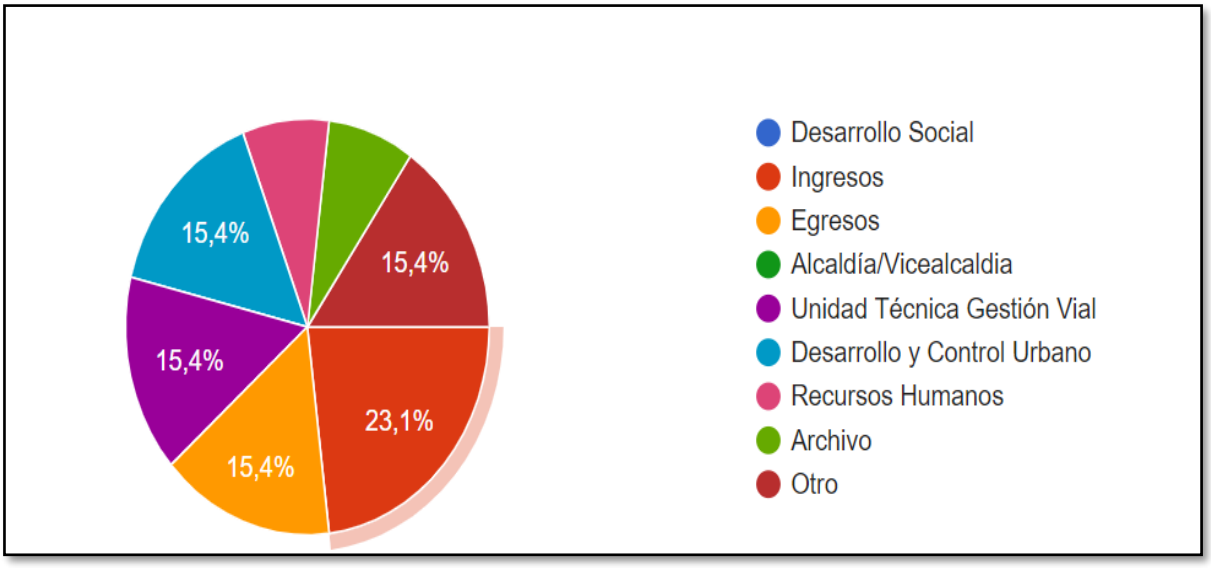


*Ilustración 4: Área a la que pertenece*

Fuente: Encuesta aplicada, año 2021

Cuando se consulta por la calidad del servicio de Internet en la municipalidad en estudio se obtiene como resultado que casi la mitad de los encuestados considera que es de regular a buena, tomando como mayor porcentaje la selección de la opción buena (53,8%). Lo anterior se puede apreciar en la Ilustración N°5:

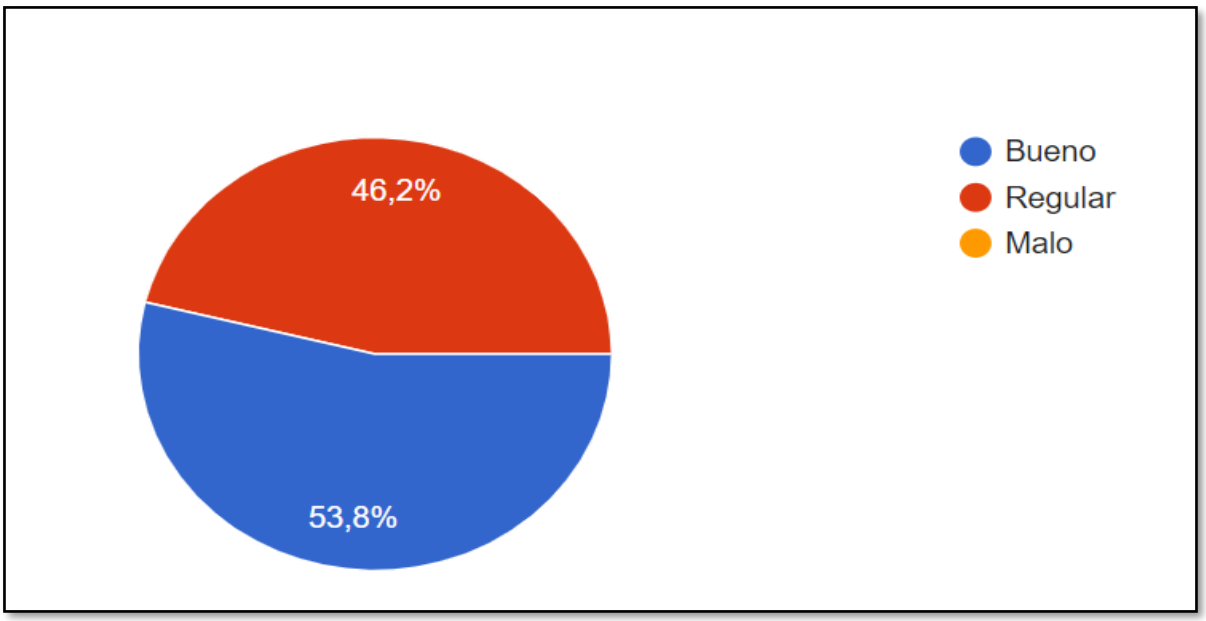


*Ilustración 5: Calificación del servicio de Internet*

Fuente: Encuesta aplicada, año 2021

En la Ilustración N°6, se observa el resultado de la pregunta sobre la importancia de las políticas de seguridad dentro de la institución. Considerando este resultado se puede interpretar que hay personas que aún desconocen de la importancia de la seguridad informática dentro de las organizaciones.

