República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil

Trabajo de Titulación

Para la Obtención del Título de:

Ingeniero En Sistemas computacionales Mención Aplicaciones Web Y Multimedia

Tema:

Guía de consideraciones en la seguridad de la información para promover el Teletrabajo en empresas de Desarrollo de Software en Guayaquil.

Autor:

Darwin Vladimir Merchán Delgado

Director de trabajo de titulación:

MSIG. Francisco Cedeño T.

2020

Guayaquil– Ecuador

Dedicatoria

El presente trabajo se lo dedico a mi familia por el apoyo incondicional y por estar conmigo en todo momento, brindándome su apoyo y comprensión, en especial a mi esposa.

Agradecimiento

Gracias a la universidad UTEG por haberme permitido formarme en ella, gracias a todas las personas que fueron participe de este proceso. A mis hermanos yen especial a mis padres que me supieron inculcar valores y responsabilidades para afrontar este duro y arduo camino de la Universidad.Una mención especial para mi gestor Luis Aguirre que con sus consejos y enseñanzas pudimos sacar este proyecto de titulación adelante.

La responsabilidad de este trabajo de investigación, con sus resultados y conclusiones, pertenece exclusivamente al autor.

……..
(Darwin Vladimir Merchán Delgado)

GUÍA DE CONSIDERACIONES EN LA SEGURIDAD DE LA INFORMACION PARA PROMOVER EL TELETRABAJO EN EMPRESAS DE DESARROLLO DE SOFTWARE EN GUAYAQUIL

Darwin Vladimir Merchán Delgado
dar.merchan@gmail.com

Resumen

La presente investigación tiene como finalidad, dotar de parámetros de control que sirvan como una guía de consideraciones para promover el teletrabajo en empresas de desarrollo de software, se evidencia también que la legislación que ampara o norma esta modalidad, fue normada de manera integral a raíz de la pandemia del COVID-19 que obviamente también afecto al Ecuador y que por motivos del confinamiento inicial se forzó a las empresas a emplear el teletrabajo, pero que en empresas como las de desarrollo de software por manejar información sensible, se hizo necesario garantizar la Seguridad de la Información al momento de aplicar el teletrabajo.La presente investigación utiliza una metodología descriptiva y explicativa, con enfoque cualitativo, utilizando el método empírico, el cual obtiene información mediante la observación y la medición, basándose en analizar los datos obtenidos por medio de una entrevista a los Gerentes de las firmas más importantes de desarrollo de software de Guayaquil, se realizó también una encuesta a las empresas de desarrollo de software en Guayaquil lo cual permitió conocer cuáles de estas contaban con la certificación ISO/IEC 27001:2013 que es la que norma y garantiza la seguridad de la Información, así como también en base a esta norma se desarrolló una guía de consideraciones para la implementación del teletrabajo en las reducir los mismos y realizar las auditorias correspondientes para garantizar la seguridad de la información a lo largo del tiempo.

Palabras clave: Seguridad de la Información, teletrabajo, desarrollo de software

Introducción

En la actualidad, uno de los activos más valiosos que posee toda empresa es la información, la misma que no solo corresponde al giro del negocio o la que produce por sí misma, sino también la que recopila del mercado para poder utilizarla a su favor mediante la toma de decisiones gerenciales.

Para esto es necesario implementar y adoptar practicas o procesos que permitan garantizar la seguridad de la información, por supuesto siempre apegados a las normativas vigentes o regulaciones del país, sumados a los procesos de evaluación y análisis de riesgos con la finalidad de garantizar la calidad de esta información.

La presente investigación tiene como finalidad establecer los controles de Seguridad de la Información, que debe mantener toda empresa de desarrollo de software que requiera implementar teletrabajo, identificando las posibles vulnerabilidades y proponiendo soluciones de control que permitan mitigar los riegos en cuanto a la seguridad.

Las empresas de desarrollo de software brindan servicios a empresas tanto públicas como privadas, ya sea en el mantenimiento y actualización de sus sistemas informáticos y desarrollo de nuevos requerimientos o funcionalidades, pero por la velocidad o celeridad de los requerimientos, sumados a las restricciones de movilidad y trabajo colectivo actualmente por la pandemia, empujan u orientan a que el trabajo pase de ser desarrollado dentro de la empresa, a otros espacios fuera de la organización mediante el teletrabajo.

En cuanto a las TIC, en la actualidad se presentan como uno de los mayores soportes para el desarrollo de las empresas o negocios a nivel global, pues permiten soportar el crecimiento de la empresa, industria y comercio, de hecho todas ellas necesitan de software que permitirá el

control del negocio y a su vez dotara de información que ayudara en la toma de decisiones, generando así empleo, productividad, satisfacción al cliente, de esta manera se genera tributos aportando al crecimiento de los indicadores económicos del país (Palvia, Baqir, & Nemati, 2017)

.

Es importante realizar un diagnóstico al interior de la empresa de desarrollo de software, pues de esta manera permitirá en corto o mediano plazo el diseño e implementación de un Sistema de Gestión de Seguridad de la Información – SGSI alineado al estándar ISO/IEC 27001:2013, lo que permitirá a la organización se capaz de controlar las amenazas, vulnerabilidadesy riesgos de seguridad que se ven expuestas las empresas.

Cuando se la implementa, es necesaria la intervención y compromiso de todo el personal, partiendo desde la alta gerencia hasta los mandos medios y operativos, a fin de garantizar el control, continuidad y recursos en el manejo de los activos y sistemas informáticos existentes, en desarrollo y futuros.Deberán estar encuadrados todos estos pasos, mediante procesos lógicos, sistemáticos y documentados, también creando las condiciones para una buena difusión interna de los objetivos planteados que permitan la gestión adecuada de la Seguridad de la Información, considerando también el ciclo de la mejora continua (Planear, Hacer, Verificar; y Actuar - PHVA).

Adicional es necesario conocer la norma ISO/IEC 27001en cada uno de los dominios, una vez realizado esto, se está en condiciones de aplicar la metodología para realizar un análisis de evaluación de riesgo basado en los 3 criterios de información que son la integridad, la disponibilidad y la confidencialidad de la información.Por lo cual surge la siguiente pregunta:

¿Cuáles son las consideraciones de Seguridad de la Información que necesitan implementar las empresas de Desarrollo de Software en Guayaquil para promover el Teletrabajo?

