UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2021 - ABRIL 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA:

Análisis de un SGSI con Normas ISO/IEC 27001 para complementar las normas de control interno de CGE, relacionadas con Tecnologías de la Información para el Gobierno Autónomo Descentralizado del Cantón Guaranda.

EGRESADA:

GABRIELA NATHALY GAROFALO SERRANO.

TUTOR:

ING. HARRY ADOLFO SALTOS VITERI.

RESUMEN

La seguridad de la información, es notorio entre cualquier entidad, empresa o institución. El Gobierno Autónomo Descentralizado del Cantón Guaranda, es una entidad pública gubernamental, donde se maneja información y a la vez se ejecutan diversos procesos, mediante este caso de estudio se busca analizar y garantizar la Seguridad de la Información de dichos procesos. La indicada norma está compuesta de varios dominios entre ellas políticas de seguridad, gestión de activos, control de acceso, recursos humanos y la seguridad física cada una de ellas constan con controles definidos que serán analizados detenidamente. La fase del análisis y evaluación del estado sobre la seguridad de la información se obtienen por medio de entrevistas, análisis y observación directa mediante visitas realizadas frecuentemente a la institución.

Una vez concluido el estado actual de la institución se origina a definir la relevancia esperada para posteriormente cumplir con el análisis completo de los controles que serán aplicados por medio de una declaración de aplicabilidad basada necesariamente en las necesidades institucionales, posteriormente se especifica políticas de seguridad para una gestión adecuada de la seguridad de la información, dichas políticas se instauran dentro de los límites de cumplimiento institucional.

Palabras Claves

SGSI, Norma ISO/IEC 27001, Seguridad de la Información, Riesgos, Amenazas.

INTRODUCCIÓN

En la actualidad la importancia de la seguridad de la información es muy indispensable para una empresa e instituciones, tanto en lo que se refiere a la parte física la cual es que se encarga del almacenamiento de toda la información, en la parte administrativa se trabaja en el manejo adecuado de la misma. Además del incremento de ataques a nivel organizacional podría verse afectada por las continuidades operacionales de la empresa, esto hace necesaria la búsqueda de soluciones porque así permite contrarrestar el impacto que generaría dichas amenazas.

En la actualidad la mayor parte de la información se tiende a guardar en forma digital, y esto hace que no solo se pueda ceder a la misma de una manera local, para lo cual se tienen grandes redes que conectan a varias partes del mundo, es decir viaja grandes distancias hasta que llega a su destino, y es ahí donde la seguridad de la información trata de impedir que pase algo que complique la llegada a su destino de una forma correcta.

Del mismo modo una gran cantidad de equipos interconectados entre sí, esto con el fin de tener un intercambio de información, también se debe advertir que solo puedan acceder a ella los usuarios que estén estrictamente autorizados, con respecto al manejo que dichos usuarios realizan mediante su acceso sea debidamente controlado, es decir, la seguridad de la información se debe detectar, corregir y prevenir errores en la entrega de la misma.

DESARROLLO

El GAD del Cantón Guaranda, es un organismo autónomo, descentralizado que impulsa al desarrollo social, étnico, cultural, económico y ético del cantón, coordinando y facilitando los esfuerzos y talento humano, a su vez la planificación, organización, dirección y control de procesos políticos administrativos orientados a satisfacer las aspiraciones y necesidades ciudadanas. Es por eso que el poder ejecutivo está representado por el alcalde, y el poder legislativo está formado por los miembros del Consejo cantonal. Por disposición del artículo 238 de la Constitución de la República de 2008, "Los gobiernos autónomos descentralizados gozarán de autonomía política, administrativa y financiera, y se regirán por los principios de solidaridad, subsidiariedad, equidad territorial, integración y participación ciudadana. En ningún caso el ejercicio de la autonomía permitirá la secesión del territorio nacional. Constituyen gobiernos autónomos descentralizados las juntas parroquiales rurales, los concejos municipales, los concejos metropolitanos, los consejos provinciales y los consejos regionales".

Cabe mencionar, además que circula información relevante que se almacena en las bases de datos del sistema, aquellas albergan información del sistema financiero, impuestos prediales, información de trabajos de agua potable y el registro de la propiedad todos estos datos se encuentran propensos a ser atacados de diferente manera, lo que requiere un sistema de seguridad que garantice el acceso solo a persona autorizadas.