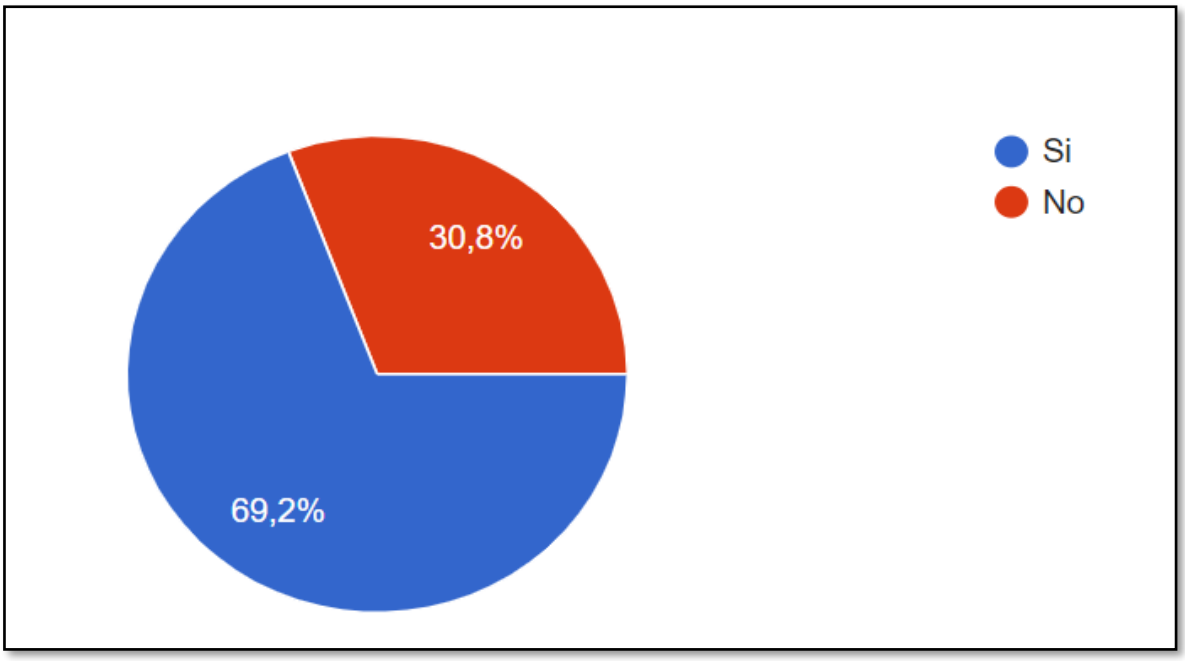


*Ilustración 6: Conoce las políticas de seguridad*

Fuente: Encuesta aplicada, año 2021

### 4.2 Observación al Departamento de Tecnologías de Información

A continuación, se detalla información obtenida de la observación realizada al Departamento de Tecnologías de Información de la institución en estudio. Además, del análisis general de los datos arrojados de las mismas.

Utilizando el diagrama de causa y efecto o bien, un diagrama de Ishikawa, se tomarán los resultados de la observación aplicada al Departamento de Tecnología de Información para poder identificar su principal problema, factores y subfactores influyentes.

Se observó que, en cuanto a materiales, existen protocolos y procedimientos de seguridad los cuales son aprobados por un superior dentro de la jerarquía institucional.

En cuanto a equipos o personal, se evidenció un exceso de control por parte de la jefatura, lo cual general una presión extra en los subalternos, lo que redunda en un clima laboral desfavorable y falta del trabajo en equipo, que se muestra disconforme con la falta de capacitaciones que reciben anualmente.

Dentro de los métodos de trabajo, utilizaban reportes de incidentes por medios establecidos y comunicados a los usuarios finales. Una vez ingresados los incidentes, aplican el método FIFO, por sus siglas en inglés First in, First out; así mismo se realiza un sobrecontrol de todos los procesos internos del departamento, donde deben de registrarse cada uno de los movimientos y comunicarlos a la jefatura inmediata, así como tener su visto bueno para realizar cualquier gestión.

Sobre el ambiente laboral, se tenían niveles jerárquicos bien establecidos, además existía una falta de habilidades blandas tanto en el personal como en las jefaturas y falta comunicación asertiva dentro del departamento de TI.

Dentro de los procesos, se obtuvo que la mayoría están tercerizados por la falta de personal para que puedan abarcar todos los proyectos tecnológicos que la Municipalidad requiere y necesita. Las áreas sensibles del área de Informática estaban muy accesibles a terceros y no se llevaba un control de acceso a las personas tanto internas como externas a la institución.

Como la mayoría de las instituciones públicas, la burocracia puede ser un aspecto negativo, para la compra de recursos de emergencia, contratación de personal y hasta para mejoras dentro de las oficinas que requieran materiales o mano de obra externa a la institución, por lo que se hace más complicadas las mejoras o bien la programación de proyectos cortos o de bajo impacto para la organización.

En la Ilustración N°7, se puede observar con detalle cada uno de los puntos indicados.

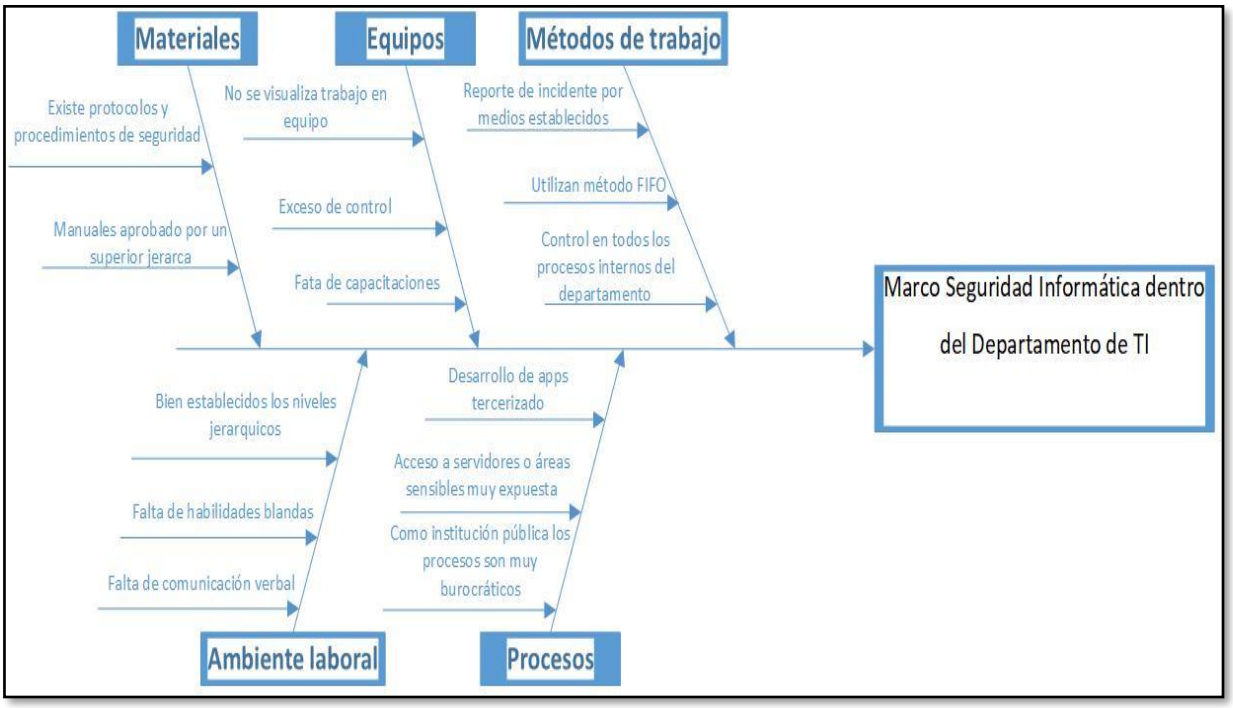


*Ilustración 7: Diagrama de Ishikawa*

Fuente: Observación aplicada, año 2021

# Capitulo V. Propuesta de Solución

Las amenazas en las TIC son globales, y están repartidas en distintos niveles de criticidad, según la orientación y el ámbito de su utilización. Es preocupante para grandes, medianas y pequeñas organizaciones el espionaje industrial, los ladrones de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información.