Esta investigación es de suma importancia pues permitirá definir los controles de seguridad existentes en la empresa y su aplicaciónpara promover el teletrabajo, clarificar o establecer los controles definidos por la norma ISO/IEC 27002, como así también políticas y procedimientos que permitan la continuidad de la aplicación de la norma de la implementación futura de un SGSI para poder hacer frente a los riesgos que se encuentren o se presenten.

Explica también la metodología que se utiliza para aplicar los procesos de análisis y evaluación de los riesgos en sus fases de conocimiento inicial del problema, la identificación de las vulnerabilidades, riesgos y amenazas de seguridad, para poder determinar el nivel de riesgo en el cual se encuentra la empresa.

La investigación pone en conocimiento los lineamientos de seguridad de la información, que permitan garantizar la disponibilidad, integridad y confidencialidad de la información.

Objetivo general

Identificar los controles de la Seguridad de la Información, estableciendo las posibles vulnerabilidades,proponiendo soluciones de control que permitan mitigar los riegos en cuanto a la seguridad al implementar el teletrabajo.

Objetivos específicos

- Identificar los beneficios y ventajas de orientar la forma tradicional de desarrollo de software ***in Company*** hacia la modalidad de teletrabajo.
- Identificar posibles vulnerabilidades, amenazas y riesgos en los que pudiese ver expuesta las empresas de desarrollo de software.

- Evaluar los riesgos probables en la seguridad de la información, mediante un sistema de control de Gestión de la Información alineado al estándar ISO/IEC 27001 para garantizar disponibilidad, integridad y confidencialidad de la información.

Marco Teórico

Empresas Desarrolladoras de Software

Las empresas desarrolladoras de software, son aquellas que desarrollan software o programas de acuerdo a los requerimientos específicos de los clientes, este tipo de empresas basan sus ingresos en la venta de programas diseñados a la medida, o en la venta de horas hombre, es decir horas de trabajo especializadas, las mismas que son desempeñadas por profesionales en desarrollo de software.

Entre otra de las características que tienen este tipo de compañías es que la propiedad intelectual de los programas que desarrollan les pertenece, pues normalmente parten de cero y su desarrollo es integral, al cliente le venden el software para su uso y aplicación, pudiendo también complementar con actualizaciones, mantenimientos, o nuevos desarrollos en base al software base desarrollado (solusoft, 2019)

Estándares de Calidad

En cuanto al uso de estándares de calidad, el más difundido en Ecuador es la norma ISO 9001:2015. Cabe resaltar un pronunciamiento durante los últimos 10 años, al pasar de 486 certificados en el 2006 a 1233 en el 2016, lo que supone un incremento del 154%. (Servicio de Acreditción Ecuatoriano, 2017)

Figura 1 Empresas certificadas con la norma ISO 9001
Fuente: (Servicio de Acreditción Ecuatoriano, 2017)

Las empresas de Desarrollo de Software de Guayaquil solo el 36% poseen certificación de calidad ISO/IEC 27001:2013

Figura 2 Empresas de desarrollo de software de Guayaquil con certificado ISO/IEC 27001:2013
Fuente: Investigación del autor, imagen elaborada por el autor

Teletrabajo en tiempos de COVID-19 en Guayaquil

Ante la propagación del COVID-19, una de las opciones para garantizar la salud de los trabajadores en las empresas tanto públicas, como privadas es el teletrabajo, el mismo que refiere al desarrollo de las actividades laborales del trabajador de manera remota, normalmente desde su hogar, para ello es necesario que el trabajador cuente con las herramientas de tecnología de la información para poder acceder a los programas de la empresa o a sus bases de datos (Diario El Universo, 2020)

El teletrabajo en Ecuador no ha sido mayormente utilizado, sino hasta el inicio de la pandemia en el mes de marzo de 2020 que todos se vieron forzados a confinarse en sus hogares, que la perspectiva y las necesidades cambian, por lo que pone a las empresas en una carrera de desarrollo y ajuste de sus herramientas informáticas, su tecnología de la información con la finalidad de dar las herramientas que el trabajador necesite pero procurando garantizar de alguna manera la Seguridad de la Información, pues esta es uno de los activos más valiosos de la misma (Diaro el Comercio, 2020)

Según Escalante y otros la definición de teletrabajo es la siguiente:

> "El teletrabajo, es una aplicación de las telemáticas a entornos empresariales, el mismo implica la relación laboral por cuanto propia o por cuanto ajena, considerando de igual forma el contrato de trabajo a domicilio donde la prestación de la actividad se realiza en el domicilio del trabajador o en el lugar libremente elegido por éste, sin vigilancia del empresario y utilizando medios telemáticos proporcionados mayormente por la empresa contratante. En este sentido, el teletrabajo posibilita enviar el trabajo al trabajador; de igual forma, esta modalidad

admite la práctica de una amplia gama de actividades profesionales que pueden realizarse a tiempo completo o parcial"(Esclante & Y Otros, 2006).

Estas ideas son reforzadas por Civit y March (Civit & March, 2000) en su libro "Implementación del Teletrabajo en la empresa"en el cual hace referencia, que los nuevos tiempos, circunstancias, economía y sociedad, traen consigo nuevos estilos de convivencia y trabajo, pues es la era de reinventar la economía y la sociedad, pero por sobre todo una cambio a la conciencia de las personas que permita su interacción de una manera más civilizada, productiva y armoniosa (Welive Security, 2020)

Teletrabajo en Ecuador

La referencia del Teletrabajo en Ecuador como modalidad alternativa de ejecutar el trabajo y nueva forma laboral, encuentra soporte legal con la expedición de la ley 076 del 2020, la cual define el mismo como *"Expandir las directrices para la aplicación de teletrabajo emergente durante la declaratoria de Emergencia Sanitaria"* (Acuerdo Ministerial Nro. MDT-2020-076).

Seguridad de la Información

El marco normativo de los estándares relacionados con la seguridad informática y de la información, están los estándares ISO/IEC 27000:2013 e ISM3, estas son normas enfocadas en la gestión de seguridad de la información, pudiendo también ser aplicadas en cualquier organización, sin importar su tamaño o actividad.

La norma ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (International Organization for Standarization, en inglés) (ISACA, 2020)

También existen otros estándares relacionados a la calidad como son ISO 9001, medio ambientales como ISO 14000, de TI como el estándar CobIT y de entrega de servicios ITIL.