Se debe asociar que la evolución de la información, tecnología y métodos para vulnerar sistemas informáticos de los entes gubernamentales han puesto en alerta a las

organizaciones internacionales dedicadas a la seguridad con el fin de resguardar la información dentro de estas a través de normas, variantes de malware, ataques dirigidos.

Muchas veces la inadecuada inversión en dispositivos, aplicaciones y ausencia de normas de seguridad, da paso a vulnerabilidades que provocan la pérdida de información mediante infiltraciones de intrusos en los equipos conectados a la red, por lo que es necesario ejecutar un análisis de estas amenazas en un contexto general, con las principales causas que puedan provocar los incidentes que las normas y estándares internacionales proporcionan los mecanismos de seguridad garantizados en un rendimiento más óptimo en correspondencia a la seguridad de un departamento informático para desarrollar la confianza dentro del mismo a los proveedores, socios de negocio y empleados de manera sustentable.

En Ecuador, varios entes públicos y privados contextualizan a la información como un problema tecnológico, ya que es tiempo de reconsiderar los programas de seguridad de la información y las estrategias que las compañías deben emplear para sostener a salvo sus activos más valiosos. La seguridad de la información debe estar alineada estratégicamente con la agenda de negocios más general y basarse en la tolerancia al riesgo de una organización.

De manera que estas áreas han sido poco estudiadas tanto la gestión de riesgos como la seguridad informática a pesar de ser fundamentales no se ha incursionado dentro de estos ámbitos, a pesar de ser importantes puntos a tomar en cuenta dentro de cualquier empresa, institución y organización en la que se trabaje con un sistema informático.

Al existir varias diferencias dentro de los sistemas, cada momento se desarrollan nuevos métodos los mismos que afectan a la seguridad de la información, por esto es

necesario llevar a cabo un análisis de las amenazas existentes para poder definir un sistema de gestión de seguridad de la información de modo que ayudará a minimizar los riesgos al sistema de forma no autorizada, minimizando de esta manera el porcentaje de riesgo.

Dentro del Gobierno Autónomo Descentralizado del Cantón Guaranda se trabaja con información muy relevante de los ciudadanos del Cantón. En tal sentido es imprescindible mantener la seguridad de los sistemas con los que se trabaja cada uno de los departamentos de la municipalidad teniendo en cuenta que dicha información debe considerar aspectos como: confidencialidad, integridad y disponibilidad.

Por aquello dentro del GAD municipal del cantón Guaranda no tiene implementado ningún estándar, para asegurar la información cuenta con varias medidas preventivas las mismas que no garantizan de manera adecuada la seguridad de la información, debido a esto es posible que entidades maliciosas accedan a los datos que se manejan dentro de la institución.

En tal sentido, la línea de investigación que se sigue para este caso de estudio es la de Desarrollo de sistema informático y la sublínea es redes y tecnologías inteligentes de software y hardware porque está relacionado con Análisis de un SGSI con Normas ISO/IEC 27001 para complementar las normas de control interno de CGE, relacionadas con Tecnologías de la Información para el Gobierno Autónomo Descentralizado del Cantón Guaranda.

Consecutivamente la necesidad de que las empresas y organizaciones cuenten con normativas o sistemas de gestión de seguridad de la información, el mismo que permita de manera garantizada otorgar la información y datos que cumplan con aspectos

de confidencialidad, integridad y disponibilidad hacen que sea casi una obligación cumplir con esta.

Un SGSI en la ISO 27001 permite un manejo adecuado de la gestión de la información dentro del GAD municipal el mismo que no cuenta con una metodología que les ayude a proteger de manera adecuada su información, existen varios estándares aplicables a una organización gubernamental en este caso se decidió trabajar bajo la ISO/IEC 27001 debido a que la misma permitirá crear una estructura de seguridad de la información.

Puesto que este sistema traerá consigo diversos beneficios entre los cuales están tres puntos fundamentales como son la integridad, confidencialidad y disponibilidad. Además, se otorgarán una serie de ventajas para la institución debido a una adecuada administración que debe traer consigo mayor eficacia dentro de todos los protocolos que utilizan (Javier Solarte, 2015).

Es importante conocer aspectos teóricos que fundamentan este caso de estudio, por lo que se ha investigado bibliografía relacionada:

El estándar ISO/IEC 27001 se publica el 15 de octubre del año 2005 por ISO e IEC que conforman una metodología para la estandarización universal. La norma principal de la serie ISO 27000 contiene requisitos para la implementación del sistema de gestión de seguridad de la información (ISO/IEC, 2011).

