INSTITUTO SUPERIOR TECNOLÓGICO
"DE TECNOLOGÍAS APROPIADAS"
INSTA

ISSN 2697-3308

INSTA MAGAZINE I+D

Investigación y Desarrollo

www.tecnologicoinsta.com | VOLUMEN 02, No. 01 - ENERO 2019

SUMARIO

Seguridad en Dispositivos Móviles: Amenazas Desconocidas en las Empresas

Cadena, Alejandra[1]

[1]*Instituto Superior Tecnológico de Tecnologías Apropiadas INSTA, Quito, Ecuador*

Resumen: Los dispositivos móviles en la actualidad se han convertido en una herramienta fundamental no solo a nivel profesional, estos dispositivos móviles son empleados para diversos fines, redes sociales, telemática, comercio electrónico, banca móvil, empresarial, entre otros. Por ese motivo, foco de atención para actos ilícitos tales como, suplantación de identidad, robo de datos y otros. Los delincuentes, especialmente aprovechan el desconocimiento de la ciudadanía en general acerca de estos temas, el desconocimiento y el nivel de implicaciones para una empresa o nivel personal hace de las prácticas ilícitas una corriente cada vez más común. Un estudio revelo que en América Latina el 74% de las empresas han sufrido un ataque por un problema de seguridad móvil y como consecuencia el robo de información. En ese sentido, en el presente artículo se aborda información relevante, que debe ser tomada en cuanta para mitigar esto que se ha convertido en una amenaza para todos quienes empleamos un dispositivo móvil.

Palabras clave: Ciberseguridad, robo de datos, malware.

Movile Device Unknown Threat in Companies

Abstract: Mobile devices today have become a fundamental tool not only at a professional level, these mobile devices are used for various purposes, social networks, telematics, electronic commerce, mobile banking, business, among others. For this reason, the focus of attention for illegal acts such as identity theft, data theft and others. Criminals, especially take advantage of the general public's ignorance about these issues, the ignorance and the level of implications for a company or personal level makes illegal practices an increasingly common trend. A study revealed that in Latin America 74% of companies have suffered an attack due to a mobile security problem and as a consequence the theft of information. In this sense, this article addresses relevant information, which must be taken into account to mitigate this, which has become a threat to all of us who use a mobile device.

Keywords: Cybersecurity, data theft, malware.

INTRODUCCIÓN

El uso de dispositivos móviles ha traído un gran beneficio a nivel empresarial pero claramente hay un riesgo por la manipulación de información, lo que conlleva el robo de datos para una posterior extorsión para la recuperación de los mismos, una gran vulnerabilidad es cuando en las empresas comparten vínculos corporativos para todos sus colaboradores. Un ciberataque conocido es una técnica que realiza la suplantación de identidad conocida como phishing, tiene como objetivo robar información confidencial y contraseñas para proporcionar accesos a la banca u otros archivos sensibles.
Los trabajadores de las empresas son los más vulnerables ya que cada uno dispone de un dispositivo móvil y pasa con el todo el día, a su vez la gran mayoría de personas desconoce de estas formas de ataque así como también no cuentan con recursos económicos para protegerse correctamente

Según datos del Instituto Nacional de Seguridad (Incibe), España sufrió el año pasado 123.000 ataques de ciberseguridad, un crecimiento exponencial si se tiene en cuenta que hace tres años se detectaron 18.000 delitos de este tipo, según expuso su director, Alberto Hernández Moreno.

Además, el vicepresidente de Cepyme, Gerardo Cuerva, precisó que el "53% de las pymes sufrieron un ataque cibernético en 2017″ y que nos encontramos "no sólo ante un problema empresarial, sino un problema estatal" (Ciberseguridad, 2018)

El peligro de los USB

En la mayoría de ataques a nivel de seguridad han sido causados por el mal uso de dispositivos de almacenamiento los cuales son conectados a un ordenador o dispositivo móvil.

Toda la información guardada en estos dispositivos no son cifrados y cuando existe un ultraje, esta información esta vulnerable y la mejor forma de proteger estos datos es mediante un cifrado y una contraseña, el formateo de un dispositivo no asegura la desaparición de la información, la utilización de antivirus actualizados permite analizar de manera continua los archivos, los dispositivos USB pueden ser más que memorias puede incluir micrófonos, cámaras lo que

mayra.cadena@insta.edu.ec

no son detectados por el antivirus, cabe recalcar que el dispositivo es una herramienta útil y sencilla pero de exenta de peligros. (Ciberseguridad, 2018)

Aplicaciones de Origen Desconocido

Ten cuidado con las aplicaciones que descargas, a menudo los hacker's se molestan en duplicar aplicaciones conocidas de pago para sacar copias en versión gratuita que pueden generar brechas en nuestra seguridad. Cuando descargues una app, observa el rendimiento del móvil durante un par de días: si se calienta o va mucho más lento de lo habitual ten cuidado.

El malware puede llegar de todas partes, desde una inocente aplicación de fotos hasta una guía para tu juego favorito. Existen muchos mecanismos para evitar estas aplicaciones maliciosas pero al final la responsabilidad recae en el propio usuario, quien debe ser consciente de qué está instalado y cómo puede llegar a afectarle. (Tecnologia, 2018)

Desventajas de Dispositivos Móviles

El hecho de trabajar con dispositivos móviles conlleva una serie de riesgos importantes para la seguridad de las empresas, como por ejemplo: pérdida o robo de información, el mal uso que se pueda hacer de los dispositivos robo de los mismos, robo de credenciales, utilización de sistemas de conexión no seguros, etc. (Android, 2017)

Ventajas de Dispositivos Móviles

La utilización de dispositivos móviles personales para uso profesional, proporciona muchas ventajas para la empresa y para el empleado, entre ellas: reducción de costes y ahorro en inversión de dispositivos reducción de costes en desplazamientos aumento en la productividad y en el rendimiento de trabajo del empleado mayor satisfacción y flexibilidad de los empleados que hace que aumente su compromiso con la empresa eficiencia en el servicio al gestionarlo en tiempo real. (Android, 2017)

Robo de Credenciales

La utilización de los dispositivos personales para uso corporativo en lugares fuera de la oficina como hoteles, medios de transporte, estaciones de trenes o aeropuertos, bares, restaurantes, etc. o la propia casa del empleado, los hace especialmente sensibles al posible robo de sus credenciales de acceso. Cualquier descuido como: abandonar el equipo sin bloquear la sesión de usuario tener apuntada una contraseña a la vista de los demás en un papel, post-it, etc. teclear la contraseña a la vista de los demás tener memorizadas las contraseñas de las aplicaciones que utilizamos puede llevar a que se produzca el robo de nuestras credenciales de usuario, y a que un usuario no autorizado pueda acceder a los recursos de nuestra empresa. La utilización de estos dispositivos en situaciones fuera del entorno empresarial y la relajación en la aplicación de las normas básicas de seguridad, hace que sea más sencillo que se produzca un robo de credenciales. Por ejemplo, podemos eliminar temporalmente la contraseña de acceso a nuestro smartphone para que nuestro hijo juegue con él, y olvidarnos restituirla. (Guia de dispositivos móviles, 2017)

Conexión A Redes Inseguras

Habrá situaciones en las que el empleado deba conectar a la red los dispositivos móviles fuera de la protección que brindan las redes privadas del entorno laboral. Ya sea por ahorro en la tarifa de datos, por no tener cobertura, por no disponer de cobertura 3G o 4G, es habitual utilizar redes públicas abiertas o poco seguras para el intercambio de correo electrónico corporativo o acceder a aplicaciones de la empresa. Este tipo de redes podemos encontrarlas como servicio de cortesía en bares, restaurantes, hoteles, aeropuertos, etc. Debemos desconfiar de estas redes ya que no sabemos quién puede estar detrás de ellas o quien las administra. Antes de utilizarlas, debemos informarnos cuál es el nombre de la red (SSID) y si está debidamente protegida para que nos podamos conectar con un mínimo de confianza. Hay casos en los que los ciberdelincuentes crean una red wifi en zonas públicas con nombres similares al del lugar donde se encuentran con el objetivo de capturar conexiones y recopilar información. (Guia de dispositivos móviles, 2017)