Estándares ISO/IEC 27001:2013 e ISO/IEC 27002:2013

Un Sistema de Gestión de Seguridad de la Información SGSI, esta normado bajo las normas ISO/IEC 27001:2013 y la ISO/IEC 27002:2013 las cuales detallan los requerimientos para establecer, operar, implementar,revisar, monitorear, mejorar y mantener un SGSI, además que es especifica con los requerimientos para la implementación de controles de seguridad frente a las necesidades de toda la empresa, frente a un proceso especifico o un servicio, según el objetivo y los alcances del SGSI que defina la organización.

El estándar ISO/IEC 27001:2013 comprende dos secciones:

La primera consta de 5 cláusulas enfocadas a características metodológicas del SGSI, las mismas que son de estricto cumplimiento a fin de obtener la certificación:

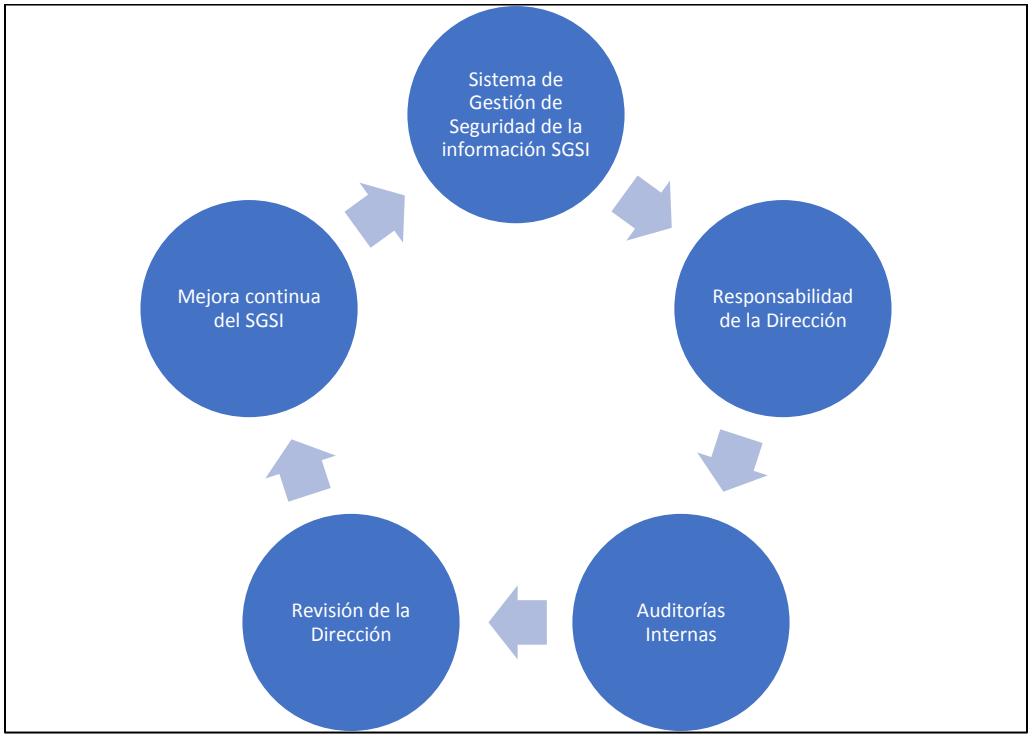

Figura 3 Detalle de la primera sección de la estructura ISO 27001
Fuente: (welivesecurity, 2015)

En la segunda sección están definidos los controles para la gestión de la seguridad de la información, determinados por el estándar ISO/IEC 27001:2013 y asociados con cada uno de los denominados en el Anexo A de la norma, desde los denominados como A5 hasta A18 en la actualización del año 2013, en el gráfico adjunto se puede apreciar el dominio ISO 27001 y el objetivo de control.

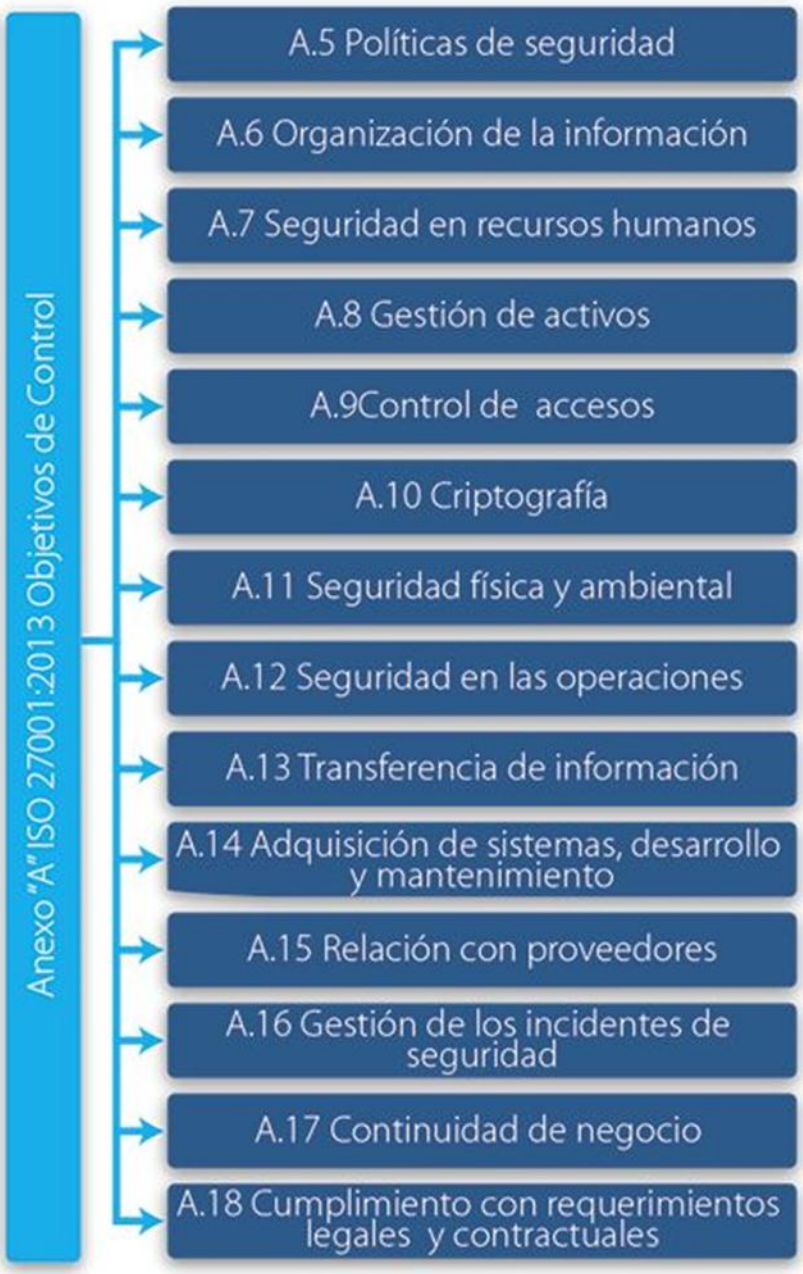

Figura 4 Objetivos de control norma ISO 27001:2013
Fuente: (San Esteban Consulting, 2018)