Dado lo anterior, en este capítulo se expone una estrategia para la gestión de políticas de seguridad informática en una municipalidad de la Región Chorotega, con el fin de minimizar el riesgo y la integridad del software y la información, la misma consta de 4 partes que se exponen a continuación.

## 5.1 Políticas de Monitoreo de la Municipalidad en Estudio

Los gobiernos locales deben alinearse con el marco de control que ofrece la Contraloría General de la República de Costa Rica, donde las políticas de monitoreo son necesarias para tener una infraestructura informática que minimice los riesgos asociados con la seguridad y los costos administrativos.

En la municipalidad en estudio, se coincide con que las políticas de monitoreo son necesarias, que deben aplicarse y aprobarse a niveles gerenciales importantes, así como darse a conocer en todo el ámbito organizacional. Sin embargo, las existentes no son de completo conocimiento de la organización, los miembros de la institución aseguran que falta información relacionada a temas de seguridad y las políticas establecidas en el Departamento de Tecnologías de Información.

Tal y como se expuso en el título Tabulación y Análisis de la Aplicación de Instrumentos, todas las políticas de monitoreo se tienen bajo papel, tomando en cuenta personas responsables, fechas y momentos en que deben realizar los monitoreos.  También, no se cuenta con controles monitorizados ni de monitoreo de redes. Es por ello que, se propone desarrollar en la Institución políticas de monitorización que puedan supervisar servidores y crear reglas para el envío de

correos electrónicos de notificación cuando sucedan ciertos eventos predeterminados por la organización en estudio. Esto permitirá obtener notificaciones en la vista de lista de servidores bajo una de columna “Avisos”. Además, puede activar el envío de estas notificaciones a las direcciones de correo electrónico establecidas para dar seguimiento oportuno

En cuanto al tema de redes de comunicación, se propone aplicar el Modelo OSI (Open Systems Interconnection), el cual es utilizado de referencia para los protocolos de red y está conformado por 7 capas o niveles, los cuales son necesarios para lograr la entrega de un paquete o que bien, que exista la comunicación.

Se debe tomar como referencia este Modelo para la gestión del tráfico de red dentro de la institución, de esta forma se dividirá cada una de las funciones de la comunicación en las 7 capas del Modelo OSI, para determinar en cual de ellas es donde pueden existir debilidades o posibles vulnerabilidades.

El modelo para utilizar se detalla en la Ilustración N°8:

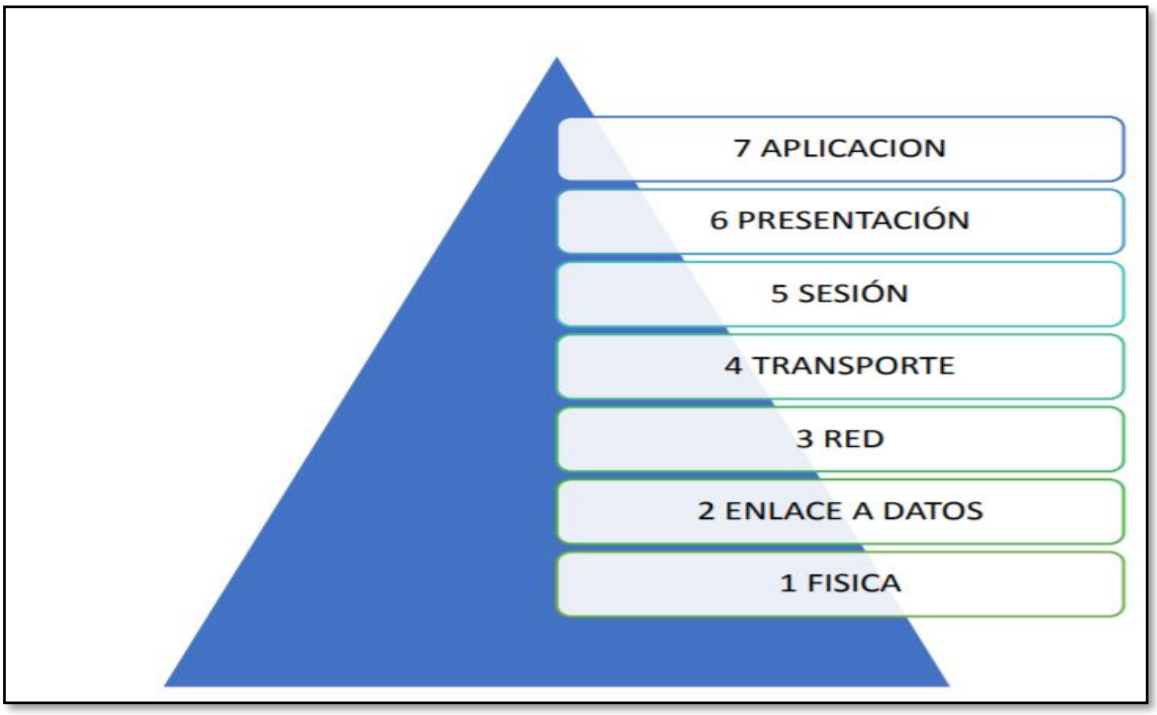


*Ilustración 8: Capas del modelo OSI*

Fuente: Elaboración propia, con base en Modelo OSI

El sistema de gestión propuesto operará bajo los siguientes pasos:

- Recolección de información acerca del estado de la red y componentes de los sistemas. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas. Utilizando herramientas para identificar monitorear estados de red, basadas en código abierto, como Zabbix o Nabios podremos identificar debilidades dentro de la red, posibles afectaciones y las acciones a realizar.
- Modificación de la información para presentarla en formatos apropiados para el mejor entendimiento del administrador. Es así como se presenta el informe completo para que sea gestionado por la persona a cargo, concentrar sus esfuerzos en diseñar una red segura, implementar soluciones, resolver problemas y mantener la infraestructura de redes para garantizar el rendimiento.
- Transporte de la información del equipo monitoreado. Como parte de una correcta gestión de información, se debe almacenar los datos de cada equipo monitoreado como un respaldo, realizar el traslado de manera integral para poder tener un registro histórico de las detecciones encontradas.
- Almacenar de los datos coleccionados. Los datos del equipo monitoreado deben de almacenarse en un repositorio de datos histórico, el cual puede ser accesible para el personal de Tecnologías de la Información.
- Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red. De esta forma, se podrá administrar y asegurar el funcionamiento correcto de las redes informáticas.
- Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor. Crear planes, manuales y procedimientos que se deberán acatar ante los eventos críticos o fallas en la red informática.