Medidas de Seguridad

Tanto los dispositivos móviles personales para uso profesional como la información corporativa que manejan estos, deben estar protegidos convenientemente, estableciendo unas buenas medidas de seguridad que ayuden a reducir todo lo posible los riesgos a los que están expuestos. A continuación se detallan algunas medidas que deben tenerse en cuenta para mitigar los riesgos a los que nos enfrentamos. Medidas como: la debida protección de la información la correcta configuración de los dispositivos o la protección de la conexión a redes inalámbricas Para implementar estas medidas, podemos incorporar herramientas específicas que gestionan dispositivos móviles y el uso de la información corporativa que se realice desde estos. En el mercado, existen diversas soluciones como los programas de gestión de dispositivos móviles o MDM (del inglés Mobile Device Management) que administran y monitorizan los dispositivos móviles de nuestras empresas. De esta forma, tendremos controlados los dispositivos y podremos valorar el grado de implantación de las medidas de seguridad de nuestra política de seguridad. Con estas herramientas será posible gestionar y controlar: los dispositivos autorizados para acceder a aplicaciones y recursos las aplicaciones instaladas en los dispositivos las configuraciones de seguridad de los dispositivos, de su wifi y de su VPN las manipulaciones indebidas de los terminales como la detección de jailbreak en iOS o rooteo en Android el bloqueo remoto de dispositivos extraviados la destrucción/formateo remoto de datos de dispositivos extraviados o robados el cifrado de datos o del dispositivo la detección de malware la fortaleza y renovación de contraseñas, etc. En el caso especial de los dispositivos personales para uso en la empresa, debemos de tener especial cuidado. Para asegurarnos el éxito de la implementación de todas estas medidas, es esencial conseguir involucrar a los usuarios en la protección de sus dispositivos. Debemos incentivar, concienciar y formar al usuario para que tome medidas destinadas a proteger los datos corporativos y personales por igual. (Emprendedores, 2018)

Autentificación Biométrica

En línea con las amenazas y la incipiente preocupación por la protección de la privacidad, el informe destaca la consolidación de los sistemas de autentificación biométrica como el elemento más habitual para el desbloqueo de estos dispositivos.

En definitiva, estas son solo algunas de las previsiones en cuanto a las amenazas a uno de los dispositivos más importantes para llevar a cabo las acciones del día a día en una sociedad cada vez más digitalizada.

Por ello, para no poner en peligro la sociedad del bienestar y las innovaciones tecnológicas, es necesario una investigación continua y la formación de profesionales en un área donde la oferta y la demanda aún no se encuentran para dar solución a los problemas en ciberseguridad. (Emprendedores, 2018)

Análisis en datos de Ciberdelincuencia.

La ciberdelincuencia no tiene fronteras y la impunidad que proporciona la distancia, los delitos son perpetrados a miles de kilómetros, impide además actuar de manera contundente y precisa. La ciberseguridad es una ciencia viva, evoluciona a la vez que los riesgos y amenazas, requiere de un rápido aprendizaje y aportar soluciones también ágiles, y precisa de profesionales en constante observación y alerta.

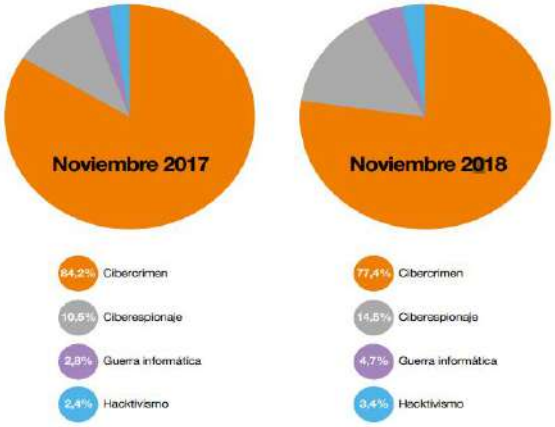

Figura 1. Motivaciones de la Ciberdelincuencia

Las amenazas son mayores que la capacidad de monitorizarlas: el 44% de las amenazas diarias no se investigan.

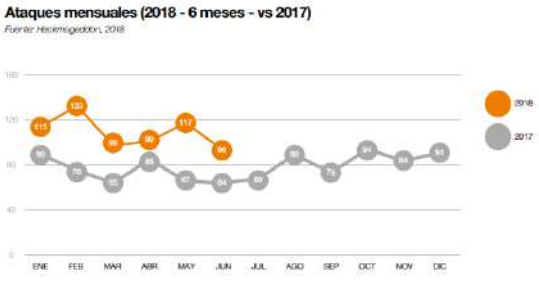

Figura 2. Ataques mensuales año 2017-2018

En el 69,9% de los ordenadores y el 77,9% de los teléfonos móviles analizados en España se han encontrado archivos maliciosos. Las empresas han pasado de sufrir 18.000 ciberataques a más de 100.000 desde 2014. La inversión en ciberseguridad de las empresas en España se ha duplicado desde 2012. La ciberseguridad con un ritmo de crecimiento anual del 13%, y creará más de 1 millón de puestos de trabajo en Europa. (Guia de dispositivos móviles, 2017)

Conexión a Redes Inseguras

Habrá situaciones en las que el empleado deba conectar a la red los dispositivos móviles fuera de la protección que brindan las redes privadas del entorno laboral. Ya sea por ahorro en la tarifa de datos, por no tener cobertura, por no disponer de cobertura 3G o 4G, es habitual utilizar redes públicas abiertas o poco seguras para el intercambio de correo electrónico corporativo o acceder a aplicaciones de la empresa. Este tipo de redes podemos encontrarlas como servicio de cortesía en bares, restaurantes, hoteles, aeropuertos, etc. Debemos desconfiar de estas redes ya que no sabemos quién puede estar detrás de ellas o quien las administra. Antes de utilizarlas, debemos informarnos cuál es el nombre de la red (SSID) y si está debidamente protegida para que nos podamos conectar con un mínimo de confianza. Hay casos en los que los ciberdelincuentes crean una red wifi en zonas públicas con nombres similares al del lugar donde se encuentran con el objetivo de capturar conexiones y recopilar información. (Guia de dispositivos móviles, 2017)

Medidas de Seguridad

Tanto los dispositivos móviles personales para uso profesional como la información corporativa que manejan estos, deben estar protegidos convenientemente, estableciendo unas buenas medidas de seguridad que ayuden a reducir todo lo posible los riesgos a los que están expuestos. A continuación se detallan algunas medidas que deben tenerse en cuenta para mitigar los riesgos a los que nos enfrentamos. Medidas como: la debida protección de la información la correcta configuración de los dispositivos o la protección de la conexión a redes inalámbricas Para implementar estas medidas, podemos incorporar herramientas específicas empresa. La utilización de los dispositivos personales para uso corporativo en lugares fuera de la oficina como hoteles, medios de transporte, estaciones de trenes o aeropuertos, bares, restaurantes, etc. o la propia casa del empleado, los hace especialmente sensibles al posible robo de sus credenciales de acceso. Cualquier descuido como: abandonar el equipo sin bloquear la sesión de usuario tener apuntada una contraseña a la vista de los demás en un papel, post-it, etc. teclear la contraseña a la vista de los demás tener memorizadas las contraseñas de las aplicaciones que utilizamos puede llevar a que se produzca el robo de nuestras credenciales de usuario, y a que un usuario no autorizado pueda acceder a los recursos de nuestra empresa. La utilización de estos dispositivos en situaciones fuera del entorno empresarial y la relajación en la aplicación de las normas básicas de seguridad, hace que sea más sencillo que se produzca un robo de credenciales. Por ejemplo, podemos eliminar temporalmente la contraseña de acceso a nuestro smartphone para que nuestro hijo juegue con él, y olvidarnos restituirla. (Guia de dispositivos móviles, 2017)

CONCLUSIONES

Los dispositivos móviles sufren de constantes amenazas, debido a que guardan información personal y empresarial, en ese sentido, son el principal y punto de ataque. Con la evolución de la tecnología, los móviles están expuestos a redes externas poco seguras, así como, a aplicaciones de origen desconocido.

En el último año la ciberdelincuencia se ha incrementado más de lo habitual, debido a que el robo de información se ha convertido en un gran negocio, el phishing es un ejemplo de secuestro de información que pretende extorsionar a la víctima a cambio de la recuperación de datos.

BIBLIOGRAFÌA

Android, K. (2017). *Seguridad en los androids.* Obtenido de https://www.xatakandroid.com/seguridad/he-instalado-todos-los-malware-de-android-esto-es-lo-que-ocurre-si-te-saltas-los-consejos-de-seguridad

Ciberseguridad. (2018). *Seguridad en dispositivos móviles: la mayor ciberamenaza está al alcance de tus manos.* Obtenido de [1]: https://www.iniseg.es/blog/ciberseguridad/seguridad-en-dispositivos-moviles/

Emprendedores. (2018). *Claves de seguridad para el móvil.* Obtenido de https://www.emprendedores.es/gestion/a27551265/claves-ciberseguridad-movil-seguridad-informatica-empresas/

móviles, G. d. (2017). *Dispositivos móviles personales para uso profesional BYOD.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

Tecnologia. (2018). *Peligro en los usb.* Obtenido de https://ticnegocios.camaravalencia.com/servicios/tendencias/guia-ciberseguridad-el-peligro-de-los-usb/

Análisis de Cableado Estructurado para Empresas PYMES.