Para cumplir con el estándar, es necesaria la existencia de factores y condiciones que garanticen el éxito tales como: el apoyo incondicional por parte de la dirección general, la compatibilidad de los controles en la cultura de la empresa,la alineación de los objetivos de seguridad con los objetivos de la empresa, , los canales de comunicación con los empleados para

dar a conocer los aspectos de seguridad, el conocimiento de los requerimiento de seguridad, la preparación y el conocimiento para la Administración de los riesgos, los controles y planes para el tratamiento de riesgo y la disposición de las políticas y procedimiento de seguridad de la información, , (ISO2700, 2020)

Vulnerabilidad Informática

Las vulnerabilidades en el sistema informático (SI) pueden generarse en cualquier momento comprometiendo tanto al software como al hardware, siendo también vulnerables la confidencialidad del sistema y los datos que en ella contiene, pero también se debe entender que la vulnerabilidad también puede estar en los medios o la vulnerabilidad de los dispositivos físicos, adicional la vulnerabilidad de las comunicaciones y la misma vulnerabilidad humana (Universidad Internacional de Valencia, 2018).

Amenazas Informáticas

Las amenazas informáticas son cada vez más comunes en el medio empresarial y comercial, inclusive a las personas naturales o comunes les puede pasar y ser víctimas de amenazas informáticas, pues son una serie de acciones o sucesos, normalmente deliberados, comprometiendo la seguridad del sistema informático.

Las amenazas que se presentan contra los sistemas de información pueden ser de diferentes tipos, como las amenazas por interrupción, modificación , intercepción, esto especialmente cuando se utiliza elementos de almacenamiento externos, y debe ser de especial cuidado cuando se maneja información sensible en la nube, por lo que siempre se debe tener cuidado y estar alertas a este tipo de amenazas (OBS Business School, 2020)

Riesgos informáticos

Para poder mitigar todos los posibles riesgos informáticos en una empresa, es necesario identificar primero todos los posibles riesgos a los que pueda estar expuesta, y luego generar un plan de gestión de riesgos informáticos.

Los riesgos pueden ser clasificados en: Riesgos de relación, Riesgos de integridad, Riesgos de Utilidad, Riesgos de accesos,Riesgos de infraestructura, por lo que debe ser tomadas todas las medidas necesarias a fin de salvaguardar los datos y la información(BASC-Costa Rica, 2018)

Sistema de Gestión de Seguridad de la Información – SGSI

La norma ISO 27001:2013 define como Sistema de Gestión para la Seguridad de la Información a una serie de procesos para ser implementados, mantenerlos y realizar mejoras de forma continua previniendo riesgos que afectan a la seguridad de la información en una organización o empresa (ISO2700, 2020)**.**

Un sistema de Gestión (SGSI) basado en ISO/IEC 27001:2013 permitirá a la organización beneficiarse de las mejores prácticas del mercado y de la industria a nivel global para garantizar la seguridad de la información. La última versión ISO/IEC 27001:2013, la norma sobre la seguridad de la información comparte la misma estructura que las normas sobre Gestión del medio ambiente ISO 14001y también sobre la gestión de la calidad ISO 9001:2015 o, lo cual facilita la integración de distintos sistemas de gestión en una empresa (isotools, 2020)

Estructura de la Normativa ISO/IEC 27000

La norma ISO/IEC 27001 cuenta con 2 cuerpos normativos.

- ISO 27001 Requisitos para un Sistema de Gestión (SGSI)
- ISO 27002 Guía de las buenas prácticas para la implementación de un SGSI

Ambas deben cumplirse para alcanzar el objetivo de implementar un sistema de gestión de la seguridad de la información(normaiso27001, 2019)

Marco Legal

En Ecuador el teletrabajo antes de la pandemia poco se lo empleaba e incluso no estaba mayormente normado, pero a partir de esta, se inicia una propuesta legislativa emergente que pretende normar sobre la aplicación del Teletrabajo durante la declaratoria de Emergencia Sanitaria, mediante el ACUERDO-MINISTERIAL-Nro.-MDT-2020-080 Normativa del teletrabajo en Ecuador por situación emergente ante el COVID-19.

En este acurdo ministerial norma el teletrabajo, considerando e indicando el por qué se lo implementa en el Ecuador apegado a esta normativa, la misma que se emitió con el fin de amparar legalmente una modalidad de trabajo que se ha empleado en casi todas las empresas motivadas inicialmente por el confinamiento y luego por un tema de seguridad en cuanto a la salud y distanciamiento social, en el Anexo 3 de la presente investigación se detalla el acurdo en todas sus partes (Ministerio de Trabajo, 2020).

Marco Metodológico

Métodos

La presente investigación utiliza una metodología descriptiva y explicativa, con enfoque cualitativo, utilizando el método empírico, el cual obtiene información mediante la observación y la medición, basándose en analizar los datos obtenidos por medio de una entrevista alos Gerentes de las firmas más importantes de desarrollo de software de Guayaquil lo cual facilito información importante y explicativa de los requisitos y condiciones para utilizar la Norma ISO-27001-2013 que es la que permite garantizar la Seguridad de la Información al implementar el teletrabajo en una empresa de desarrollo de software(Universidad de Valencia, 2019).

Se realizó también una encuesta telefónica a los representantes de las empresas de desarrollo de software en Guayaquil, pudiendo establecer características de estas y quienes tienen la certificación para la seguridad de la Información ISO 27001-2013.

Población y muestra

La población es el conjunto de elementos, individuos que poseen características similares, pudiendo de esta obtener una muestra que permita establecer parámetros o condiciones de estudio al ser estos de características similares (Carrillo, 2015).

Las empresas de desarrollo de software en Guayaquil son 60por lo tanto esta es su población, la muestra escogida es intencional, habiendo escogido a las 60 empresas para ser encuestadas telefónicamente, pues debido a lo reducido de la población, se considera a todas estas como la muestra a ser encuestada.