## 5.2 Mejoras por realizarse dentro del departamento de TI

Dentro del departamento de TI, deben de existir valores, herramientas blandas, herramientas de comunicación, habilidades y destrezas para trabajar en equipo, con el fin de impulsar la inteligencia emocional de equipo.

En la municipalidad en estudio, se propone generar un ambiente ameno, cordial y profesional, actualmente el clima organizacional de la empresa comprende un rubro muy importante para los colaboradores y puede ser un vínculo positivo dentro de la organización o un obstáculo en su desempeño.

Actualmente, se ha demostrado que el clima organizacional es muy importante en las empresas, porque es un factor que sabe mejorar la efectividad, rendimiento y productividad del capital humano de la empresa. El clima laboral incide en los comportamientos de las personas y por ello las empresas se preocupan por medirlo y conocerlo.

El ambiente afecta la estructura de las organizaciones, por la incertidumbre que causa en estas últimas. Algunas empresas encaran medios relativamente estáticos; otras, se enfrentan a unos que son más dinámicos. Los ambientes estáticos crean en los gerentes mucha menos incertidumbre que los dinámicos, y puesto que es una amenaza para la eficacia de la empresa, el administrador tratará de reducirla al mínimo. Un modo de lograrlo consiste en hacer ajustes a la estructura de la organización.

Para la municipalidad en estudio es importante mantenerse siempre actualizados con cursos de herramientas blandas, liderazgo y trabajo en equipo. Así mismo, generar un ambiente laboral agradable para que los todos puedan generar ideas, ser proactivos y utilizar de una manera más efectiva sus herramientas académicas.

Se debe intentar trabajar en equipo de la manera más eficiente de esta forma lograran agilizar los tiempos de respuesta en las atenciones de incidencias e inclusive en la gestión de proyectos informáticos.

A continuación, la tabla 1 detalla el plan de capacitación propuesto dirigido para diferentes áreas de la organización

| **Capacitación** | **Duración** | **Costo** | **Facilitador** | **Áreas Participantes** |
|---|---|---|---|---|
| Riesgos laborales | 2 horas | $300 - $600 | De acuerdo a SICOP | Todos los empleados municipales |
| Habilidades blandas | 4 horas | $500 - $700 | De acuerdo a SICOP | Todos los empleados municipales |

Tabla 1. Capacitaciones propuestas para habilidades blandas

Fuente: Elaboración propia, 2021

Dentro del Departamento de TI, se recomienda realizar las capacitaciones descritas en la Tabla 2, para aumentar el nivel de conocimiento en áreas de seguridad informática y de esta forma los mismos funcionarios de TI puedan después generar contenido para sus compañeros al exponer temas de importancia dentro del área de seguridad.

| **Capacitación** | **Duración** | **Costo** | **Facilitador** | **Áreas Participantes** |
|---|---|---|---|---|
| Seguridad Informática | 8 | $1000 | De acuerdo a SICOP | Unidad de Informática |
| Hacking y métodos de falsificación informática | 8 | $1000 | De acuerdo a SICOP | Unidad de Informática |

| | | | | |
|---|---|---|---|---|
| Seguridad Informática para usuarios finales | 8 | $0 | Departamento de TI Municipalidad | Todos los empleados municipales |
| Fomento del uso de los procedimientos elaborados en el departamento de TI | 8 | $0 | Departamento de TI Municipalidad | Todos los empleados municipales |

Tabla 2. Capacitaciones por realizar

Fuente: Elaboración propia, 2021

### 5.3 Infraestructura Tecnológica

Dentro de la infraestructura de la municipalidad en estudio, se evidenciaron debilidades en cuanto al antivirus, puesto que se está en trámites para trasladarse de proveedor o bien continuar con el mismo. Es por ello que se propone instalar un software de monitoreo de red.

Debe utilizarse una plataforma moderna de gestión de incidentes que garantiza que nunca se pasen por alto los incidentes críticos, así como que las personas adecuadas actúen en el menor tiempo posible. Es necesario contar con un software que reciba alertas de los sistemas de supervisión y aplicaciones personalizadas, y las categoriza en función de su importancia y plazo.

Se recomienda, en especial, utilizar software de código abierto o los común llamados “freeware”, tal es el caso de IP Address Tracker, que automáticamente descubre y brinda seguimiento a las direcciones IP, además se visualiza en tiempo real el uso de los datos. Como se observa en la Ilustración 9, el panel principal de la herramienta y como explora las diferentes IP’s detectadas.