Ordoñez, Luis [1]

[1]*Instituto Superior Tecnológico de Tecnologías Apropiadas INSTA, Quito, Ecuador*

Resumen: El cableado estructurado es un sistema que permite administrar y dar seguridad a las conexiones de la red de datos, permitiendo abaratar costos y soportando escalabilidad. El sistema de cableado estructurado es muy importante para una empresa porque garantiza seguridad y confiabilidad acerca de la información, proporcionando seguridad y garantizando que efectividad

Palabras clave: Cableado estructurado, pymes, normas, estándares, negocios pequeños y medianos

Analysis of Implementation of Structured Cabling for PYMES Business

Abstract: Structured cabling is a system that allows the administration and security of the data network connections, allowing lower costs and supporting scalability. The structured cabling system is very important for a company because it guarantees security and reliability about the information, providing security and guaranteeing its effectiveness.

Keywords: Structured cabling, PYME, Standards and standards, small and medium businesses.

INTRODUCCIÓN

El sistema de cableado estructurado es un método mediante el cual se puede administrar, mantener y mejorar las conexiones hacia los diferentes puestos de trabajo ya sea internamente es decir dentro de un edificio o a nivel metropolitano.
En la actualidad existen muchas empresas pymes que no aplican el sistema de cableado estructurado llevando a un desorden total y un gasto innecesario a la hora de dar mantenimiento a las conexiones de datos.
Por otra parte, las empresas pymes en la actualidad hacen caso omiso a la infraestructura de red de datos eso provoca una mala administración descuidándose del control de la intranet lo cual provoca un gasto innecesario y muy fuerte al reparar los daños o al dar mantenimiento de la red de datos sin tomar en cuenta el control de la intranet lo cual provoca un gasto innecesario y muy fuerte al reparar los daños o al dar mantenimiento de la red de la empresa.
Es muy importante que las empresas de pequeños y medianos negocios tomen en cuenta la infraestructura de la red de datos, en la actualidad existen muchos servicios los cuales viajan mediante la red de datos incluso video, y acceso de seguridad.
Este articulo también menciona algunos parámetros de estandarización y normas para el buen manejo del cableado estructurado, no se cita todas las normas porque son muy extensas, pero se cita las nomas más importantes y las necesarias para garantizar un buen cableado estructurado.

Cableado estructurado para un sistema de red de datos

El término de cableado estructurado es interpretado como un sistema de conexiones conformados por conectores, cables, ductería y dispositivos de conexión de red de datos, los cuales permiten la conexión con los diferentes dispositivos informáticos ya sea impresoras, computadoras, data-show y en la actualidad inclusive con pantallas interactivas.
El cableado estructurado tiene como finalidad mejorar y proteger las conexiones de la intranet de una empresa de manera global sin importar las dimensiones que dichas empresas tengan relacionadas con la infraestructura.

El cableado estructurado es un método que está basado en normas y estándares internacionales el cual permite la integración de voz, datos, video y control de acceso.
El cableado estructurado se divide en dos subsistemas cableado estructurado horizontal y cableado estructurado vertical

Cableado estructurado horizontal

Este subsistema permite la conexión desde el distribuidor de piso hacia los diferentes equipos informáticos ya sean estas computadoras, impresoras, pantallas de proyección o copiadoras. (Cruz & Hegel , 2013)

.

luis.ordonez@insta.edu.ec

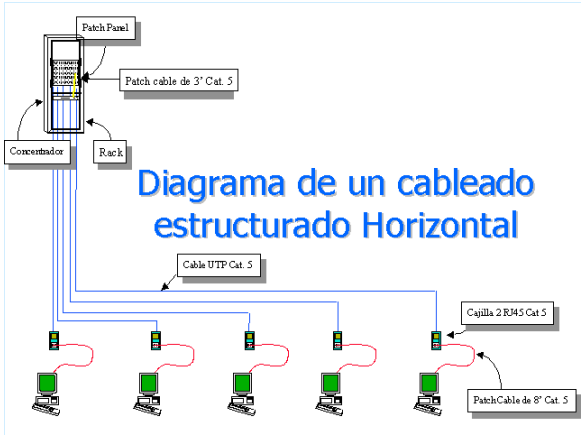

Figura 1: Subsistema cableado estructurado horizontal

Cableado estructurado vertical

Este subsistema permite la conexión desde el backbone principal ubicado en algún piso hacia los diferentes pisos del edificio. (Cruz & Hegel , 2013)

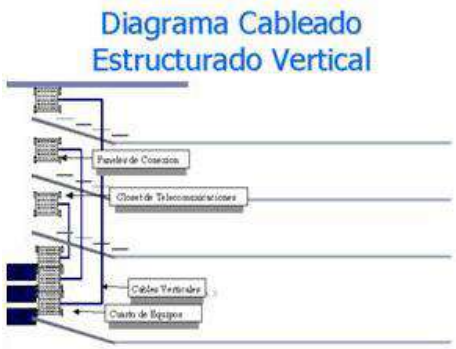

Figura2: Subsistema cableado estructurado vertical

Estos dos subsistemas conforman la estructura de una intranet, la cual nos permite interactuar con los diferentes dispositivos informáticos de la interna.

Normas y estándares del cableado estructurado

Estas normas y estándares rigen el Instituto Nacional Americano de Normalización ANSI, dicho organismo está encargado de aprobar normas y estándares para el cableado estructurado.
Existen varias normas y estándares que se aplica al cableado estructurado ya que se tiene normas para la seguridad, infraestructura y métricas de cable de red de datos.
En este artículo vamos a revisar las más relevantes para mantener un buen cableado estructurado para las empresas pymes.

Norma ANSI/TIA/EIA-568 B
Norma que plantea la instalación de cableado en edificios comerciales y de negocios. (Joskowicz, 2006)
Norma ANSI/TIA/EIA-569-A
Norma para adecuar la ubicación del cuarto de servidores o data center, así como la mejor ruta por donde pasa el cableado de par trenzado. Además, esta norma define la infraestructura del cableado de telecomunicaciones median tuberías, cajas de paso, canaletas con el objetivo de mejorar la protección y el buen funcionamiento del cableado estructurado para el futuro. (Joskowicz, 2006)
Norma EIA/TIA 570
Norma que describe la infraestructura necesaria para soportar la variedad de servicios dentro de una residencia o negocio pequeño (PYME). Estos sistemas en la actualidad incluyen datos, voz, video e inclusive accesos de control, así como también seguridad. (Joskowicz, 2006)

Empresas pequeñas y medianas pymes

Una pyme es una empresa pequeña o mediana que depende del número de trabajadores, volumen de ventas, años en el mercado y su nivel de producción. Se podría decir en el Ecuador hay más de un millón de pymes las cuales por el número de empleados y la mínima infraestructura no aplican el sistema de cableado estructurado.

Por lo general este tipo de empresas suelen tener infraestructuras de no más de dos pisos e incluso existen pymes que tiene de infraestructura un solo piso para poder trabajar, esto conlleva a que dichas empresas no inviertan en un sistema de cableado estructurado tomando en cuenta lo muy importante que hoy en día significa la tecnología para el crecimiento de las empresas. (Vásquez Saltos, 2013)

En la actualidad ya se habla de internet de las cosas y se podría decir que las conexiones tanto de voz, datos, videos y control de accesos va de la mano del cableado estructurado, entonces es muy necesario que las empresas pymes apliquen un sistema de cableado estructurado de tal manera que las pymes crezcan tanto a nivel de negocio como a nivel de tecnología.
Según el método utilizado de la visualización se sabe que la gran parte de empresas pymes no tiene cableado estructurado y se podría decir que es una falencia en cuanto a crecimiento de la empresa pyme. Según mi punto de vista si las pymes aplicaran un sistema de cableado estructurado, es decir utilizar las normas y estándares para mejorar rutas de acceso de cableado, canaletas decorativas, identificación de puntos de red de datos y seguridad en cuanto a seguridad de energía eléctrica las empresas gastarían menos dinero en mantenimiento y arreglo de una red de datos en caso de daño o fallas de conexión.

CONCLUSIONES

Mediante este análisis se puede concluir y recomendar a empresas pymes, considerar invertir en un sistema de cableado estructurado ya que, entre otras, permite crecer tanto a nivel de negocio como a nivel tecnológico.