El estándar proporciona un modelo que permite establecer, implementar, monitorear, revisar y mejorar un Sistema de Gestión De Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI en una organización es influenciado

por las necesidades, objetivos y requerimientos de seguridad, los procesos empleados, el tamaño y estructura de la organización (ISO/IEC, 2011).

La norma ISO 27001 es una herramienta técnica de mejora continua basada en la metodología PDCA, que permite implementar un Sistema de Gestión de Seguridad de la Información

Áreas o Dominios de Seguridad de la ISO/IEC 27001

1. Políticas de seguridad.
2. Organización de seguridad.
3. Administración de activos.
4. Seguridad física y ambiental.
5. Seguridad de los recursos humanos.
6. Gestión de comunicaciones y operaciones.
7. Sistema de control de accesos.
8. Adquisición, desarrollo y mantenimiento de sistemas de información.
9. Administración de seguridad de la información en la gestión de continuidad del negocio.
10. Plan de continuidad del negocio.
11. Cumplimiento.
12. Gestión de incidentes en la seguridad informática.
13. Aspectos de seguridad de la información en la gestión de continuidad del negocio.

Dentro de los antecedentes del estándar ISO 27001, hace algunos años no existía la tendencia de certificar procesos, o sistemas de gestión, por ello, ISO 9000 vino a

redefinir en el año 2000 la certificación de los sistemas de gestión de calidad, mediante la norma ISO 9001:2000.

Pero aun en el 2005, no existía una norma ISO que permitiera certificar, por alguna organización mediante sus prácticas de seguridad informática y las alternativas, en esos momentos se certificaban en normas inglesas (BS) o españolas (UNE).

Incluso en el 2005, el estándar más conocido en el entorno de seguridad informática era el ISO 17799, pero con limitación de ser un "código de prácticas" (Information technology-Security techniques- Code of practice for information security management), en el momento que se publica su última revisión, se anuncia el desarrollo de una serie de estándares ISO 27000, dedicada exclusivamente a la seguridad informática. Con eso se le da un nuevo alcance a la seguridad, porque no solo es llevar un código de mejores prácticas sino disponer un estándar certificable de forma similar al ISO 9000 (el primero de esa serie en publicarse fue el ISO 27001) (Logisman, 2011).

Las certificaciones han pasado a ser necesidad para demostrar la existencia de sistemas de gestión, con objeto de asegurar procesos consistentes. En el campo de la seguridad informática se tenían certificaciones por parte de estándares británicos y españoles pero, hace pocos años, la ISO emitió los estándares por los sistemas de gestión de seguridad informática con objeto de certificar que las recomendaciones y buenas prácticas brinden una ventaja competitiva a las organizaciones, y no dejar descubiertos todos los sistemas de información que dia con dia cobran una mayor importancia para sustentar la toma de decisiones y salvaguardar el activo más importante de una organización: la información.

Sistema de gestión de seguridad de la información (SGSI), es el concepto central sobre el que se construye ISO/IEC 27001, garantiza un nivel de protección total, si no se cuenta con una planificación adecuada, en el caso de disponer de un gran presupuesto.

El principio de un SGSI es garantizar los riegos de la seguridad de la información sean conocidos, asumidos y gestionados por la organización de una forma documentada, sistematizada, eficiente y adaptada a los cambios que se produzcan en los riesgos, en el entorno y la tecnología (Neira & Spohr, 2016).

El sistema de gestión y seguridad de la información, según ISO 27001 (ISO/IEC 27001), consiste en alcanzar confidencialidad, integridad y disponibilidad de los activos más importantes de la organización.

Tenemos tres términos constituyen la base del SGSI su análisis se describe a continuación:

Confidencialidad: Es el requisito que intenta que la información privada o secreta no se delate a individuos no autorizados. La protección de la confidencialidad se aplica a los datos almacenados durante su procedimiento, mientras se transmiten y se encuentran en tránsito (Bertolin, 2008).

Asimismo, existen otros objetivos más generales como:

- Conocer todos los riesgos de seguridad asociados a la organización.
- Establecer un conjunto equilibrado de requisitos de seguridad de acuerdo con los riesgos identificados, para satisfacer las necesidades de un determinado proceso de negocio.