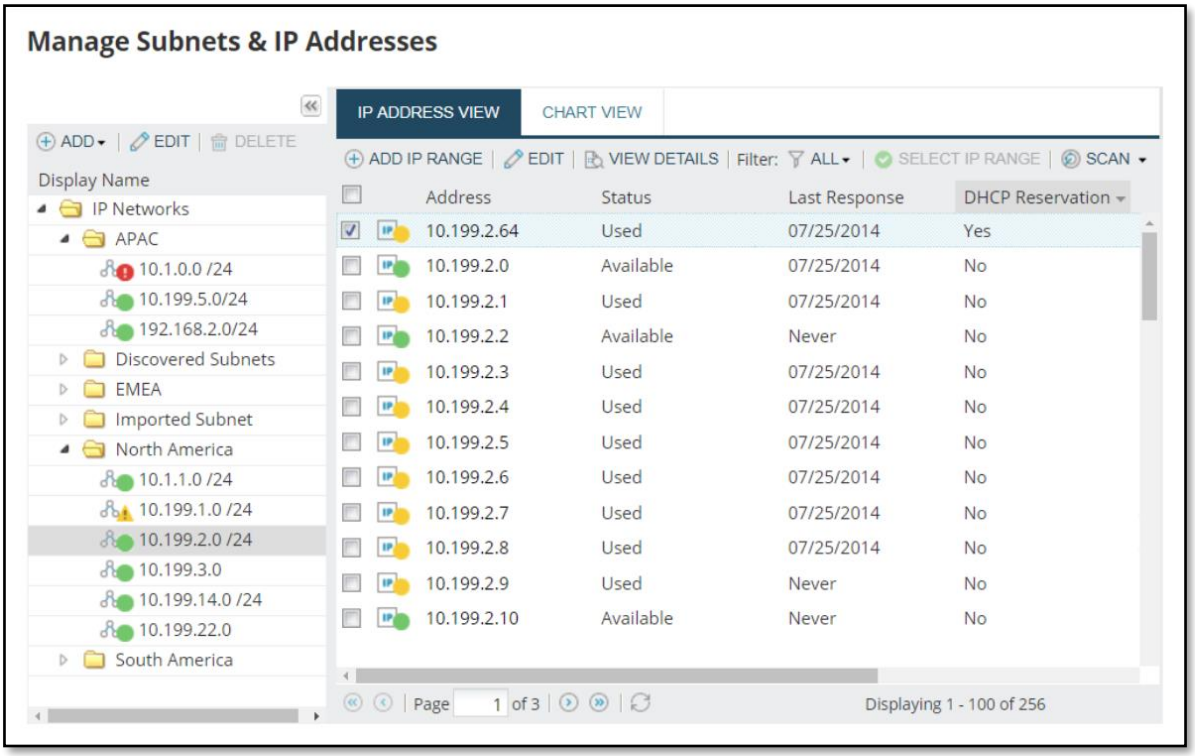


*Ilustración 9: IP Address Tracker Software*

Fuente: https://www.solarwinds.com/ip-address-manager

DBA xPress es una herramienta que también se recomienda utilizar para comparar las bases de datos y sincronizar el esquema y los datos entre ellos, también analizar dependencia y conexiones entre tables, usuarios, funciones y políticas de seguridad. Se puede automatizar las tareas, de esta forma ahorra tiempo y reducir el riesgo de errores humanos.

A continuación, en la Ilustración 10 se muestra el panel principal de la herramienta.

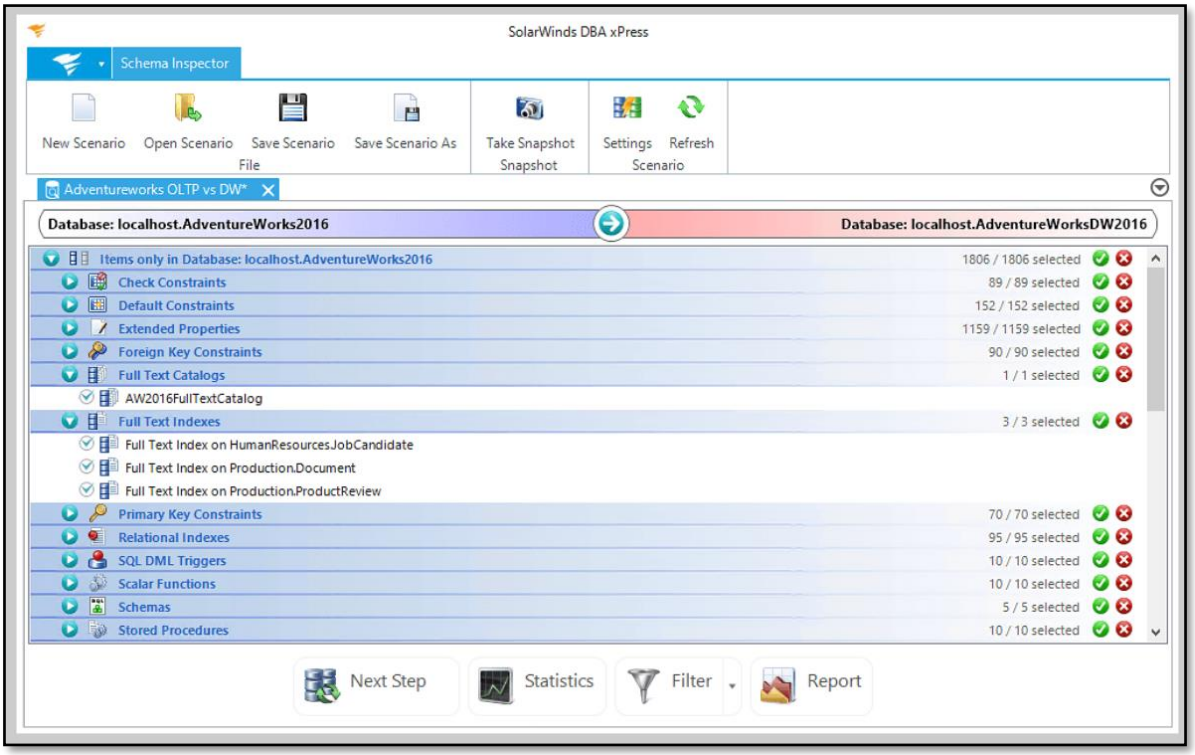


*Ilustración 10: DBA xPress Software*

Fuente: https://www.solarwinds.com/ip-address-manager

La herramienta puede crear comparaciones detalladas entre la información almacenada en dos diferentes bases de datos y ayuda a sincronizar los datos entre ellas. Cuando la comparación está completa, se pueden ver detalles como las filas de la tabla encontrada únicamente en la fuente o en el destinatario y las filas que son diferentes entre ellas.

En la Ilustración 11, se puede observar el panel inspector de la herramienta propuesta.