Hoy en día existen varios profesionales tecnólogos, que cuentan con la experiencia para realizar la implementación de un sistema de cableado estructurado.

RECOMENDACIONES

Es recomendable considerar las llamadas normas y estándares, en la implementación del cableado estructurado ya que gracias a ellas podemos estandarizar y dar seguridad a la infraestructura de la red interna denominada también intranet.

Aplicando de manera efectiva las normas y estándares del sistema de cableado estructurado, se garantiza la conexión de red de datos, video, voz y control de accesos y, además, se garantiza que el cableado de red se mantenga en óptimas condiciones durante mucho tiempo.

Finalmente, el sistema de cableado estructurado permite la escalabilidad de la red interna, por tal motivo, bajaría el costo del mantenimiento y futuras conexiones da datos.

BIBLIOGRAFÌA

Cruz , P., & Hegel , B. (2013). *edes: instalación, administración y soporte.* Macro.

Joskowicz, J. (2006). *Cableado Estructurado.* Montevideo, Uruguay.

Vásquez Saltos, L. (2013). *Ecuador su realidad: 2013 – 2014.* Ecuador: Edagar Tello.

Sistema Start-Stop: Implementación como Mecanismo de Reducción de Combustible

Congacha, Jorge [1]

[1]*Instituto Superior Tecnológico de Tecnologías Apropiadas INSTA, Quito, Ecuador*

Resumen: En la actualidad a nivel mundial la principal fuente de energía es el petróleo, sin embargo, el consumo de este hidrocarburo presenta varios problemas por su escasez, costo y contaminación. Actualmente en el área automotriz existen varias tecnologías encaminadas a disminuir el impacto negativo de este elemento. El sistema Star Stop,es un sistema automático de encendido y apagado del vehículo en situaciones frecuentes como la luz roja de un semáforo o congestión vehicular, este mecanismo evita la contaminación que emite el vehículo cuando se encuentra en ralentí, y permite el ahorro de combustible. En ese sentido el presente artículo sustenta bibliográficamente y mediante un ensayo práctico la posibilidad de adaptar este mecanismo en vehículos que no cuenta con esta tecnología.

Palabras clave: Star-stop, reducción, combustible, consumo

Start-Stop System: Implementation as a Fuel Reduction Mechanism

Abstract: At present worldwide the main source of energy is oil, however, the consumption of this hydrocarbon presents several problems due to its scarcity, cost and pollution. Currently in the automotive area there are several technologies aimed at reducing the negative impact of this element. The Star Stop system is an automatic system for turning the vehicle on and off in frequent situations such as the red light of a traffic light or traffic congestion, this mechanism avoids the pollution that the vehicle emits when it is idling, and allows fuel savings. In this sense, the present article bibliographically supports the possibility of adapting this mechanism in vehicles that do not have this technology.

Keywords: Star-stop, reduction, fuel, consumption.

INTRODUCCIÓN

El continuo aumento de precios de los combustibles fósiles, la mayor severidad de las leyes sobre las emisiones de escape que rigen el territorio nacional y la conciencia ambiental creó la necesidad de buscar posibilidades que permitan reducir el consumo energético y las emisiones de gases contaminantes.

En Quito también hay un uso excesivo del vehículo particular, porque está valorado no solo como un medio de transporte sino como un elemento de status y una aspiración social congestión vehicular presentan, según la edición 2018 de la tabla global sobre tráfico Inrix. Estos datos revelaron que en Quito se pierden 173 horas en atascos al año. (Carvajal, 2019)

El 52% de emisiones de CO_2 en Quito proviene de vehículos. El 35% es industrial y el 13%, producto de la basura. La huella de carbono es la medición del impacto que causa una persona o actividad mediante la liberación a la atmósfera de dióxido de carbono (CO_2). En 2015, las emisiones de CO_2 sumaron 5,7 millones de toneladas en la capital. De ellas, el 52% está vinculado a la combustión de diésel y gasolina para transporte; 35% al consumo de energía por parte de la industria (generación eléctrica y uso de gas y diésel) y 13% a la descomposición de residuos sólidos. (Enríquez, 2017)

El consumo de combustibles realizado por los vehículos depende del escenario o condiciones presentes, como: cilindraje, tráfico, carga, tipo y característica de la vía, provocando cantidades diferentes de consumo, es así que de acuerdo a la investigación, el consumo de combustible aumenta desde un 30% en los vehículos al circular en tráfico por vías urbanas o periféricas. (Lopez, 2013)

Los avances tecnológicos son importantes para mejorar la eficiencia energética y reducción de la contaminación. El sistema Start-Stop que se encarga de detener el motor automáticamente por un lapso de tiempo corto, al encontrarse el vehículo estático sea en un semáforo, un cruce o en el caótico tráfico de la ciudad de Quito. Para reanudar la marcha del motor no es necesario girar nuevamente la llave del switch de encendido, tan solo apretar el acelerador como en una condición de conducción normal.

Este trabajo se elaboró con el propósito de generar un impacto social en el ámbito automotriz tanto de propietarios de vehículos, así como en autoridades encargadas de la gestión de la calidad de aire, direccionado a disminuir el consumo de combustibles y la contaminación ambiental.

jorge.congacha@insta.edu.ec

Se recolectó información técnica relevante de otros estudios relacionados con este tema para dar a conocer los aspectos relevantes, es así como se fundamentó el estudio de la presente investigación.

Análisis del Sistema

El sistema Start-Stop es un sistema que sirve para reducir el consumo de combustible, porque se encarga de parar el motor automáticamente en las fases en las que el vehículo se ha detenido, y no se considera necesario su activación, volviendo a arrancarlo cuando detecta que el conductor quiere ponerse en marcha. La activación de la función Start-Stop se efectúa de una manera automatizada.
El funcionamiento del sistema Start-Stop se realiza a través de la gestión electrónica del motor y va integrado en el software de la unidad de control del mismo.

Componentes del Sistema

Los dispositivos eléctricos que componen el sistema start-stop son el motor de arranque, la batería, módulos y demás sistemas de conexión y transmisión de datos

Motor de arranque

El motor de arranque consiste básicamente en un motor eléctrico auxiliar alimentado por corriente continua con imanes de tamaño reducido, empleado para facilitar el encendido del motor de combustión interna.[4] Por otro lado, es importante destacar que el motor de arranque es puesto en funcionamiento con ayuda de la batería del auto, ya que esta le genera y almacena la corriente eléctrica necesaria para que este produzca a su vez energía mecánica que se transmitirá al motor haciéndolo poner en marcha.

En un motor de arranque para un sistema start-stop, el número de solicitaciones para la puesta en marcha incrementa en comparación con las realizadas en auto convencional. Esto influye directamente en un mayor consumo de corriente.

.

Figura 1: Motor de arranque

Batería

La batería es un elemento que generalmente encontramos en el vano del motor de nuestro vehículo. Su finalidad reside en el almacenaje y producción de la energía eléctrica necesaria, por medio de un proceso químico.

Está constituida por un acumulador que por lo general tiene nueve placas: cinco negativas y cuatro positivas, unidas de manera alterna por medio de un puente. Cada una de las partes de la batería está en un compartimento con una solución electrolítica que se compone de agua destilada y ácido sulfúrico, por lo que al combinar esta disolución con las distintas placas de plomo, se produce una reacción química que genera corriente eléctrica. Cuando administramos electricidad a la batería, el proceso se invierte haciendo volver el sulfato desde las placas hasta el electrolito. (Rueda, 2005)

Figura 2: Batería del vehículo

El sistema start-stop genera una gran demanda de consumo de corriente de las baterías debido a que requiere arrancar el automóvil varias veces al día. En comparación con una batería convencional, aquellas utilizadas para aplicaciones start-stop deben tener como función primaria la habilidad de encender el motor un elevado número de veces y mantener períodos extendidos de motor apagado.

Unidad de mando

La unidad de control electrónico es un dispositivo que toma señales del estado en tiempo real del vehículo, que pueden provenir de los diferentes subsistemas, específicamente del motor, es encargada de realizar operaciones basadas en un algoritmo y ejecutar acciones a través de los actuadores del sistema.