Al tener claro estos objetivos lo primero que se debe realizar es una lista de todos los activos de cada departamento con su respectivo análisis de riesgo.

La gestión de riesgo es una parte importante de la gestión de la seguridad y se define como el proceso que se encarga de identificar y cuantificar la probabilidad de que se produzcan amenazas y de establecer un nivel aceptable de riesgo para la organización, considerando el impacto potencial de un incidente no deseado.

Las valoraciones de riesgos es el proceso consistente en identificar los problemas antes que aparezcan.

En la gestión de riesgos, existe un factor de incertidumbre asociado con la probabilidad de que aparezcan las amenazas, que sea diferente, dependiendo de cada situación. Cada amenaza se puede predecir dentro de ciertos límites.

Un incidente no deseado presenta tres componentes: amenazas, vulnerabilidad e impacto. La vulnerabilidad indica la debilidad del activo que puede ser explotada por una amenaza. Los riesgos disminuyen con controles o medidas (Bertolin, 2008).

Elementos de gestión de la seguridad de los sistemas de información.

Entre los elementos involucrados están:

- Identificación de todos los activos
- Identificación de amenazas a los activos
- Identificación de vulnerabilidades
- Identificación de impacto
- Identificación de riesgos
- Aplicación de controles

Integridad: Se encarga de garantizar que la información del sistema no haya sido alterada por usuarios no autorizados mientras se almacena, procesan o transmiten así evitando la pérdida de consistencia (Bertolin, 2008).

Disponibilidad y accesibilidad de los sistemas y datos: Solo para uso autorizado, es un requisito necesario que garantiza que el sistema trabaja puntualmente, con prontitud y que no se deniegue a ningún usuario autorizado (Bertolin, 2008).

Alcance del estándar

El estándar abarca organizaciones como: empresas comerciales, agencias gubernamentales, instituciones sin fines de lucro, etc. Especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos generales de la organización (ISO/IEC, 2011).

El SGSI dispone un ciclo continúo conocido por sus siglas PDCA o ciclo de Deming, llamado así en honor a su creador el estadista estadounidense William Edwards Deming, el cual se sustenta en que cuatro fases fundamentales: Planificar- Hacer- Verificar- Actuar (acrónimo de sus siglas en inglés Plan- Do-Check-Act), que es tradicional en los sistemas de gestión de calidad, este proceso mejora continuamente para que así, el sistema tenga un largo ciclo de vida (Excellence I, 2016).

A continuación, se detalla cada etapa del proceso.

La planificación establece el alcance, políticas, objetivos, procesos y procedimientos del SGSI en términos de la organización, sus activos, tipo de tecnología a utilizar, se identifican los riesgos, amenazas y vulnerabilidades a los que se exponen los activos, y la asignación del propietario del SGSI.

El hacer, esta parte ejecuta el plan de tratamiento de riesgos para alcanzar los objetivos planteados, es aquí donde se gestionan los recursos asignados al SGSI para el

debido mantenimiento de la seguridad de la información implementado procedimiento y controles que permitan una detección y respuesta a los incidentes de seguridad.

La verificación se ejecuta para detectar errores, identificar brechas, detectar incidentes etc. Para garantizar que el modo de seguridad funciona de acuerdo a lo previsto es preciso revisar regularmente la efectividad del SGSI atendiendo al cumplimiento de los objetivos planteados, además de verificar si el alcance definido sigue siendo el adecuado y si las mejoras son evidentes, actualizando los planes de seguridad en base de las conclusiones generadas durante las actividades de revisión, para esto es importante registrar las acciones y eventos que pudieran presentarse sobre la efectividad del SGSI.

El Act (actuar), realiza acciones preventivas y correctivas de acuerdo a las lecciones aprendidas de las experiencias propias y de otras organizaciones, comunicando a las mismas a todas las partes implicadas en el SGSI, y plantear mejoras que alcancen los objetivos previstos. (ISO/IEC, 2011).

Los activos son el medio por el cual una compañía tiene valor hacia el público, la protección de activos debe ser fuerte y confiable, a base de métodos de seguridad para la continuidad de acciones de la organización.

En el caso de que ya no exista información una empresa se detiene, esta información o activo se podrá valuar según el costo que provoque a la empresa esta detección, es decir que tan importante y valioso es el tipo de activo que maneja una entidad, para que sea necesario un sistema de seguridad (SGSI, 2010).