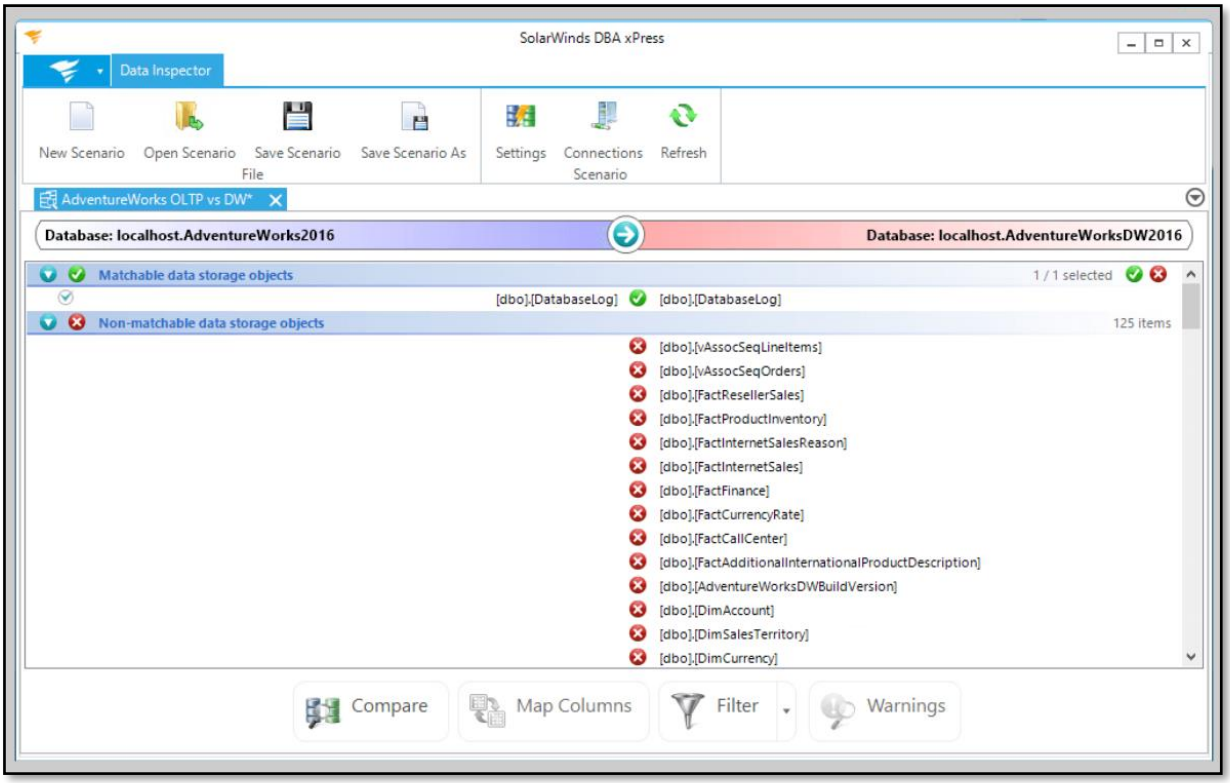


*Ilustración 11: DBA xPress Software*

Fuente: https://www.solarwinds.com/ip-address-manager

Otra herramienta que se recomienda utilizar es el Analizador para el Directorio Activo, a fin de identificar rápidamente los permisos de los usuarios, buscar permisos por usuario o por grupos y el análisis de permisos basados en la suscripción de grupos y permisos.

Con esta herramienta, podrá tener fácil acceso a los permisos de usuarios brindados, mejorar la seguridad y mitigar las posibles intrusiones internas, además brinda reportes sobre los datos de críticos.

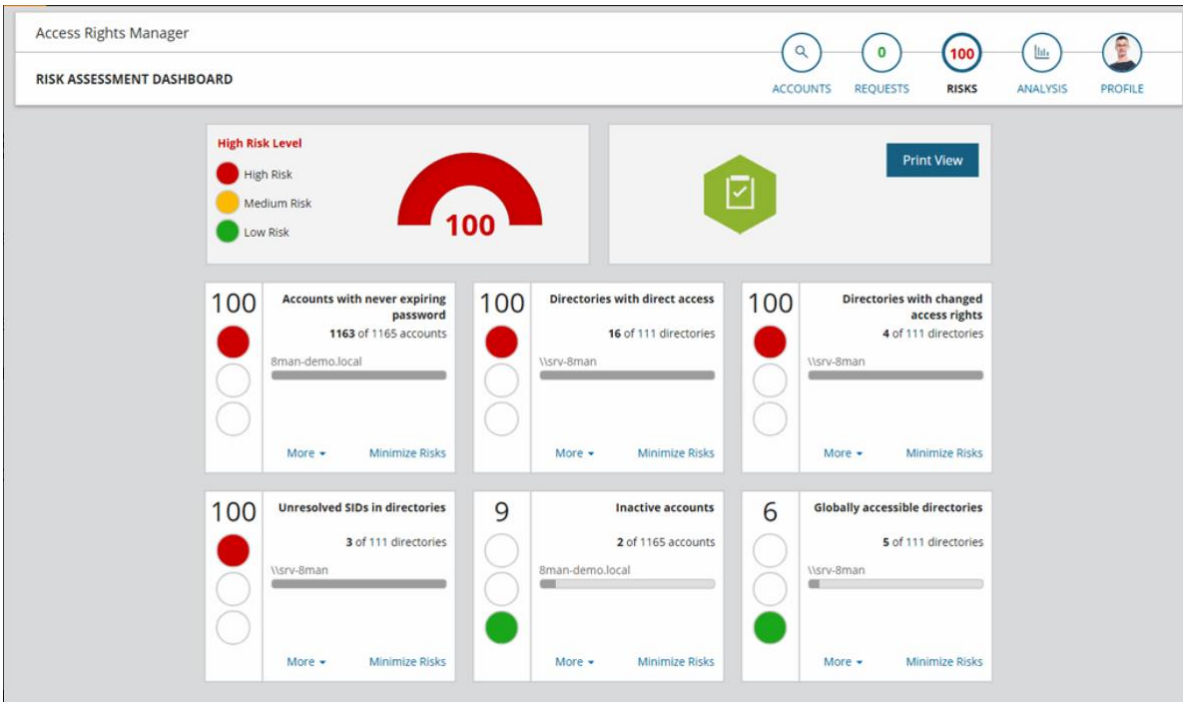


*Ilustración 12: Analizador para el Directorio Activo*

Fuente: https://www.solarwinds.com/free-tools/permissions-analyzer-for-active-directory

### 5.4 Políticas de Seguridad

Políticas de seguridad o manuales de procedimientos contienen una descripción de actividades a seguir. Es necesario especificar también las personas implicadas en el proceso, los responsables y los afectados, así mismo, se debe brindar un visto bueno por un alto jerarca dentro de la institución y comunicarlo a toda la organización.

A continuación, se propone una estructura básica de políticas de seguridad que permiten establecer un sistema de información o bien modificar el ya existente en la municipalidad en estudio, el responsable de realizar las políticas de seguridad siempre será el Encargado de Seguridad Informática de la Institución.

- Logotipo de la organización.
- Nombre oficial de la organización.
- Denominación y extensión: relacionada directamente con el índice determinado de acuerdo con la Unidad de Archivo para cada unidad.

- Lugar y fecha de elaboración.
- Número de páginas
- Número de revisión. se deberá indicar la cantidad de revisiones e irá relacionado con las versiones del documento.
- Unidades responsables de su elaboración, revisión y/o autorización: de acuerdo con el manual a elaborar se determinará quienes son los autores, los que revisaron el documento y quienes brindaron su autorización para la publicación de este dentro de la institución.
- Clave de la forma: en primer término, las siglas de la organización, en segundo lugar, las siglas de la unidad administrativa donde se utiliza la forma y, por último, el número de la forma. Entre las siglas y el número debe colocarse un guion o diagonal.