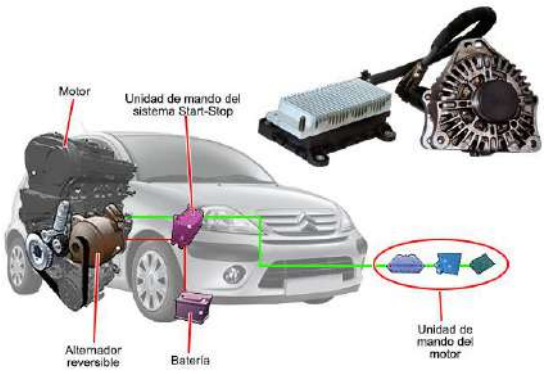

Figura 3: Unidad de mando

Para el sistema Start-Stop es importante saber si el nivel de carga de la batería de arranque, temperatura del motor, velocidad de desplazamiento del vehículo, marcha seleccionada, para permitir volver a arrancar el motor. Este proceso se denomina, predicción de estatus del vehículo, lo que significa que se evalúan todas las propiedades y valores del motor en lo que respecta un nuevo arranque.

Las señales necesarias para saber el estado del vehículo se detallan continuación

Sensor CKP

El sensor CKP (Sensor de posición del cigüeñal) es un dispositivo electrónico utilizado en un motor de combustión interna, tanto de gasolina como en motores de combustible diésel, para controlar la posición o la velocidad de rotación del cigüeñal.
En resumidas cuentas, para saber si el motor está en funcionamiento o no.

Sensor de temperatura

Parte fundamental de vehículos que poseen gestión electrónica. Sus aplicaciones incluyen el monitoreo de parámetros del motor, como la temperatura del: aire, refrigerante y aceite. La mayoría están basados en resistencias de coeficiente térmico negativo (NTC), que aumenta a medida que disminuye la temperatura.

Para el presente caso la señal de este sensor se aplica para verificar si el motor alcanzo temperatura normal de funcionamiento, caso contrario no permite el corte de energía para apagar el motor.

Sensor de posición de la palanca de cambios

Este dispositivo determina si la transmisión del vehículo se encuentra en neutro o en marcha a través de su posición.

Sensores de posición del pedal de embrague

Conocer si el pedal de embrague está presionado o no, es una condición fundamental del sistema start-stop que indica si el vehículo debe arrancar o apagarse.

Sensor de voltaje de batería

El sensor de voltaje de la batería provee información sobre el estado de la batería y permite, prever las reservas de energía. Mide la tensión, la intensidad y la temperatura de la batería, para calcular su vida útil y su capacidad de arranque.

Relee

Es un dispositivo electromecánico que posee dos circuitos: uno de control que tiene una corriente de activación baja y otro de potencia que va a soportar la corriente del consumidor eléctrico. (Rueda, 2005)

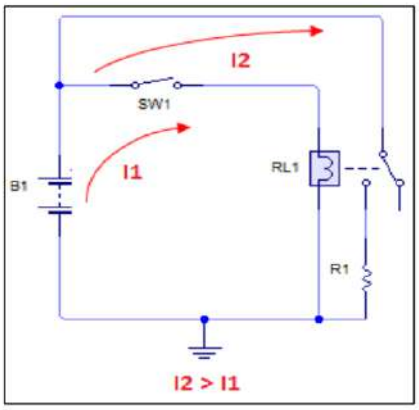

Figura 4: Esquema de control del mediante relé

La activación del motor de arranque para encender el vehículo se controla electrónicamente, energizando un relevador cuando se cumplen las siguientes condiciones: motor de combustión interna apagado, vehículo detenido (velocidad cero), posición neutro de la palanca de cambios y pedal de embrague presionado.

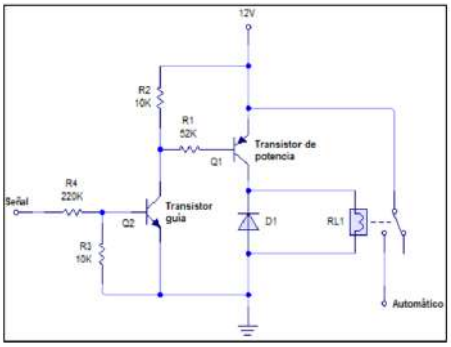

Figura 5: circuito de control del sistema de encendido

El corte del sistema de encendido para apagar el motor de combustión interna se controla electrónicamente, activando a un dispositivo electromagnético cuando se cumplen condiciones como: temperatura de funcionamiento de motor superior a 80 C, posición neutro de la palanca de cambios, sistema de embrague sin accionar, vehículo detenido (velocidad cero) y régimen de giro en ralentí (800 rpm).

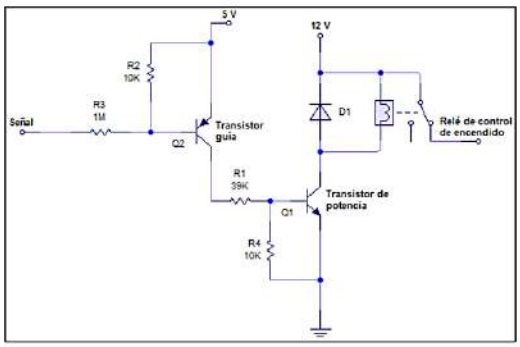

Figura 6: circuito de control del sistema de encendido, posición apagado

Una vez que se tiene claro el método de corte y accionamiento del motor se necesita un elemento que evalué y emita las señales de activación y corte de corriente para ello se necesita un microcontrolador.

Para seleccionar el microcontrolador se consideró los siguientes parámetros: velocidad del microcontrolador, puertos analógicos y digitales de entrada, puertos digitales de salida y memoria. La velocidad del microcontrolador determina si el dispositivo puede contar el tiempo más bajo que exista entre cada cambio de flancos de los trenes de pulsos de la velocidad del motor y del vehículo, del que se obtuvo el tiempo de pulso en el que el motor alcanza una velocidad de 6000 rpm, que es de 0,002 segundos. Con la ecuación 8 se obtuvo el valor de frecuencia mínimo al cual debe funcionar el microcontrolador. (Aguilar, 2017)

Figura 7: Placa de Arduino

Para realizar las pruebas necesarias de consumo de combustible se llevó a cabo un protocolo NEDC, mismo que es un ciclo de homologación obligatorio para todos los coches que se quieran comercializar en Europa. Dicha prueba se realiza en un banco dinamométrico, obteniendo el consumo de combustible y las emisiones de gases contaminantes.

Se obtuvo los valores promedios de consumo de combustible utilizando el ciclo NEDC (New European Driving Cycle). con el vehículo estándar y con el sistema implementado, en el primer caso se tiene 0,065 l/km y para el start-stop 0,059 l/km. (Aguilar, 2017) En la Tabla 1 se observa la representación de este análisis comparativo.

Tabla1: Prueba de consumo de combustible

NEDC								
Parámetros	**Estándar**				**Start-stop**			
	1	**2**	**3**	**Promedio**	**1**	**2**	**3**	**Promedio**
Consumido (l)	0,68	0,77	0,71	0,720	0,67	0,66	0,64	0,656
Consumo (l/km)	0,06	0,07	0,06	0,065	0,06	0,06	0,06	0,059
Rendimiento (km/gal)	61,32	54,15	58,73	58,064	62,23	63,18	65,15	63,518

CONCLUSIONES

Durante el ensayo, se determinó los parámetros de consumo de combustible y emisiones con el sistema convencional y con el sistema start-stop. Además, se realizó la compilación de requerimientos de la implementación del sistema start-stop para conocer las condiciones iniciales de funcionamiento. Se estableció que el sistema start-stop no afecto el funcionamiento convencional del vehículo, por lo que se determinó que su implementación es totalmente factible. El sistema start-stop basa su funcionamiento en señales digitales y analógicas obtenidas de sensores como velocidad del vehículo, temperatura del motor, posición del cigüeñal, estado de batería, posición de la palanca de cambios y embrague.

BIBLIOGRAFÌA

Aguilar, J. (2017). *Investigación De La Eficiencia Energética En Relación Al Consumo De Combustible Y Emisiones Al Implementar El Sistema Start-Stop En El Vehículo Hyundai Getz 1,6.* Quito: Escuela Politécnica Nacional.

Carvajal, A. (26 de Septiembre de 2019). Investigación mundial sobre movilidad ubica a Quito en el puesto 26 entre 200 ciudades con más problemas de tráfico. *EL COMERCIO*.

Enríquez, D. (5 de agosto de 2017). Los vehículos son los que más contaminan el aire. *EL TELEGRAFO*.

Lopez, J. (2013). *Evaluación del consumo de combustible de vehículos livianos en el distrito metropolitano de Quito.* Quito: Escuela Politécnica Nacional.

Rueda, J. (2005). *Técnico en Mecánica & Electrónica automotriz* (Tercera ed.). Cali, Colombia: Disel.