La seguridad de la información es conjunto de métodos preventivos y reactivos de las organizaciones con sus sistemas tecnológicos los cuales permiten salvaguardar la

información. En seguridad de la información se plantea la protección a diferentes niveles (CHALÁ, 2015).

En cuanto a la identificación de amenazas, al tener identificados los activos más valiosos de la organización, es necesario identificar las amenazas desde su origen, y examinar la gravedad en caso de pérdida o al mismo tiempo daño de algún activo, para ellos se identifican las debilidades que existen en el sistema (Seguridad en sistemas de información, 2010).

Las amenazas se clasifican en cuatro grupos:

Destrucción de la información: Este tipo de amenaza busca destruir todo o gran parte de la información para que así no pueda ser utilizada.

La modificación de la información se diversifica el contenido de mensajes, pudiendo cambiar, robar o agregar partes del mismo, en vista de perjudicar las comunicaciones.

El robo de información se produce cuando receptan la información de una manera indebida, por eso cuando se publica ciertas informaciones entre los usuarios que no tienen permiso para acceder a la misma.

Para lo cual interrupción de servicio, consiste en evitar que los usuarios de un servicio accedan al mismo, evitando así que cumplan con las tareas.

La evaluación de riesgos son posibilidades de que una amenaza se materialice aprovechando la vulnerabilidad en el sistema, siendo así, un riesgo no existe, si no existe la vulnerabilidad y no existe la vulnerabilidad cuando no existe alguna amenaza, existen dos formas principales de que los riesgos se materialicen (SGSI, 2010).

Que sea de impacto potencial, producido por un desperfecto provocado mal intencionado para perder la integridad, disponibilidad y confidencialidad de los activos o información. Que sea probable la ocurrencia de un desperfecto o por el mal manejo de los activos sin mala intención.

Las vulnerabilidades son las probabilidades que existen cuando una amenaza se ejecuta contra el sistema, no todos los activos están expuestos a las mismas amenazas, la lista de vulnerabilidades se genera cuando se realiza el análisis de los riesgos (López, 2010).

A continuación, se detalla una lista para analizar diferentes tipos de vulnerabilidades:

- Vulnerabilidades físicas, por ejemplo: incendios, terremotos, inundaciones, etc.
- Las deficiencias en el diseño de los sistemas.
- Software malicioso como son los virus.
- Debilidades en los protocolos utilizados por el sistema.
- Las debilidades en los códigos ejecutados por el sistema.
- Vulnerabilidades humanas con o sin mala intención.

Un ataque es el resultado accidental o a la vez intencionalmente provocado contra el sistema producto de la materialización de una amenaza, un ataque se ejecuta por distintos motivos, su estructura puede ser simple o completamente organizada (López, 2010).

Los tipos de ataques según la función de impacto que tiene los ataques estos se clasifican en:

Ataques activos: Estos alteran, dañan, eliminan o insertan información, también puede darse el caso que manipulen el sistema de manera que alteran la disponibilidad del servicio.

Ataques pasivos: El agente solo ingresa a observar la información y no realizan ninguna acción, solo observa la misma, este tipo de ataques son muy difíciles de detectar ya que no dejan ningún rastro de a su paso (López, 2010).

Ataques en relación al enfoque del SGSI en cuanto a los objetivos principales de la seguridad.

- Ataques de Acceso: Este tipo de ataque es aquel que quiere acceder a los recursos de los activos atacando la privacidad del mismo.
- Ataque de Modificación: Este tipo de ataque es el que una vez dentro del sistema realiza cambios en la información atacando la integridad de los activos.
- Ataque de Denegación de servicio: Este tipo de ataque se enfoca en lo que es alterar la disponibilidad de algún sistema o servicio.

En definitiva, el Ing. Edgar Carpio, jefe de Operaciones de la Cooperativa San José Ltda. En su opinión da a conocer que dentro del GAD del Cantón Guaranda específicamente dentro del Departamento de Tecnologías de la Información se encuentra políticas que están definidas, porque en su mayoría están orientadas hacia los usuarios, la carencia de políticas para los sistemas de información hace que la misma pueda ser vulnerada. Por otro lado, el Ing. Roy Olaya, manifiesta que una vez sufrieron un ataque de saturación en el servicio de internet dentro del Gad municipal, por lo tanto, tuvieron que deshabilitar una interfaz con la cual un servidor se conecta a Internet. El Ing. Fabian Loor comenta que en la actualidad no existe ningún tipo de sistema de

seguridad que proteja la red a nivel lógico como un Firewall ya sea en los equipos o en algún software, donde nos da a entender que la red está abierta al mundo.