Además, debe contener las siguientes secciones dentro del documento:

- Índice: en este apartado se presentan de manera sintética y ordenada, los apartados principales que constituyen el manual.
- Introducción: se refiere a la explicación que se dirige al lector sobre el panorama general del contenido del manual, de su utilidad y de los fines y propósitos que se pretenden cumplir a través de él. Incluye información de cómo se usará, quién, cómo y cuándo hará las revisiones y actualizaciones, así como la autorización del titular de la Dependencia.
- Objetivos: el objetivo deberá contener una explicación del propósito que se pretende cumplir con el manual de procedimientos. El objetivo deberá ser lo más concreto posible, y su redacción clara y en párrafos breves; además, la primera parte de su contenido deberá expresar QUÉ SE HACE; y la segunda, PARA QUÉ SE HACE.
- Responsables: personas responsables de cumplir con ese manual
- Políticas o normas de operación: Descripción de las normas que se tomaron en cuenta para la realización de este
- Conceptos básicos: conceptos descriptivos para que todos los leyentes puedan entender lo redactado en el manual o política.

- Procedimientos: desarrollo del procedimiento, identificando alcance, responsabilidades y el método de trabajo.
- Diagramas de flujos: incorporar diagramas brinda una mejor oportunidad de aprendizaje a los lectores.
- Glosario de términos: glosario con los términos más importante dentro del manual

Para la elaboración de las políticas se deberán considerar los siguientes puntos:

- Las políticas serán lineamientos de carácter general que orienten la toma de decisiones en cuanto al curso de las actividades que habrán de realizar los servidores públicos en sus áreas de trabajo. Estas deberán ser claras y concisas, a fin de que sean comprendidas, incluso, por personas no familiarizadas con el procedimiento, asimismo serán específicas de la acción que regule el curso de las actividades en situaciones determinadas, serán de observancia obligatoria en su interpretación y aplicación.
- Deberán establecer las situaciones alternativas que pudieran presentarse durante la operación del procedimiento.
- Las políticas se definirán por los responsables de la operación de los procedimientos y serán autorizadas por el titular de la unidad administrativa correspondiente.
- Se preverá la posibilidad de incumplimiento de las situaciones normales y sus consecuencias o responsabilidades, ya sea porque no se den las condiciones supuestas, o porque se violen o alteren deliberadamente.
- Entre las políticas, han de existir jerarquías y secuencias lógicas de operación, por ejemplo, se propone: en el tema de incidencias del personal, exponer primero de retardos, luego de faltas y después de bajas.
- Las políticas considerarán disposiciones oficiales acerca de requisitos, así como de los responsables, recursos y usuarios que intervengan de manera determinante en la operación del procedimiento.

# Capítulo VI. Conclusiones y Recomendaciones

## 6.1 Conclusiones

Muchas instituciones públicas mantienen estructuras de comunicaciones complejas, debido a la necesidad de mantenerse comunicados con los clientes o en este caso sus contribuyentes; por lo que precisan de una buena administración de red que permita un mejor manejo y control de los elementos que la conforman.

Una buena herramienta para gestión de redes debe ser fácil de instalar y usar para que, de esta forma, se pueda llevar un correcta gestión y administración de los recursos de la red, sus posibles vulnerabilidades y forma en que podrían evitar un posible ataque.

Con la observación realizada al Departamento de TI, se logró conocer el marco de control que posee actualmente, abarcando las políticas de monitoreo y seguridad, manuales de procedimientos y vulnerabilidades dentro del departamento, es así como se logra ver desde una óptica más objetiva los debilidades y riesgos para brindar una propuesta integral y completa.

La institución contaba con algunos manuales de procedimientos y políticas de seguridad, pero les hace falta comunicarlos a los nuevos funcionarios, recordárselos a los funcionarios que tienen más tiempo y la forma de realizar esto es mediante capacitaciones, que incluyan a todos los funcionarios municipales.

Con el establecimiento de políticas de seguridad informática que permitan gestionar los riesgos del departamento dentro de la institución y la correcta comunicación de estas a sus colaboradores, pueden crear un ambiente controlado de la infraestructura tecnológica.

## 6.2 Recomendaciones:

Aplicar esta propuesta en la institución y comunicar a los demás colaboradores los cambios realizados en los manuales y procedimientos creados a partir de este documento.

Que el administrador de redes realice auditorías constantes del estado de la memoria y almacenamiento de los servidores, así como revisión de directorio activo. De esta forma, se estarán agregando más puntos de control para monitorear y verificar si se requieren actualizaciones de software importante.

Se recomienda una herramienta de monitoreo para los servidores que involucre el consumo y espacio de disco duro, memoria RAM, temperatura y acceso de terceros.

Se deben brindar capacitaciones sobre el manejo de estrés, trabajo en equipo, habilidades blandas y ponerlas en práctica diariamente tanto a lo interno del departamento de TI como a nivel de organización para brindar un servicio integran a los contribuyentes.

Se recomienda manejar la atención de incidentes de los usuarios internos, así como educarlos sobre las diferentes políticas y procedimientos que estarán realizando en pro de mejorar la gestión de TI dentro del Departamento de Informática de la Municipalidad en estudio.

# Capitulo VII. ANEXOS

## 7.1 Anexo 1

Cuestionario
Universidad de Costa Rica
Sistema de Estudios de Posgrados
Estudios de Posgrado en Computación e Informática

UNIVERSIDAD DE COSTA RICA

Objetivo: analizar el contexto informático en el que se desenvuelven los funcionarios de la institución a analizar.

Los datos recopilados por este medio serán utilizados únicamente con fines académicos.

I. Información General

1. Marque con una equis (x) los años que tiene laborando para la institución
   a) 1 a 5 años
   b) 5 a 10 años
   c) Mas de 10 años
2. Seleccione su genero
   a) Femenino
   b) Masculino
3. Seleccione el área a la que pertenece
   a) Desarrollo Social
   b) Ingresos
   c) Egresos
   d) Alcaldía/Vicealcaldía
   e) Unidad Técnica Gestión Vial
   f) Desarrollo y Control Urbano
   g) Recursos Humanos
   h) Otra_____

II. Percepción de los servicios informáticos brindados

1. ¿Como calificaría la calidad del servicio de internet brindado por la institución?
   a) Bueno
   b) Regular
   c) Malo

2. ¿Considera usted apropiado el uso que se le da a equipos de cómputo?
   a) Sí
   b) No
   c) No sé
3. ¿Conoce usted de políticas de seguridad implementadas en la institución?
   a) Sí
   b) No
4. ¿Comunica de manera oportuna cuando recibe un correo dudoso o sobre un posible hackeo de su cuenta?
   a) Siempre
   b) A veces
   c) Nunca
5. ¿Considera usted que es importante contar con políticas de seguridad dentro de la institución?
   a) Sí
   b) No
6. ¿Comparte información como nombres de usuario, contraseñas o accesos de sistemas a terceras personas?
   a) Si
   b) A veces
   c) No
7. ¿Están claramente identificados los procedimientos para la solicitud de accesos a los diferentes sistemas de la institución?
   a) Sí
   b) No
8. ¿Considera que existe alguna posibilidad de mejora para la institución en cuanto a la seguridad informática?