Análisis de los Beneficios Económicos y Sociales para la Implementación de Iluminación LED en el Alumbrado Público

Villarroel, Holger [1]

[1]*Instituto Superior Tecnológico de Tecnologías Apropiadas INSTA, Quito, Ecuador*

Resumen: El presente artículo pretende exponer información relevante, acerca del uso de un sistema de tecnología LED para el alumbrado público, del mismo modo, resaltar sus beneficios económicos y sustentabilidad. Se aborda, además, información detallada y requerida para la implementación de un proyecto con iluminación LED, especialmente para un sistema de alumbrado público.

Palabras clave: Beneficios, Económico, Social, Iluminación LED, Público

Analysis of the Economic and Social Benefits for the Implementation of LED Lighting in Public Lighting

Abstract: This article aims to present relevant information about the use of an LED technology system for public lighting, in the same way, highlight its economic benefits and sustainability. It also addresses detailed information required for the implementation of a project with LED lighting, especially for a public lighting system

Keywords: Benefits, Economic, Social, LED Lighting, Public

INTRODUCCIÓN

A media que evoluciona la tecnología debemos buscar alternativas mediante diferentes dispositivos de iluminación que prometan recudir costos y lograr tener una energía sustentable para nuestro entorno para futuras generaciones y en sí para nuestro hogar el planeta Tierra.

Es así que la beneficio que ofrece las lámparas LED cuyas siglas en inglés provienen de Light Emitting Diode (diodo emisor de luz), es un dispositivo semiconductor (diodos) que emite luz policromática (diferentes longitudes de onda) cuando se polariza en directa y circula corriente continua. El color depende del material semiconductor empleado en la construcción del diodo, pudiendo variar desde el ultravioleta, pasando por el espectro de luz visible, hasta el infrarrojo.

La aplicación de esta tecnología es justificable en virtud de poder lograr una mayor eficacia y eficiencia en el ámbito económico y energético, en relación a los sistemas convencionales de alumbrado público que utiliza el Estado, logrando con esta inversión un ahorro a mediano y largo plazo en las arcas fiscales por contar este sistema con una vida útil mucho más prolongada que la tecnología convencional y de mayor facilidad en su mantenimiento, así como mejorar la calidad de vida de sus habitantes brindando seguridad a conductores, pasajeros y peatones, de allí la importancia en su implementación en vista de la situación económica y social actual que atraviesa nuestro país y la región así como también los problemas y consecuencias del calentamiento global y el efecto invernadero a nivel mundial, es por esto que estamos obligados a buscar medidas y procesos de cambio sustentables.

La situación actual mundial está exigiendo cada vez más tecnología que implique reutilizar productos, que tenga una larga vida útil, que sean sistemas de ahorro tanto económicos como energéticos y a la vez que puedan conducir a procesos de iluminación pública para contribuir a mejorar la seguridad en las ciudades, es por esto que necesitamos direccionarnos hacia sistemas sostenibles que ahorren energía, que sean económicamente viables y que traigan beneficios al medio ambiente y a la sociedad en general.

En América Latina Buenos Aires en este año, se convirtió en la primera de América Latina y el Caribe con un alumbrado público completamente LED. Además de un ahorro importante de energía y de reducción de emisiones de CO2, sus autoridades destacan el impacto social que ha supuesto esa transformación tecnológica y concluyen que una mejor iluminación genera una mayor seguridad, ya que las luces blancas LED favorecen el reconocimiento facial y la correcta percepción de colores, a simple vista y a través de cámaras

.En nuestro país en el necesario interés por la implementación de este sistema en la ciudad de Quito en el mes de julio del 2019, el Cabildo firmó un convenio con la EEQ para en una primera intervención se instale iluminación tipo LED focos ambientalmente amistosos, de mejor tecnología y mayor durabilidad) en 20 plazas y parques del centro, sur y norte de la ciudad, se identificó que se iluminarán espacios ubicados en los barrios de La Colmena, San José de Puengasí, San Blas, Villa Flora, La Bretaña, Quitumbe, La Gatazo, Carapungo,

holguerva@hotmail.com

Solanda, Pisulí y San Antonio de Pichincha. Son sectores donde existen espacios públicos utilizados por la comunidad y en los cuales se han reportado problemas como zonas oscuras e inseguridad. Emprendedores (2018)

Aquí se realiza un análisis de costo beneficio que esta tecnología representaría tanto en su implementación, y ahorro, además de evidenciar los favores ambientales y sociales que forman parte de este sistema de iluminación.

Sistema *eco-friendly*

Es decir es un sistema *eco-amigable,* hace referencia sobre el respeto y conservación del medioambiente. En la búsqueda de sistemas sustentables de energía es la opción que permite un desarrollo económico sin afectar ni dañar el planeta. En el caso de las luces LED, estas reducen el gas de efecto invernadero (GEI) ya que gastan, como promedio, un 70 % menos que las tradicionales.

Estudio comparativo lámparas de mercurio o sodio vs LED

La emisión LED es hasta 10 veces mayor que una lámpara de mercurio o de sodio, con una duración de 50.000 horas. Además, si consideramos factores como las emisiones de metales pesados, contaminación lumínica e impacto sobre la salud humana, los sistemas de iluminación LED superan a los demás.

La siguiente es una tabla comparativa entre los tres tipos de luminarias que se utilizan en alumbrado público:

Tabla 1. Características de las luminarias para alumbrado público

Características	Vapor de mercurio	Vapor de sodio alta presión	LED de alta potencia
Vida útil (horas)	25.000	12.000	>50.000
Eficacia (lm/W)	60	100	110
Mantenimiento de lúmenes	Malo	Bueno	Bueno
Índice de rendimiento de color	46%	22%	70 - 90%
Temperatura de color (K)	4.100	1.900 - 2.200	2.700 - 5.700
Calor a disipar	46%	37%	75% - 85%
Encendido (min)	10	3-5	Al instante
Rendimiento (min)	3	1	Al instante

Análisis económico y energético de un sistema de iluminación LED

Aparentemente el costo de una lámpara LED para la vía pública superaría en costo a las tradicionales lámparas HPS (High Pressure Sodium), algunos ejemplos Luminarias HPS 250W HPS: High Pressure Sodium - Sodio de Alta Presión valor $110 aproximadamente mientras que las luminarias LED en el mercado sus precios varían desde Lámpara Vial Cobra 150w U$S 169, 08, Luminarias LED Alumbrado Público Osram Ledvance de 150 w U$S 366.60, Luminaria LED 150w Alumbrado Público Alt Intensidad Pastoral U$S 457 [7] Pero debemos tomar en cuenta el ahorro en la sustitución de lámparas LED ya con una duración de 50.000 horas prácticamente triplican a una convencional.

Pero la gran diferencia radica en el costo de operación, con un ahorro energético entre 3 y 5 veces mayor que la convencional HPS. Vamos a suponer el siguiente ejemplo; un costo de operación con lámparas LED de$10.000 equivaldría con las luminarias convencionales a un valor entre $30.000 y $50.000 Además la emisión LED es hasta 10 veces mayor que una lámpara de mercurio o de sodio. Por otra parte si tomamos en cuenta factores como las emisiones de metales pesados, contaminación lumínica e impacto sobre la salud humana, los sistemas de iluminación LED superan a los demás.

Análisis de beneficios económicos y sociales

Al implementar sistemas de alumbrado público LED vamos a lograr ser eficaces y eficientes, en el primer caso debido a que podemos cumplir con varios objetivos por parte del Estado entre los cuales tenemos mejorar el alumbrado y por ende la seguridad y bienestar de sus habitante y por el otro siendo eficientes al reducir costos de operación, mantenimiento y servicio, ya que brinda una atención remota por cada poste de luz, en que cada uno de ellos se regula de manera independiente de esta manera optimizando los recursos públicos,. Existe un gran mercado en marcas de iluminación que ofrecen soluciones de alumbrado público que permiten programar su funcionamiento de acuerdo a las necesidades de cada usuario., logrando así un control efectivo de su uso, en su interior contiene un driver programable que puede ser ajustado según los parámetros eléctricos de funcionamiento, ofreciendo un control del flujo luminoso y un consiguiente ahorro en el consumo de la luminaria. En el caso de la opción de programación previa permite que trabaje a diferentes potencias durante el día, dependiendo del flujo vehicular y peatonal, sin la necesidad de intervenirla una vez instalada.