Gestión de Datos

La investigación realizada tiene como base el análisis de la información obtenida de la entrevista realizada a varios Gerentes de las compañías más grandes y posicionadas de desarrollo de software en Guayaquil, quienes dotaron de información relevante para el desarrollo de la presente investigación, asítambién mediante la herramienta de la encuesta, que mediante llamadas telefónicas se pudo realizar la encuesta a las 60 empresas de desarrollo de software existentes en la ciudad de Guayaquil.

Se realizó una investigación acerca del certificado de seguridad de la información ISO27001,la encuesta se basó en una única pregunta que era el conocer si cuentan con la certificación ISO 27001:2013 y se complementa con la guía de recomendaciones y consideraciones para la aplicación de la norma ISO27001:2013 para garantizar la seguridad de la información al implementar el teletrabajo en una empresa de desarrollo de software.

Resultados

Análisis de los resultados de las entrevistas

En las entrevistas realizadas a los Gerentes de varias empresas desarrolladoras de software y con mayor presencia en la ciudad de Guayaquil,se pudo conocer a detalle todas las consideraciones que como compañía han tenido para poder implementar el teletrabajo especialmente motivados por la pandemia del COVID-19.

Manifiestan que sus empresas tienen en promedio más de 15 años en el mercado desarrollando software bancario y empresarial, en lo que se refiere al trabajo remoto lo han aplicado solo cuando las condiciones lo han ameritado, como son las implementaciones donde el cliente en su fase de arranque, pero actualmente por el tema de la pandemia debido al COVID-19

se han visto forzados a implementar el teletrabajo con cada uno de los ingenieros de su staff de desarrolladores.

Con relación a esto, recalcan que las implementaciones debieron realizarlas siguiendo estrictos protocolos apegados a las normativas de la ISO 27001:2013 que es la certificación con la que actualmente cuentan, esta normativa determina procesos y procedimientos que ayudan a identificar, proteger y controlar la información y cualquier tipo de equipo o hardware, utilizado para procesar, transmitir y almacenar la información, que se esté trabajando, desarrollando o modificando.

A este respecto se refierenlos expertos que justamente una de las motivaciones para certificarse con la ISO 27001:2013 que es la certificación internacional en Seguridad de la Información, es poder mantener controlados todos los parámetros de seguridad que deben funcionar para implantar los requisitos que garanticen la Seguridad de la Información y también para poder gestionar los riesgos asociados al acceso a los sistemas o del servicio brindado.

En torno a las consideraciones de seguridad que se deben tener en cuenta para poder autorizar a un desarrollador aplicar el teletrabajo, manifiestan que, si el mismo necesita acceso a la red interna de la empresa, el equipo con el que trabaje o se conecte sea de la empresa, de esta manera el control total del equipo que se conecte será de la empresa y estará bajo el control del Equipo de Seguridad de la misma, junto al departamento de Tecnología.

También se deberá utilizar una VPN[1]que es la manera con la cual se garantiza poder establecer conexión de forma segura entre el desarrollador y la empresa. En cuanto al acceso al correo electrónico es necesario que cuente con acceso pudiendo ser desde el propio dispositivo

[1]VPN Virtual Private Network, es una red privada virtual que permite enlazar varios dispositivos digitales de forma segura por internet siendo este el método mayormente utilizado por la seguridad y privacidad brindadas para poder acceder redespúblicas y/o privadas(top10VPN, 2019).

del empleado, para ello deberá ser aplicados firewalls o antimalware, inclusive si amerita el caso debe ser instalada en la máquina del empleado las licencias que correspondan para garantizar el buen funcionamiento de estos, también es importante considerar el limitar la descarga, copia o almacenamiento de datos, a fin de evitar el posible mal uso de datos confidenciales de la empresa. También se puede considerar el uso de máquinas virtuales limitando la exposición de la red de la empresa frente al entorno doméstico.

Es importante considerar una MFA[2], la autenticación multifactor es un sistema de seguridad el cual requiere más de una forma de autenticación, a fin de verificar la legitimidad de una transacción. Debido a esto es considerada la mejor forma de seguridad que cada usuario debería implementar para garantizar la Seguridad de la Información.

Importa y por muchas razones el hecho de que la implementación del trabajo remoto tenga presión de tiempo para ser implementada, ante lo cual, si se utilizan sistemas basados en aplicaciones, los tiempos se reducirán como así también la necesidad de adquirir y distribuir hardware para tal efecto.

Encuesta a las empresas de desarrollo de software en Guayaquil

Actualmente en Ecuador existen más de 250 empresas dedicadas al desarrollo de Software, siendo las ciudades con mayor presencia de desarrolladores las de Guayaquil, Quito y Cuenca.

Se determinó que existen 250 empresas Desarrolladoras de Software asentadas en estas tres ciudades, distribuidas de la siguiente manera: 60 en Guayaquil, 164 en Quito, y 26 en Cuenca. En Guayaquil y Cuenca la mayoría de las empresas son pequeñas mientras que en Quito son medianas y grandes (Espinoza & Barzola, 2017)

[2]MFA Autenticación Multi Factor, es un Sistema de seguridad que requiere más de una forma de autenticación lo que garantiza su idoneidad en cuanto al acceso a la misma (OnTek, 2020).

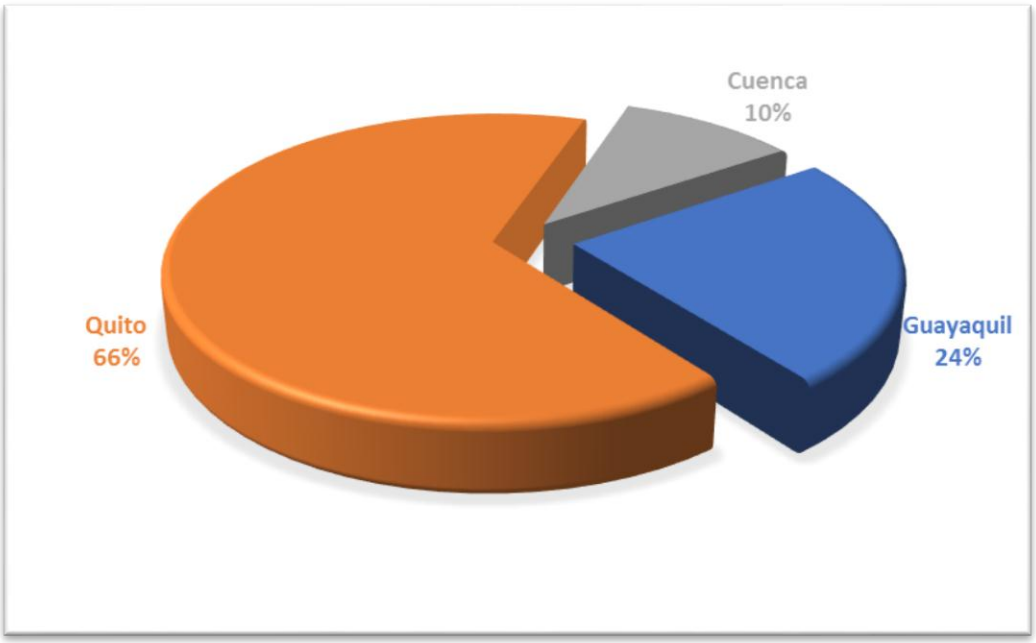

Figura 5 Empresas de desarrollo de software en Ecuador -Principales ciudades
Fuente: (Computeworld, 2015)