Mediante la elaboración del análisis de un SGSI que se llevó a cabo, basado en la norma ISO/IEC 27001, se logra conocer las distintas vulnerabilidades a las que está expuesta la información por la falta de controles sobre la seguridad. Consecuentemente sobre la ejecución del análisis de riesgos se conoce el nivel de impacto que tiene la ocurrencia de las amenazas identificadas ya sea en cada activo de la información que afecta, datos relevantes utilizados o resultantes de la ejecución.

Los resultados obtenidos dan a conocer que, para minimizar los riesgos existentes, según el autor es necesario implementar controles de seguridad, esto va a ayudar a fortalecer los tres aspectos más importantes los cuales son: confidencialidad, integridad y disponibilidad de la información, los resultados también muestran una gran importancia del compromiso y trabajo en equipo que debe tener el Gobierno Autónomo Descentralizado del Cantón Guaranda.

Modalidad de Investigación

Este caso de estudio será de Investigación, análisis y resultado debido a que se recolectara información y más adelante se analizara la misma y por último se recomendara que medida se tiene que tomar para así mejorar la seguridad de la información en la empresa, la investigación será bibliográfica por se utilizara fuentes como libros, documentos, artículos, revistas. La investigación tendrá la modalidad de campo porque se buscara obtener dicha información en el mismo lugar que se llevara a cabo el caso de estudio.

CONCLUSIONES

El Gobierno Autónomo Descentralizado del Cantón Guaranda, actualmente no cuenta con políticas y procedimientos que puedan salvaguardar la seguridad de la información, se realizan procesos, pero estos no se basan en políticas establecidas, es por ello que se aplica ciertas normas, las cuales no garantizan totalmente la integridad, disponibilidad y confidencialidad de la información. Por lo consiguiente se evidenciaron falencias en lo que respecta a la gestión de seguridad de la información, en los servidores por lo que se procesa la información sustancial de la institución, y esto hace que estén expuestos a distintas amenazas y vulnerabilidades, asimismo se deben tomar hechos correctivos para la seguridad de la información para que no sea quebrantada.

De la misma forma para garantizar la gestión de la seguridad de la información del GAD municipal en cuanto a proteger la confiabilidad, disponibilidad e integridad, se ha realizado un análisis donde se ha especificado que varios activos se encuentran desamparados por ende se han concretado políticas de seguridad y controles que consoliden la protección de la información.

BIBLIOGRAFÍA

- Neira, A. L., & Spohr, J. R. (2016). El portal de ISO 27001 en español. Obtenido de www. iso27000. Es
- E. Mi and R. A. Guevara, "Sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para el departamento de tecnologías de la información y comunicación del distrito 18d01 de educación," 2017.
- bsi. (s.f.). Seguridad de la información ISO/IEC 27001. Recuperado el 15 de mayo de 2013, de http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-degestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001
- CHALÁ, A. Y. (mayo de 2015). DISEÑO DEL MODELO DE SEGURIDAD DE DEFENSA EN PROFUNDIDAD EN LOS NIVELES DE USUARIO, RED INTERNA Y RED PERIMETRAL, APLICANDO POLÍTICAS DE SEGURIDAD EN BASE A LA NORMA.
- López, «Seguridad Informática» Editex, 2010, 2016, p. 30.
- Anfinson, D. (2009). Fundamentos de la tecnología de la información: hardware y software para PC. PRENTICE-HALL.
- Excellence, I. (28 de julio de 2017). SGSI. Obtenido de Blog especializado en Sistemas de Gestión: https://www.pmg-ssi.com/2015/07/que-es-sgsi/
- Javier Solarte, F. N., Enríquez Rosero, E. R., & Benavides Ruano, M. d. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL – RTE, 493- 498.
- Javier Areitio Bartolin, Seguridad de la Información – Redes, informática y Sistemas de información.