Beneficio económico y energético

Al hablar de beneficios en la implementación de tecnología LED tenemos la capacidad de ahorro de energía, el que puede ubicarse entre el 50 % y el 90 % respecto a lo que se gastaba con las convencionales. En cuanto, al desembolso económico por motivo de renovación pasa a ser mucho menor, ya que su vida útil que alcanzan las luminarias LED es 50 000 horas en promedio, cifra muy superior a las 2000 de las incandescentes, es decir por cada 25 luminarias incandescentes se cambiaría a penas una LED

Contribución a la seguridad urbana

En toda urbe es necesario como parte de una política conjunta de seguridad el manejo de sistemas lumínicos que se complementen con otros dispositivos tecnológicos que contribuyan en la seguridad a través de una mejor iluminación de los espacios públicos y en esto el tono de luz de las luminarias LED ayuda a la mejora en la detección facial y a la buena percepción de colores, tanto de manera directa como mediante cámaras de vigilancia, aspecto que favorecería fuertemente el reconocimiento y localización de, por ejemplo, la identificación de delincuentes y de delitos en la vía pública.

Innovación y proyección de imagen

El crecimiento constante y desarrollo de las urbes obliga a las autoridades locales en el mejoramiento y recuperación de espacios públicos para sus pobladores y la de sus potenciales visitantes. En Latinoamérica ciudades como Buenos Aires, Medellín y Sao Paulo ya han llevado a cabo un constante trabajo de implementación en este tipo de iluminación como forma de modernizar sus calles y velar por el desarrollo de la imagen de las urbes, dando niveles más altos de seguridad a su población y por ende al turista. Es por esto que nos vemos obligados a no quedarnos al margen de todas aquellas naciones y ciudades que buscan: cuidado ambiental, seguridad, así como fomentar y hacer crecer su turismo interno y externo, a través de tipo de tecnologías en iluminación

Mejores prácticas para el diseño y despliegue de redes FTTH-GPON

Lema, Víctor [1]

[1]*Instituto Superior Tecnológico de Tecnologías Apropiadas INSTA, Quito, Ecuador*

Resumen: El artículo tiene por objetivo, abordar las mejores prácticas aplicables al diseño y despliegue de las redes de fibra óptica GPON, las cuales garantizan la estabilidad de los servicios que se brinden a través de dichas redes; por otro lado, se consideran los aspectos técnicos de los equipos activos, la red pasiva y el crecimiento de la tecnología. Los lineamientos que se exponen durante el desarrollo del artículo, son aplicables a cualquier tipo de red GPON sin distinción de las marcas de equipos activos que se utilicen o la operadora que brinde los servicios, esto, debido a que se basan en el cumplimiento de normas internacionales vigentes.

Palabras clave: Fibra óptica, Red pasiva, OLT, ONT, ODN.

Analysis of the economic and social benefits for the implementation of LED lighting in public lighting

Abstract: The aim of the article is to address the best practices applicable to the design and deployment of GPON fiber optic networks, which guarantee the stability of the services provided through said networks; on the other hand, the technical aspects of active equipment, the passive network and the growth of technology are considered. The guidelines that are exposed during the development of the article are applicable to any type of GPON network without distinction of the brands of active equipment that are used or the operator that provides the services, this, because they are based on compliance with standards current international

Keywords: Fiber optic, Passive network, OLT, ONT, ODN.

INTRODUCCIÓN

Según la Unión Internacional de Telecomunicaciones (UIT), por primera vez en la historia, la mitad de la población mundial utiliza el Internet. En el caso de Ecuador, de acuerdo con la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), entidad adscrita al Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), a septiembre del año 2018, la penetración de Internet, fija y móvil, por cada 100 habitantes, asciende a 64,69%, lo que nos ubica por encima de este indicador a nivel mundial. (MINTEL, s.f.)

Según la Unión Internacional de Telecomunicaciones (UIT), por primera vez en la historia, la mitad de la población mundial utiliza el Internet. En el caso de Ecuador, de acuerdo con la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), entidad adscrita al Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), a septiembre del año 2018, la penetración de Internet, fija y móvil, por cada 100 habitantes, asciende a 64,69%, lo que nos ubica por encima de este indicador a nivel mundial. (MINTEL, s.f.)

El alto consumo de ancho de banda por el uso de aplicaciones web, aulas virtuales, juegos en red, video streaming, redes sociales y transmisión de video en alta definición; incrementa la necesidad del usuario de contar con un servicio de acceso a internet de calidad y con el ancho de banda suficiente para satisfacer sus necesidades. De acuerdo con los últimos datos de la Encuesta de Tecnologías de la Información y la Comunicación, del Instituto Nacional de Estadística y Censos (INEC), realizada en el Ecuador a 31.092 hogares en Diciembre de 2016, reflejó que existe una penetración del servicio de internet del 36,0 por ciento a nivel nacional de los cuales un 75,6 % acceden a través de redes de acceso fijo, y tan solo un 24.4 % acceden a internet a través de redes inalámbricas (INEC, s.f.); lo cual evidencia la necesidad de uso de tecnologías de banda ancha para satisfacer los requerimientos actuales de los clientes.

Tomando en cuenta las vulnerabilidades de una red de cobre tales como la distancia, atenuación por inducción, atenuación por bajo aislamiento a tierra, ruido electromagnético y peligro de robo de cables, es necesario optar por la implementación de una tecnología que brinde el servicio de internet de alta velocidad y pueda ser utilizada para dar varios servicios por la misma red, tal es el caso de la fibra óptica.

Una red óptica es una red de telecomunicaciones en donde se utilizan fibras ópticas como enlaces de transmisión y cuya arquitectura se diseña para aprovechar las características de este medio. El diseño e implementación de una red óptica requiere de la combinación de elementos ópticos y electrónicos, así como del software adecuado que garantice el

victor.lema@insta.edu.ec

correcto funcionamiento del sistema. (Capmany y Ortega, 2009, p.17)

La tecnología GPON permite la convergencia de varios servicios de telecomunicaciones sobre una misma infraestructura de red, lo cual influye en la disminución de costos de despliegue de red de las operadoras, evitando instalar y mantener redes paralelas para cada uno de sus servicios. Esto contribuye a mediano plazo, a la reducción de tarifas por servicio de los abonados finales.

El presente artículo se encuentra organizado de la siguiente manera: Sección I Introducción, estadísticas y detalle del problema; Sección II Detalle de las mejores prácticas aplicables; Sección III Conclusiones.

Una vez que se ha analizado la necesidad de uso de redes de fibra óptica GPON como medio de acceso fijo a internet, a continuación, se detallan las mejores prácticas para su diseño y despliegue:

Criterio 1: Dimensionar el alcance físico de la red.

El criterio 1 hace referencia a conocer el sector en el cual se desea implementar la red GPON, el número de habitantes, así como su densidad poblacional y la tasa de crecimiento anual, a fin de determinar la posible demanda vigente y futura, para garantizar que la red que se diseñe y despliegue sea perdurable en el tiempo y soporte el incremento de clientes por la vida útil que se defina para la red. Para la estimación de estos datos es importante considerar las estadísticas de penetración de la tecnología GPON en el sector, acceso al servicio de internet, censos realizados sobre la densidad poblacional y demás estadísticas que se realizan por las entidades correspondientes y entes reguladores de cada país.

Ejemplo: Para una red GPON con 200 posibles clientes actuales, en un sector con crecimiento poblacional del 3% anual y una vida útil de la red definida para 15 años; se determina (1):
Clientes vigentes=200
Clientes por crecimiento poblacional anual = 200 x 3% = 6
Clientes futuros por vida útil de red= 6 x 15 años= 90
Clientes vigentes + futuros= 290

Criterio 2: Dimensionar el ancho de banda máximo para cada cliente.

Para determinar el AB máximo por cada usuario, se debe considerar la situación económica media de los posibles clientes y del sector en general; así como los objetivos por los cuales el cliente prevé contratar los servicios. Tal es el caso de que, si se trata de un sector comercial con negocios operando, la demanda de AB será mayor a la demanda que tenga un sector de viviendas en su mayoría.

El AB máximo que se determine para cada cliente, definirá adicionalmente el splitteo máximo (división de potencia óptica) que se aplicará a cada puerto PON (generador de potencia óptica en la OLT) del diseño.