En la ciudad de Guayaquil existen 60 empresas de desarrollo de software, por lo cual es imperante para el desarrollo de la presente investigación, saber cuántas de estas empresas cuentan con la certificación ISO 27001:2013 que es la que garantiza de acuerdo a su normativa la Seguridad de la Información.

Para este efecto se realizó una encuesta telefónica dirigiendo una sola pregunta que es saber si cuentan o no con la certificación, como resultado de la misma solo 22 empresas cuentan con el certificado, correspondiendo al 37%, y 38 empresas no cuentan con el certificado correspondiendo al 63%.

Figura 6 Resultado de la encuesta aplicada a las empresas de desarrollo de software
Fuente: Investigación del autor

Guía de consideraciones para garantizar la Seguridad de la Información promoviendo el teletrabajo aplicando la norma ISO27001:2013

En esta parte de la investigación se detallan las consideraciones de seguridad recomendadas para promover el teletrabajo en las empresas, las mismas que están alineadas a la aplicación de la norma ISO 27001:2013 a fin de garantizar la Seguridad de la Información en las empresas de Desarrollo de Software.

Es importante contar con una estrategia que permita establecer ciclos de mejora continua, el más recomendado es el ciclo Deming, también denominado PHVA, esta consta de cuatro pasos que son Planear, Hacer, Verificar y Actuar.

Planear, - Es cuando se definen los temas a trabajar, se identifican los riesgos, se establecen las acciones a seguir, se trabaja en definir las alternativas para el tratamiento de los riesgos, aceptando su situación actual y estableciendo las acciones para mitigarlos o eliminarlos.

Hacer, - En esta parte del ciclo se pone en acción los planes para mitigar o tratar los riesgos encontrados, se implementan controles, se definen los indicadores de gestión, se gestiona el trabajo y alcance del Sistema de Gestión de Seguridad de la Información, también se debe implementar los procedimientos y controles para gestionar los incidentes que se puedan presentar con los incidentes de seguridad.

Verificar, - Es cuando se realiza los seguimientos y revisión de los controles con la finalidad de garantizar la eficacia del Sistema de Gestión de Seguridad de la Información, también se debe probar la eficacia de los controles de seguridad y también que se cumplan con los requerimientos de seguridad, también deben ser evaluados los riesgos de manera periódica, y complementar realizando auditorías internas que garanticen el cumplimiento de las normas y políticas establecidas.

Es importante también actualizar los planes de seguridad, adicional a que deben establecerse áreas de mejora del Sistema de Gestión de Seguridad de la Información, como así también dejar registradas las situaciones o acciones que podrían repercutir a la eficacia del SGSI.

Actuar, - En esta parte deben ser implementadas todas las acciones de mejora que fueron identificadas en las auditorias, tanto preventivamente, como correctivamente, siendo uno de los factores principales el de la comunicación ya que debe ser comunicado a todas las áreas involucradas, de esta manera se lograra el compromiso y que se cumplan todos los objetivos trazados o planificados.

Figura 7 Ciclo Deming
Fuente: (Gestion.org, 2018)

Posterior a lasconsideraciones de mejora continua, es de suma importancia establecer auditorías a la seguridad de la información, de esta manera se realizarán análisis y evaluaciones de riesgos aplicados ala seguridad de la información la misma que debe estar realizada bajo la normaISO/IEC 27001, por lo tanto, para aplicar teletrabajo en empresas de desarrollo de software debemos cuidar siempre que se cumplan y se respeten las normas de seguridad establecidas.

La norma ISO 27001 indica que deberealizarse el proceso de control en etapas sucesivas, las mismas que deben contar de objetivos y metas, las cuales deberán cumplirse, pues al ser un proceso continuo y sucesivo deben utilizarse los resultados de la primera en la segunda y así sucesivamente.

Fase I. Determinación de riesgos, amenazasy vulnerabilidades

En esta parte debe hacerse un análisis pormenorizado de los riesgos, amenazas y vulnerabilidades de cada una de los puntos donde se instalará el teletrabajo, para esto deberán

realizarse visitas o auditorías al sitio donde estará el desarrollador aplicará el teletrabajo, es común que este se desarrolle en el domicilio del desarrollador, de esta manera los auditores definen, una vez realizada la visita se definen las vulnerabilidades o amenazas encontradas, determinando también los riesgos en los que podría estar siendo vulnerable o podría ser afectada la organización.

Como parte final en esta fase se seleccionan los dominios y objetivos de control de acuerdo a la norma ISO/IEC 27001, pues de acuerdo a esta norma se evaluarán los servicios, procesos y al personal que está aplicando teletrabajo, los análisis de riesgos se enfocan en analizar los activos informáticos disponibles, así como también los riesgos, amenazas y vulnerabilidades que puedan presentarse.

Fase II: Análisis de riesgos y diagnóstico de la seguridad de la información:

En esta fase se utilizará el estándar MAGERIT para el análisis y evaluación de riesgos, el mismo que permite valorar los criterios de información evaluados, identificando las posibles causas a los hallazgos confirmados, lo que facilitará la disminución o eliminación de los riesgos encontrados y que estos no vuelvan a repetirse.

El estándar MAGERIT en su versión 3.0 permite hacer una clasificación de las amenazas y riesgos, esta muestra las escalas de valoración y los criterios de información que serán evaluados, en esta fase también deben ser aplicadas las listas de chequeo que determinan la existencia de controles de la Seguridad de la Información, de acuerdo a la norma ISO/IEC 27002.

