UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE – MARZO 2019

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA:

ESTUDIO DE LOS FACTORES QUE INCIDEN EN LA FUGA DE INFORMACIÓN DIGITAL EN LA RED DEL GAD MUNICIPAL DEL CANTON JUJAN

EGRESADO:

Estiven Joel Solis Tobar

TUTORA:

Ing. Ana del Roció Fernández Torres

AÑO 2019

Tema

Estudio De Los Factores Que Inciden En La Fuga De Información Digital En La Red Del Gad Municipal Del Cantón Jujan

I. Introducción

El cantón Alfredo Baquerizo Moreno (JUJAN), Se encuentra ubicado al noroeste de la provincia del Guayas, a 60 km de Guayaquil, su altura es de 9m sobre el nivel del mar, la temperatura oscila entre 24 y 25 grados centígrados, tiene una población de 25.179 habitantes.

Su economía se basa en la agricultura de productos como: Arroz, Cacao, Caña de Azúcar, Maíz, Banano, Soya y alimentos de Ciclos Cortos.

El GAD Municipal del Cantón Alfredo Baquerizo Moreno (Jujan), se encuentra ubicado en las calles Jaime Roldos aguilera #313 y José Domingo Delgado.

Su Misión es que el Gobierno Autónomo Descentralizado Municipal de A.B.M "JUJAN" contribuye a la sociedad del Cantón de Montecristi brindando obras y servicios públicos de buena calidad en forma equitativa respetando la biodiversidad y la diversidad cultural en consecución del buen vivir; además, trabaja con transparencia y crea espacios para la participación protagónica de la ciudadanía en la toma de decisiones en los ámbitos sociocultural, ambiental económico y político institucional, con lo que promueve el desarrollo cantonal planificado y sustentable del cantón en el corto mediano y largo plazo.

Su Visión es que el Gobierno Autónomo Descentralizado Municipal de A.B.M. "JUJAN", se constituirá en un ejemplo de desarrollo local con un personal capacitado que trabaja planificada mente basado en principios y valores como solidaridad, honestidad, responsabilidad; es una institución que realiza autogestión sostenible y eficiente; promueve la participación de la ciudadanía para la distribución eficaz y equitativa de los recursos; sus servicios son de calidad

y trabaja en forma transparente; sus acciones permiten preservar el medio ambiente, la diversidad cultural, la equidad de género y generacional, convirtiéndolo en un municipio para todas y todos.

En el GAD Municipal (JUJAN) obtiene a diario información de todos los ciudadanos que residen en el cantón, estos datos son almacenados en los servidores los cuales se pueden encontrar vulnerables, debido a que las redes de datos cada vez son más útiles e importantes para cualquier entidad, es necesario conocer las vulnerabilidades y los factores con las que se podría llegar concretarse dejando como resultado la creación de problemas que podrían ocasionar el mal funcionamiento de la red.

II. Desarrollo

La seguridad es uno de los aspectos fundamentales para obtener un adecuado funcionamiento de la red informática, ya que mediante la seguridad se respalda la integridad y confidencialidad de los datos. De tal manera se plantea la necesidad de identificar las amenazas y vulnerabilidades en la red informática en las que se encuentra expuesta, para tener así una percepción sobre la situación actual de la red.

Este trabajo mantiene una sublínea de investigación que se ubica en procesos de transmisión de datos y telecomunicaciones dentro de la línea de investigación de desarrollo de sistemas de la información, comunicación y emprendimientos empresariales y tecnológicos.

Como afirma (Hoyos, 2016) "El estudio de caso es una estrategia cualitativa que busca documentar, interpretar y valorar, en el contexto de su desarrollo, la particularidad y complejidad de un objeto de estudio que es concreto, contemporáneo y no controlable por el investigador."

La metodología cualitativa fue utilizada en este estudio de caso, debido a que la información que se ha obtenido ha sido de fuentes primarias y directas. Las herramientas utilizadas en este caso de estudio fueron: la Entrevista en profundidad es la técnica más empleada en las distintas áreas del conocimiento y también la de Observación que es una técnica para la recogida de datos sobre comportamiento no verbal.