La recomendación ITU.T G.984.x establece las siguientes velocidades de Uplink y Downlink de la tecnología GPON, así como el nivel máximo de splitteo de cada puerto PON de la OLT (2):
Velocidad de Uplink= 1.25 Gbps*
Velocidad de Downlink= 2.5 Gbps*
Splitteo máximo: 1 a 128

Por lo tanto, tendríamos las siguientes velocidades máximas para cada cliente según los niveles de splitteo más usados en un puerto PON:

Splitteo 1:128
Velocidad de Uplink en puerto PON/128=9.8 Mbps
Velocidad de Downlink en puerto PON/128=19.5 Mbps

Es decir, cada cliente dispondría de un máximo de 19.5 Mbps en Downlink y un máximo 9.8 Mbps en Uplink

Splitteo 1:64
Velocidad de Uplink en puerto PON/64=19.5 Mbps
Velocidad de Downlink en puerto PON/64=39 Mbps

Es decir, cada cliente dispondría de un máximo de 39 Mbps en Downlink y un máximo 19.5 Mbps en Uplink

Splitteo 1:32
Velocidad de Uplink en puerto PON/64=39 Mbps
Velocidad de Downlink en puerto PON/64=78 Mbps

Es decir, cada cliente dispondría de un máximo de 78 Mbps en Downlink y un máximo 39 Mbps en Uplink

Cabe aclarar que lo anterior no determina el número máximo de clientes de la red, pesto que para el efecto se utilizan uno o más puertos PON según sea la demanda de clientes del sector.

Ejemplo: Para cubrir la demanda de los 290 clientes del sector analizado en el punto anterior y considerando que la necesidad de AB de los clientes es de al menos 50 Mbps, lo recomendable sería utilizar un nivel de splitteo de 1:32 en los 10 puertos PON necesarios para atender con el servicio a los 290 clientes.

Sin embargo, de lo expuesto, en la práctica existen casos en los cuales el mismo sector al que se va a atender con la red GPON, se encuentra dividido en subsectores en función de necesidad de AB, para lo cual se deberán asignar diferentes niveles de splitteo para cada sector según la necesidad.

Criterio 3: Selección de los equipos activos (OLT y ONT)

Desde el punto de vista técnico, todos los equipos activos que cumplan con la recomendación ITU-T G.984.x, tendrán características de funcionamiento similares, por lo que la decisión de utilizar una u otra marca de equipos activos se deberá enfocar al ámbito comercial y a las soluciones específicas que ofrezcan los fabricantes, sin embargo, es

importante verificar el cumplimiento de al menos los siguientes parámetros de funcionamiento de las ONT`s y OLT`s descritas en la recomendación ITU-T G.984.2, puesto que definirán el funcionamiento de nuestra red:

Tabla 1: Parámetros de potencia OLT/ONT

ITEM	UNIDAD	Valor
OLT		
Potencia Tx Media Mínima	dBm	1.5
Potencia Tx Media Máxima	dBm	5
ONT		
Potencia Tx Media Mínima	dBm	0.5
Potencia Tx Media Máxima	dBm	5
Sensibilidad del receptor	dBm	-27

Un ítem crucial para la selección de los equipos activos, es garantizar la interoperabilidad de marcas, puesto que si nuestra red inicialmente se despliega con equipos OLT y ONT`s de la marca X y no se definió la interoperabilidad de marcas como parte de los requisitos iniciales de la adquisición, estaríamos obligados a seguir adquiriendo dichos equipos o en su defecto pagar licencias adicionales cuando sea la necesidad comercial de operar con equipos de la marca Y. Este mismo caso se aplica para software de gestión y configuración de servicios que suelen entregarse como parte de la contratación de OLT`s, al ser propietarios de una marca en específico, no podrán ser utilizados para equipos ONT`s de marcas diferentes sin pagar licencias adicionales de funcionamiento.

Criterio 4: Determinación de la pérdida máxima del sistema.

Para que nuestro diseño sea optimo y operativo durante la vida útil definida para la red, soporte las atenuaciones adicionales futuras ocasionadas por reparaciones, mantenimientos correctivos y demás imprevistos que son inherentes de las redes de planta externa; es necesario considerar en el diseño, los valores de pérdidas por eventos (fusiones, conectorizaciones) y los valores de potencia de Tx/Rx de la OLT/ONT más críticos disponibles. De tal manera que se determine la pérdida máxima que soportará la red con un valor conservativo y a su vez, se determine el tipo de módulo SFP que se usará en cada puerto PON.

En virtud de lo expuesto, se determina (3):

$$P_{Rx} = P_{tx} - Atenuación\ total$$

$$P_{tx\ mínima\ OLT} = 1{,}5\ [dBm]$$

$$P_{Rx\ mínima\ ONT} = Sensibilidad\ del\ receptor = -27\ [dBm]$$

Reemplazando (4):

$$Atenuación\ total = 1{,}5\ [dBm] + 27\ [dBm] = 28{,}5\ [dB]$$

Una vez que se dispone del cálculo de la perdida máxima de la red en la cual se garantiza que la ONT recibirá una potencia mayor o igual a la sensibilidad del receptor, se debe determinar el tipo de módulo SFP a utilizar en cada puerto PON, puesto que su costo varía de forma directamente proporcional a la perdida máxima que soporta:

Tabla 2: Pérdida máxima por tipo de SFP

	Clase A	Clase B	Clase B+	Clase C
Máxima Pérdida	20 dB	25 dB	28 dB	30 dB

Criterio 5: Determinación de la pérdida de los clientes finales.

Una vez que se conoce el valor máximo de perdida que soporta la red, es importante verificar que dicho valor sea concordante con el valor máximo de perdida calculado para el despliegue de la red, lo cual incluye: perdidas por fusión, perdidas por conectorizacion, perdidas por Km de fibra óptica y pérdidas por splitteo.

Siguiendo los lineamientos anteriores, este cálculo debe considerar los valores de perdida más críticos a fin de garantizar el correcto funcionamiento de la red a lo largo del tiempo, mismo que deberá ser menor o igual a la perdida máxima calculada para el sistema.

Criterio 6: Fiscalización de la red.

La fiscalización de la red es el punto crítico que garantiza la operación futura de la misma, por tanto, es necesario que para el efecto se disponga de los diseños GPON iniciales bajo los cuales se construyó la red a fin de verificar que los valores de potencia de Rx que se obtiene en el cliente final, sean mejores o en el peor de los casos iguales a los del diseño planteado para dicho cliente. Si en una fiscalización de red GPON se verifica que la potencia de Rx que recibe un cliente está dentro del rango de la sensibilidad del receptor, no es motivo suficiente para determinar que la red se encuentra en óptimas condiciones, puesto que la sensibilidad del receptor determina el rango de funcionamiento de la ONT, mas no determina que el despliegue haya sido ejecutado de forma correcta y como se previó en el diseño.
Ejemplo: Si una red GPON fue diseñada para que el cliente se disponga de una potencia de Rx de -22 dBm y en la fiscalización se verifica que la potencia de Rx es de -23 dBm, se determina que la red tiene desperfectos en su construcción, a pesar de que el valor de potencia que se recibe se encuentra dentro del rango de la sensibilidad del receptor, en otras palabras, el cliente si tendrá servicio, pero bajo un escenario no optimo puesto que la construcción de la red tiene desperfectos.

Con el fin de cumplir con las características de una red GPON, se recomienda seguir los lineamientos planteados en el diseño de la red; de tal manera que se logre explotar todos los

beneficios que ofrece la tecnología GPON, instalando la mayor cantidad posible de servicios por usuario.

Se recomienda aprovechar la disponibilidad de infraestructura civil y de telecomunicaciones disponible para el despliegue de la red, a fin de abaratar costos derivados de infraestructura.

Se considera indispensable el constante monitoreo y mantenimiento de la red GPON que se despliegue cualquier sector, para mantener la operatividad eficaz de la red y evitar inconformidades de los usuarios finales.

BIBLIOGRAFÌA

Android, K. (2017). *Seguridad en los androids.* Obtenido de https://www.xatakandroid.com/seguridad/he-instalado-todos-los-malware-de-android-esto-es-lo-que-ocurre-si-te-saltas-los-consejos-de-seguridad

Ciberseguridad. (2018). *Seguridad en dispositivos móviles: la mayor ciberamenaza está al alcance de tus manos.* Obtenido de [1]: https://www.iniseg.es/blog/ciberseguridad/seguridad-en-dispositivos-moviles/

Emprendedores. (2018). *Claves de seguridad para el móvil.* Obtenido de https://www.emprendedores.es/gestion/a27551265/claves-ciberseguridad-movil-seguridad-informatica-empresas/

móviles, G. d. (2017). *Dispositivos móviles personales para uso profesional BYOD.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

Tecnologia. (2018). *Peligro en los usb.* Obtenido de https://ticnegocios.camaravalencia.com/servicios/tendencias/guia-ciberseguridad-el-peligro-de-los-usb/

VOLUMEN 02
NÚMERO 01
ENERO
2019

INSTA MAGAZINE I+D

Investigación y Desarrollo

INSTITUTO SUPERIOR TECNOLÓGICO
"DE TECNOLOGÍAS APROPIADAS"
INSTA