Fase III. Definición de controles para el diseño del SGSI que incluya políticas y procedimientos para mitigar los riesgos:

En esta fase, una vez definidas las causas que originaron los hallazgos, se definen los controles adecuados de acuerdo a la norma ISO/IEC 27002, diseñando políticas y procedimientos en las cuales incluyan los controles necesarios y que permitirán establecer el Sistema de Gestión de Seguridad de la Información SGSI.

Una vez terminada esta fase, se debe elaborar un informe final que servirá de base para el diseño e implementación del SGSI, teniendo en cuenta el ciclo de mejora continua PHVA que facilite planear, hacer, verificar y actuar, logrando el control de todos los procesos y servicios dentro de la organización.

Conclusiones

Mediante la presente investigación se pudo establecer qué tipo de controles son los que se deben implementar para garantizar la Seguridad de la Información, los cuales permiten establecer las vulnerabilidades y establecer los mecanismos de control al implementar el teletrabajo en las empresas de software.

También se pudo identificar las ventajas de establecer el teletrabajo en una empresa de software, entre las cuales se puede mencionar como la mejora del ambiente laboral del trabajador, incrementa la calidad del trabajo y su productividad, es más flexible, disminuye los costos, brinda más tiempo al trabajador y lo hace más responsable, ya que el trabajo se lo realiza por objetivos, existen también ventajas para la empresa como la reducción del espacio físico, la disminución de gastos en alimentación, uniformes y transporte, e incremento de la productividad.

En cuanto a las amenazas y riesgos también se pudo establecer diferentes formas de amenazas y riesgos que podrían afectar, entre ellas la calidad de conexión, la seguridad en los protocolos de acceso al sistema de la empresa, en no contar con accesorios que permitan la encriptación o acceso seguro.

Se pudo establecer que mediante un sistema de control de Gestión de la Información alineado al estándar ISO/IEC 27001, es posible evaluar los riesgos probables de la Seguridad de la Información, aplicando un proceso de mejora continua VHPA y complementado aplicando por fases la política de control de acuerdo a la norma ISO/IEC 27001:2013.

Bibliografía

BASC-Costa Rica. (2018). Obtenido de www.centa.gob.sv: http://www.centa.gob.sv/docs/PLANIFICACION/4.7%20Riesgos%20Informaticos%20descriptivos.pdf

Carrillo, F. A. (2015). Obtenido de http://ri.uaemex.mx: http://ri.uaemex.mx/oca/view/20.500.11799/35134/1/secme-21544.pdf

Civit, & March, M. y. (2000). *Implementación del Teletrabajo en la Empresa.* Barcelona: Ediciones Gestión 2000.

Computeworld. (2015). Software. *Computeword-Ecuador*, 30-46. Obtenido de https://issuu.com/ekosnegocios/docs/cw276-webok

Diario El Universo. (24 de 04 de 2020). Obtenido de www.eluniverso.com: https://www.eluniverso.com/noticias/2020/04/24/nota/7821597/investigacion-mercado-modalidades-trabajo-consultora-deloittetouche

Diaro el Comercio. (2020). Obtenido de https://www.elcomercio.com: https://www.elcomercio.com/actualidad/teletrabajo-consejos-seguridad-informatica-coronavirus.html

Esclante, Z., & Y Otros. (2006). El teletrabajo y sus implicaciones legales en el estado Zulia. *Revista Gaceta Laboral, 12*.

Espinoza, M. A., & Barzola, G. D. (2017). La industria del software en Ecuador: evolución y situación actual. *Espacios*. Obtenido de http://www.revistaespacios.com/a17v38n57/a17v38n57p25.pdf

Gestion.org. (2018). Obtenido de https://www.gestion.org: https://www.gestion.org/la-calidad-total-en-las-empresas/

ISACA, I. 2. (2020). *Estandares de Seguridad,ISACA, COBIT*. Obtenido de www.isaca.org

ISO2700. (2020). Obtenido de https://www.iso27000.es: https://www.iso27000.es/sgsi.html

isotools. (2020). Obtenido de https://www.isotools.org/: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Ministerio de Trabajo. (03 de 2020). Obtenido de http://www.trabajo.gob.ec: http://www.trabajo.gob.ec/wp-content/uploads/2020/03/ACUERDO-MINISTERIAL-Nro.-MDT-2020-080-signed.pdf

normaiso27001. (2019). Obtenido de https://normaiso27001.es/: https://normaiso27001.es/#iso27001

OBS Business School. (2020). Obtenido de https://obsbusiness.school: https://obsbusiness.school/es/blog-investigacion/propiedad-intelectual-y-seguridad-de-la-informacion/10-amenazas-informaticas-en-el-punto-de-mira#:~:text=%22Wannacry%22%20y%20%22Petya%22,Gusano%20inform%C3%A1tico.

OnTek. (2020). Obtenido de www.ontek.net/: https://www.ontek.net/que-es-autenticacion-multifactor/

Palvia, P., Baqir, N., & Nemati, H. (2017). ICT for socio-economic development: A citizens' perspective. *Science Direct, 55(2)*, 160-176. Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S037872061730410X#:~:text=ICT%20has%20the%20potential%20to,life%2C%20education%2C%20and%20healthcare.&text=Using%20this%20methodology%2C%20a%20model,socio%2Deconomic%20development%20is%20presented.

San Esteban Consulting. (2018). Obtenido de https://san-esteban.com: https://san-esteban.com/2013/09/28/iso-270012013-nuevo-standard/

Servicio de Acreditción Ecuatoriano. (29 de 09 de 2017). Obtenido de Servicio de Acreditción Ecuatoriano: https://www.acreditacion.gob.ec/encuesta-iso-2016/

solusoft. (2019). Obtenido de https://www.solusoft.es: https://www.solusoft.es/servicios/desarrollo-de-software

top10VPN. (2019). Obtenido de https://www.top10vpn.com/: https://www.top10vpn.com/mejores-vpn/?v=header&bsid=c0mejse1kw272&gclid=CjwKCAjwps75BRAcEiwAEiACMSkOxfaFQMTheh5MBWR4xh23c4du_8l7Cbk8J2rPF9fv248ca4DuDRoCmhsQAvD_BwE#maincontent

Universidad de Valencia. (2019). Obtenido de https://www.uv.es/: https://www.uv.es/webgid/Descriptiva/331_mtodos.html

Universidad Internacional de Valencia. (2018). Obtenido de https://www.universidadviu.com: https://www.universidadviu.com/vulnerabilidad-informatica-tipos-debilidades-principales/

Welive Security. (16 de 03 de 2020). Obtenido de https://www.welivesecurity.com/la-es/2020/03/16/recomendaciones-seguridad-teletrabajo-covid-19/

welivesecurity. (julio de 2015). Obtenido de https://www.welivesecurity.com/: https://www.welivesecurity.com/la-es/2015/07/02/idea-central-aplicar-iso-27001/

Anexos

Anexo 1

Entrevista realizada al Gerente de la compañía de desarrollo de software de Guayaquil

P.D. Esta entrevista se realizó a compañías que se dedican al servicio de Desarrollo de Software, por temas de seguridad no se revelará el nombre de la empresa que se utilizó como muestreo para la investigación.