- Excellence, I. (16 de febrero de 2016). IsoTools Blog Calidad y Excelencia. Obtenido de Descubre qué es un SGSI y cuáles son sus elementos esenciale: https://www.isotools.org/2016/02/16/descubre-que-es-un-sgsi-y-cuales-son-suselementos-esenciales/
- Excellence, I. (Lues de marzo de 2016). Software ISO Riesgos y Seguridad. Obtenido de Sistemas de Gestión de Riesgos y Seguridad: https://www.isotools.org/pdfs-pro/iso27001-sistema-gestion-seguridad-informacion.pdf
- S. G. d. ISO, «Organismos Nacionales de Normalización en Países en Desarrollo,» 2010. [En línea]. Available: http://www.iso.org/iso/fast_forwardes.pdf.

ANEXO 1

FORMULARIO DE ENTREVISTAS

Relacionado con: Análisis de un SGBI con Normas ISO/IEC 27001 para complementar las normas de control interno de CGE, relacionadas con Tecnologías de la Información para el Gobierno Autónomo Descentralizado del Cantón Guaranda.

1. **¿Se aplican políticas que gestionan la seguridad de la información dentro y fuera de la institución?**

2. **¿La red de datos ha sufrido alguna vez algun ataque lógico?**

3. **¿Existe algún sistema de seguridad en la actualidad que proteja la red de algún ataque lógico?**

ANEXO 2

UNIVERSIDAD TECNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
DECANATO

Babahoyo, febrero 16 de 2022
D-FAFI-UTB-041-UT-2022-2

Señor
Luis Medardo Chimbolema
ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUARANDA
Ciudad. -

De mi consideración:

La Universidad Técnica de Babahoyo y la Facultad de Administración, Finanzas e Informática (FAFI), con la finalidad de formar profesionales altamente capacitados busca prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

La Señorita **GAROFALO SERRANO GABRIELA NATHALY,** con cédula de identidad No. 0202113478, Estudiante de la Carrera de Ingeniería en Sistemas, matriculada en el proceso de titulación en el período Noviembre 2021 – Abril 2022, trabajo de titulación modalidad estudio de caso para la obtención del grado académico profesional universitario de tercer nivel como **INGENIERA EN SISTEMAS.** El Estudio de Caso**: ANÁLISIS DE UN SGSI CON NORMAS ISO/IEC 27001 PARA COMPLEMENTAR LAS NORMAS DE CONTROL INTERNO DE CGE RELACIONADAS CON TECNOLOGÍAS DE LA INFORMACIÓN PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GUARANDA.**

Es por esta razón, solicito a usted si es posible se sirva autorizar el permiso respectivo para que la señorita Garofalo pueda desarrollar la investigación en la institución de su acertada dirección.

Por su gentil atención al presente, se extiende el agradecimiento institucional.