Primero es saber que los municipios son entidades que pertenecen al estado con la función de administrar una ciudad y cantones.

Dicha institución ya antes mencionada es conformada por un Alcalde, que es la máxima autoridad en los terrenos de ese municipio, y por el resto de concejales.

El presupuesto de una municipalidad suele componerse de los aportes realizados por el Estado, por lo general, las autoridades de dicha entidad también están facultadas para cobrar impuestos

y generar recursos propios con los cuales se pueden realizar obras para la cuidad y cantones aledaños.

En la actualidad el GAD Municipal(JUJAN), cuenta con infraestructura de red adecuada a diferencia de la antigua institución no contaba, con esto no se hace referencia que actualmente o antiguamente no pueda tener algún tipo de vulnerabilidades o factores que incidan en la fuga de información digital.

El manejo de la información aún la mantienen de forma física con respaldo digital puesta en medio electrónico, backups que se puede encontrar por toda la infraestructura de red.

La mayoría del personal no tiene la capacitación adecuada con respectos a medios electronicos u computacionales, la manera más fiable es que la institución realice programas de concientización u/o capacitaciones con el hecho del que el trabajador tenga conocimiento de los procesos que están establecidos al momento de la manipulación y clasificación de información. "**El usuario es el eslabón más débil e importante en la cadena"** (Sociales) en lo que se refiere a fuga de información tiene componentes tanto humano como social muy importante.

La delimitante de este caso se basa en dar soporte a la seguridad de la red de una manera más asequible posible, para poder facilitar el estudio de las vulnerabilidades y los factores que puedan incidir en la fuga de información en la red del GAD Municipal (JUJAN).

Ante lo mencionado también es de suma importancia dar a conocer esos factores en lo cual se pueda producir una fuga de información dentro de la institución a continuación se da a conocer de forma breve dichos factores.

Entre los factores tenemos el factor humano es de suma importancia tenerlo en cuenta ya que se encuentra ubicado en la sima de la pirámide de la seguridad, es uno de los elementos más expuesto a ser un blanco habitual de los delincuentes informáticos.

Ellos juegan un rol importante dentro de la institución ya que ellos interactúan a diario con los sistemas computacionales.

Luego de realizarse un analisis a este factor podemos mencionar algunos que otros errores habituales que suele encontrarse en entornos institucionales.

Es común ver escritorios vacios y computadoras personales desatendidas y cualquier persona puede fácilmente acceder a ella y substraer información por el simple hecho de que dicho acceso está abierto sin ningún tipo de seguridad como un bloqueo de pantalla con protección de contraseña.

El uso de dispositivos extraíbles ajenos a la institución, por general es habitual que el empleado posea dichos dispositivos de uno a mas dispositivos de almacenamiento de información con el cual pueden hacer trasferencia de información de un computador a otro.

Muchas de estas personas suelen llevarse almacenada información di dicho trabajo que pudo haber estado manipulando en la institución y por carencia de tiempo no le dio oportunidad de finalizarla en la comodidad de su hogar, a su vez transportan música o juegos desde los computadores personales a la institución no tomando en cuenta que dicha información suele llevar con ellos virus informáticos por el simple hecho de poseer máquinas sin la debida protección adecuada.

No toman en cuenta que suelen ser usuarios temerarios que descargan todo tipo de información si tomar en cuenta que dicha información o la visita a espacios web suelen contener algún contenido que tenga algún tipo de infestación (VIRUS INFORMATICO), y la consecuencia del riesgo que conlleva.

No basta simplemente que la institución se preocupe por la información, sino que deben tener en cuenta todos los escenarios en que las personas o empleados son el primordial factor a una explotación de vulnerabilidades.

El factor externo es un factor de suma importancia a conocer porque dicho factor puede ser de suma importancia como lo es el factor humano.

Este factor tiene como definición a toda relación que existe con organizaciones (OUTSOURCING), aquellas organizaciones que prestan servicios, proveedores, etc.