Para ejemplo didáctico se utilizará el nombre de Fabrica de Software

1 **¿Tiempo en el mercado?**

La Fabrica de Software tiene 25 años en el mercado nacional e internacional

2 **¿Consideraciones que tomaron en cuenta para aplicar teletrabajo?**

La Fabrica ya tenia inicios de trabajos Home Office, pero por tema del confinamiento y problemas de la pandemia registrada en el 2020, COVID-19 se tuvo que masificar el teletrabajo en la compañía.

Se consideraron varios aspectos para poder realizar Teletrabajo, como obligar a los recursos tener actualizados el software que utilizan en sus laptops personales, el acceso a la información debía de ser cifrada y sus equipos contar con bloqueos de accesos a sus discos duros.

A nivel de enlaces se realizo trabajos con el proveedor de internet para incrementar el ancho de banda.

3 **¿Tienen ustedes alguna normativa o regulación para aplicar la seguridad de la información en la aplicación de Teletrabajo?**

La Fabrica de Software si cuenta con certificación ISO/IEC:27001 y cuneta con SGCI.

- Políticas de seguridad
- Análisis de Riesgo
- Gestión de Riesgo

4 ¿Qué los llevo a certificarse en la norma ISO/IEC 27001:2013?

Al ser una empresa de servicio de Core Bancario, por normativas y regulaciones del país es obligado tener este tipo de certificaciones.

5 ¿Qué consideraciones debe tenerse en cuenta para poder autorizar a un desarrollador a fin de aplicar teletrabajo?

Para que el recurso trabaje desde su casa practicando teletrabajo debe considerar:

- Buenas practicas de seguridad de la información
- Mantener su Sistema Operativo Actualizado
- Mantener seguridad de acceso con usuario/clave de su equipo de trabajo
- Contar con un Antivirus actualizado
- Cifrado en los correos electrónicos
- Bloqueo de los discos duros de su equipo personal
- Utilizar contraseñas robustas y cambiarlas al menos un par de veces al año
- Realizar periódicamente copias de seguridad de la información de su equipo
- Instalar software licenciados

Anexo 2

Encuesta realizada a las compañías de desarrollo de software de la ciudad de Guayaquil

¿Cuenta su compañía con certificación de Seguridad de la Información bajo la Norma ISO 27001:2013?

SI

NO

Anexo 3

ACUERDO-MINISTERIAL-Nro.-MDT-2020-080 Normativa del teletrabajo en Ecuador por situación emergente ante el COVID-19

Art. 1.- Del Objeto. - El objeto del presente acuerdo es viabilizar la aplicación de teletrabajo emergente durante la declaratoria de emergencia sanitaria por coronavirus (COVID-19).

Art. 2.- Del Ámbito. – En virtud de la emergencia sanitaria declarada, las directrices del presente acuerdo son de aplicación para las instituciones del sector público, de conformidad con el artículo 225 de la Constitución de la República del Ecuador; así como para el sector privado.

Art. 3.- De la adopción de teletrabajo emergente. – A fin de garantizar la salud de los trabajadores y servidores públicos, durante la emergencia sanitaria declarada; será de potestad de la máxima autoridad institucional del sector público y/o del empleador del sector privado adoptar la implementación de teletrabajo emergente.

Art. 4. – De la implementación de teletrabajo emergente. – Es la prestación de servicios de carácter no presencial en jornadas ordinarias o especiales de trabajo, a través de la cual la o el servidor público o la o el trabajador realizar sus actividades fuera de las instalaciones en las que habitualmente desarrolla sus actividades laborales.

La implementación de teletrabajo emergente en relación contractuales existentes, modifica únicamente el lugar en que efectúa el trabajo, sin afectar ni alterar las condiciones esenciales de la relación laboral, por tanto, no vulnera derechos y no constituye causal de terminación de la relación de trabajo.

Durante la emergencia sanitaria declarada, el teletrabajo emergente tanto para el sector público como para el privado se aplicará de la siguiente manera:

a) La máxima autoridad institucional del sector público o empleador del sector privado, autoriza prestar sus servicios desde fuera de las instalaciones habituales de trabajo precautelando la prestación y operatividad de servicios.
b) Corresponde a la máxima autoridad institucional del sector público o al empleador del sector privado; o sus delegados, establecer directrices, controlar y monitorear las actividades que la o el teletrabajador emergente ejecute durante la emergencia sanitaria declarada.
c) La o el teletrabajador será responsable del cuidado y custodia de las herramientas y/o equipos para el desarrollo del teletrabajo emergente que le sean provistos.
d) La o el teletrabajador emergente es responsable de la custodia y confidencialidad de la información, que será exclusivamente utilizada para la ejecución del trabajo.
e) Para la implementación e inicio del teletrabajo emergente, solo será necesario el registro descrito en el siguiente artículo.

Los servidores públicos y trabajadores a los cuales la autoridad competente les disponga aislamiento como medida de prevención para evitar el contagio, se acogerán al teletrabajo emergente.

Art. 5. – Del registro de teletrabajo emergente. – Para el sector público la Unidad de Administración del Talento Humano institucional deberá remitir al correo electrónico infoteltrabajo@trabajo.gob.ec, el formulario de registro de teletrabajadores emergente disponibles en nuestra página web www.trabajo.gob.ec/registro-4/.

Para los empleadores del sector privado, el registro lo deberán realizar en la plataforma SUT (Sistema Único de Trabajo), editando el registro vigente de cada trabajador.

Con la información remitida el Ministerio de Trabajo realizará el registro de los servidores públicos y trabajadores que se acogieron a esta modalidad.

Art. 6. – De la terminación de teletrabajo emergente. – El teletrabajo podrá culminar por:

a) Acuerdo de las partes.
b) Finalización de la declaración de emergencia sanitaria (Ministerio de Trabajo, 2020)