Atentamente,

UNIVERSIDAD TECNICA DE BABAHOYO FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA DECANATO

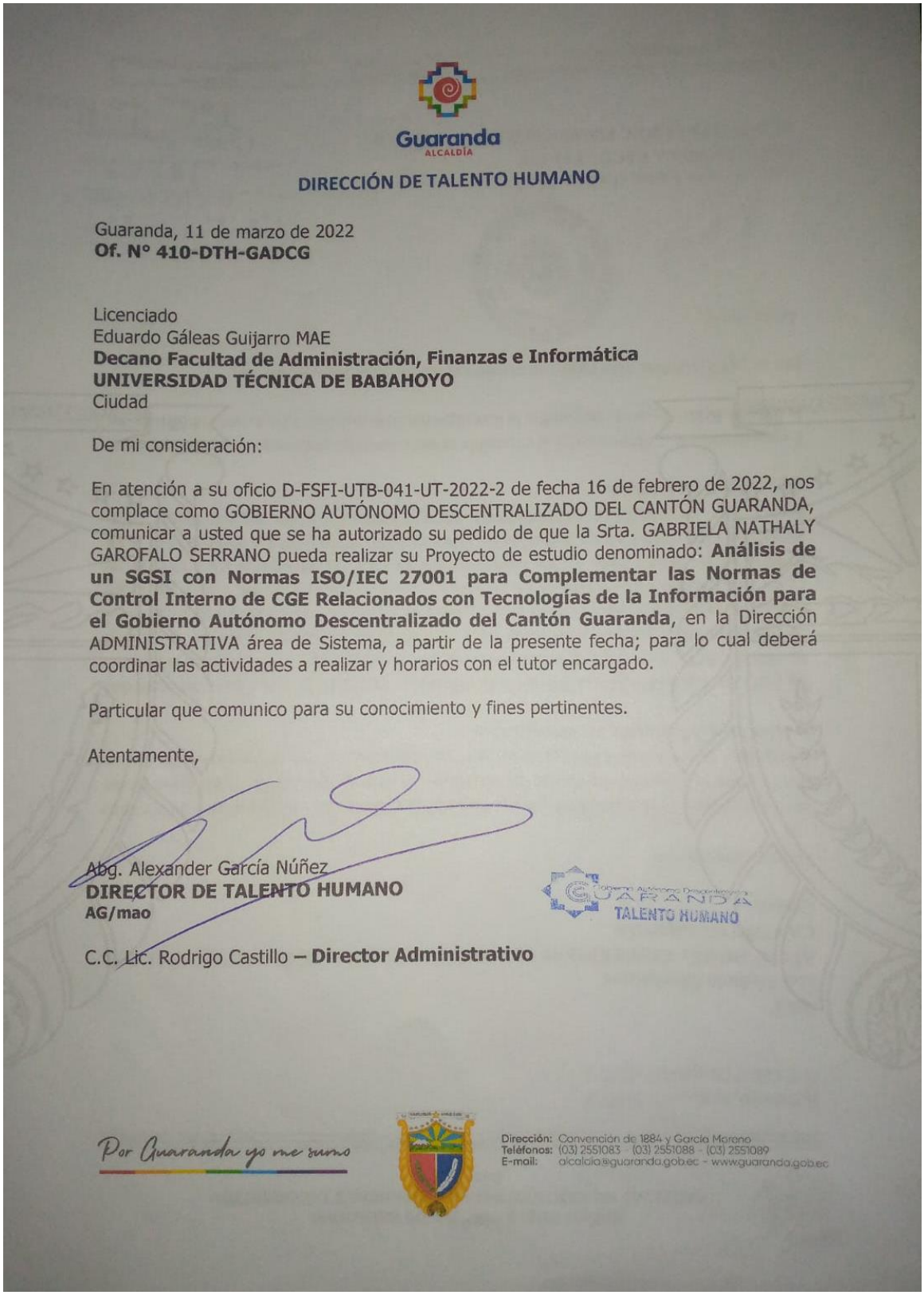
Lcdo. Eduardo Gáleas Guijarro, MAE
DECANO DE LA FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

GUARANDA
RECEPCIÓN
FECHA 07/03/2022
TRAMITE 18023
13:42

Talento Humano

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanatofafi@utb.edu.ec	Elaborado por: Mercedes Soto Valencia	Revisado por: Lcdo. Eduardo Galeas Guijarro, MAE

ANEXO 3



Guaranda
ALCALDÍA

DIRECCIÓN DE TALENTO HUMANO

Guaranda, 11 de marzo de 2022
Of. N° 410-DTH-GADCG

Licenciado
Eduardo Gáleas Guijarro MAE
Decano Facultad de Administración, Finanzas e Informática
UNIVERSIDAD TÉCNICA DE BABAHOYO
Ciudad

De mi consideración:

En atención a su oficio D-FSFI-UTB-041-UT-2022-2 de fecha 16 de febrero de 2022, nos complace como GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA, comunicar a usted que se ha autorizado su pedido de que la Srta. GABRIELA NATHALY GAROFALO SERRANO pueda realizar su Proyecto de estudio denominado: **Análisis de un SGSI con Normas ISO/IEC 27001 para Complementar las Normas de Control Interno de CGE Relacionados con Tecnologías de la Información para el Gobierno Autónomo Descentralizado del Cantón Guaranda**, en la Dirección ADMINISTRATIVA área de Sistema, a partir de la presente fecha; para lo cual deberá coordinar las actividades a realizar y horarios con el tutor encargado.

Particular que comunico para su conocimiento y fines pertinentes.

Atentamente,

Abg. Alexander García Núñez
DIRECTOR DE TALENTO HUMANO
AG/mao

GUARANDA
TALENTO HUMANO

C.C. Lic. Rodrigo Castillo – **Director Administrativo**

Por Guaranda yo me sumo

Dirección: Convención de 1884 y García Moreno
Teléfonos: (03) 2551083 (03) 2551088 - (03) 2551089
E-mail: alcaldia@guaranda.gob.ec - www.guaranda.gob.ec