_____
_____
_____

¡Muchas Gracias!

## 7.2 Anexo 2

Guía de Observación
Universidad de Costa Rica
Sistema de Estudios de Posgrados
Estudios de Posgrado en Computación e Informática

UNIVERSIDAD DE COSTA RICA

Objetivo: conocer la forma en que se desenvuelve el entorno organizacional del departamento de Tecnologías de Información tomando en cuenta la seguridad informática.

Los datos recopilados por este medio serán utilizados únicamente con fines académicos.

| Aspectos a observar | Sí | No | No aplica | Observaciones |
|---|---|---|---|---|
| El personal conoce sobre los procedimientos informáticos de la institución | | | | |
| Se cuenta con acceso a las políticas de seguridad informática | | | | |
| Existe un encargado de seguridad informática dentro de la institución | | | | |
| Los manuales, procedimientos y políticas son aprobados por un superior jerárquico | | | | |
| Hay restricciones de acceso a áreas críticas dentro del departamento de TI | | | | |
| Están identificadas las áreas como: Cuarto de TI, Cuarto de Servidores, Cuarto de Telecomunicaciones, Oficina, área de soporte técnico | | | | |
| El personal conoce sobre el procedimiento para la solicitud de accesos (sistemas, dominio, correo electrónico) | | | | |
| Se brinda monitoreo de los servicios de antivirus establecidos por la institución | | | | |
| Existen políticas de control de acceso a los servidores | | | | |

| | | | | |
|---|---|---|---|---|
| Se utilizan control de puertos de entrada y salida por medio de firewall o antivirus | | | | |
| Existen reglas de acceso para las conexiones remotas a la red interna (trabajo remoto) | | | | |
| Se brindan capacitaciones al personal sobre temas relacionados a seguridad informática | | | | |
| Se envían correos brindando información al personal sobre temas de seguridad y buenas prácticas de las TIC's | | | | |
| Mantienen actualizados los servidores y equipos de trabajo de los funcionarios | | | | |
| Se crean manual de usuario para compartirlos con los funcionarios y estos sepan el buen uso de las herramientas tecnológicas | | | | |
| Se actualiza periódicamente el antivirus en servidores y equipos de trabajo | | | | |
| Los equipos tienen software actualizado | | | | |
| Se cuenta con un procedimiento establecido para el reporte de incidentes relacionados a seguridad informática | | | | |
| La documentación como políticas, manuales, directrices son de acceso público para los funcionarios | | | | |
| Al finalizar el periodo laboral de un empleado, se comunica al departamento de TI para proceder a eliminar los accesos de los servicios tecnológicos | | | | |
| Se realizan copias de respaldos internas y externas a la institución | | | | |
| Existen equipos de contingencia para solventar problemas urgentes o cambios de equipos defectuosos | | | | |

## Capitulo VIII. Referencias

Antonio, C., & Clavijo, D. (2006). Políticas de seguridad informática. 2(1), 86–92.

Fernández, V. (2020). *Fundamentos de Metodología de Investigación.* August. https://doi.org/10.3926/oss.38es

Hechos y preguntas frecuentes sobre los virus informáticos y el malware | Kaspersky. (n.d.). RetrievedOctober 25, 2020, from https://www.kaspersky.es/resource-center/threats/computer-viruses-and-malware-facts-and-faqs

Ledo, M. J. V., & Pérez, A. B. A. (2012). Gestión de la información y el conocimiento. *Revista Cubana de Educación Médica Superior*, 26(3), 474–484.

Lobo, E. J. (2014). Administración Pública Municipal. 135, 123–174.

Modelo OSI - Concepto, cómo funciona, para qué sirve y capas. (n.d.). Retrieved June 26, 2021, from https://concepto.de/modelo-osi/

Molina, P. (2019). *Trabajo de investigación sobre Seguridad Informática* (p. 23). Universidad Nacional de la Rioja.

Municipios: 200 años de un hito en la democracia de Costa Rica - La Nación. (n.d.). RetrievedNovember 14, 2020, from https://www.nacion.com/viva/cultura/municipios-200-anos-de-un-hito-en-la-democracia-de-costa-rica/Q3ASXUMIWZGZZBUBSTSYYTUVLU/story/

¿Qué es el malware y cómo funciona? | Definición de malware | Avast. (n.d.). RetrievedOctober 18, 2020, fromhttps://www.avast.com/es-es/c-malware

¿Qué es un virus informático? | La guía definitiva sobre virus informáticos | AVG. (n.d.). RetrievedOctober 18, 2020, from https://www.avg.com/es/signal/what-is-a-computer-virus

¿Qué son las TIC? | BMN. (n.d.). Obtenido16 octubre, 2020, de http://www.bmns.sld.cu/que-son-las-tic

Rica, D. C., María, E., & Chavarría, Z. (2016). De 1813 a 2016: 202 años de elecciones municipales. *Revista de Derecho Electoral, 21(1), 36–71.*

Romo, H. L. (1998). La metodología de encuesta. Técnicas de Investigación. En Sociedad, Cultura y Comunicación., 33–73.

Salazar, J. B., & Campos, P. G. (2009). Modelo para seguridad de la información en TIC*. CEUR Workshop Proceedings*, 488, 234–253.

Sampieri, R. H. (2014). *Metodología de la Investigación.*

Sánchez, E. D. (2008). Perspective. *Revista Electrónica Educare*, XII(7), 155–162. https://doi.org/10.1016/b978-0-240-80740-9.50147-1

Sánchez, E. D. (2008). Perspective. *Revista Electrónica Educare*, XII(7), 155–162. https://www.redalyc.org/articulo.oa?id=194114584020

Significado de TIC (Tecnologías de la información y la comunicación) (Qué son, Concepto y Definición) - Significados. (n.d.). RetrievedOctober 24, 2020, from https://www.significados.com/tic/

Sistema Costarricense de Información Jurídica. (n.d.). RetrievedOctober 18, 2020, from http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=40197&strTipM=TC

Taylor, S. ., &Bogdan, R. (2000). Introducción a los métodos cualitativos. In *Introducción a los métodos cualitativos de investigación* (p. 301).

Tecnologías de la información y las comunicaciones - EcuRed. (n.d.). RetrievedOctober 25, 2020, from https://www.ecured.cu/Tecnologías_de_la_información_y_las_comunicaciones

Vieites, Á. G. (2007). Enciclopedia de la Seguridad informática (p. 696). http://www.casadellibro.com/libro-enciclopedia-de-la-seguridad-informatica/9788478977314/1109334