Es de suma importancia suscribirse con dichas empresas a un acuerdo de confidencialidad al momento que inicie actividades con terceros.

En este factor existe riesgo ya que estos están directamente involucrados con el tratamiento de la información, ya que en dichas instituciones se suelen contratar servicios como los proveedores de internet entre otros, estas organizaciones para brindar sus servicios siempre tienen que tener algún tipo de acceso dentro de la institución o fuera en el caso de dar soporte técnico de modo remoto esto a veces implica que organizaciones terceras trabaje directamente con el usuario final (EMPLEADO).

El factor hardware es un elemento de suma importancia tener en cuenta que la falla de este puede ocasionar perdidas dentro de la institución.

El hardware suele estar expuesto a distintas amenazas como las malas condiciones ambientales, el vandalismo, la falta de fuentes de energia, etc.

El factor software al igual que el factor hardware van de la mano ya que este es aquel que nos permite el procesamiento de información.

En busca de vulnerabilidades el software siempre es atacado, los principales riesgos que está expuesto este factor son el software legal y el ilegal.

El software legal es aquel que siempre este explotado por los delincuentes informáticos en busca de vulnerabilidades, por ello los fabricantes proporcionas actualizaciones o parches que permite la corrección de las fallas que pueda ver en su programación.

El software ilegal son aquellos medios informales que se suele adquirir más fácil y por menor precio que el software legal estos suelen traer acompañados de programas maliciosos que suelen albergase en el sistema sin que se den cuenta.

El factor inmobiliario este factor no solo afecta la seguridad de la información ya que este tiene relación con la seguridad de los recursos humanos.

En este factor se suelen encontrar de forma cotidiana por ejemplo fuentes de energia con algún tipo de falla el cuales son peligrosas si no se le da la debida observación, ya que este tipo de fallas a futuro puede ser fuente principal de incendios o provocar cualquier otro tipo de accidente laboral.

Una fuga de información es un incidente que le da poder a una persona no perteneciente a la institución, dicha información solo tiene que estar disponible para el personal de la misma.

Una fuga deliberada es cuando tiene por objeto ser de manera intencionada, es decir si sufre un ataque en el que se roban, burlan la información confidencial aprovechándose de alguna vulnerabilidad de los sistemas u/o algún fallo de la configuración, también si se engañan para tener acceso a ella mediante el uso de algunas técnicas de la ingeniería social. Estos también son incidentes que se puede dar por el hurto de celulares de uso personal, portátiles o pendrives. El origen de la fuga deliberada de los datos se puede una de manera ajena como en el caso de que roban todos los correos de los clientes, por ciberdelincuentes que quieren de una manera u otra dañar la imagen. (Incibe, 2017)

También se puede tener cierto origen de manera interna, ejemplo, empleados con algún tipo de descontentos que actúan, llevándose, extrayendo u/o enviando información a terceras personas ajenas a la empresa o/u organizaciones, con la intención de para su propio beneficio. Pero la fuga de datos también puede ocurrir por algún error ocurrido por trabajadores o de otra forma no intencionada, como cuando se pierde un dispositivo de almacenamiento de los datos como el pendrive/flashmemory o la portátil, o si se envía por equivocación información que no se debería haber enviado o la utilización de almacenamiento de datos en la nube o de aplicaciones de móviles que no están permitidas y dicha seguridad desconocemos en sí de esa aplicación. (Incibe, 2017)

La fuga de información es aquel incidente de seguridad que tiene un afecto sobre toda la confidencialidad de los datos, hace mucho no se contaba con que para evitar la fuga de información se tiene que empezar por tener que conocer qué información se maneja u/o se clasifica, También es útil la instalación de unos cortafuegos. (Incibe, 2017)

estos resultados con la compañía o/u organización, estrategias, correos electrónicos y las conversaciones interinas son información de manera confidencial, hay que poner protección de la información está sujeta alguna propiedad intelectual como la de especificaciones de productos, código fuente u/o creación o el desarrollo propio, el estudio sobre la competencia entre otros documentos estratégicos, Sin duda la información siempre tiene una sensibilidad para la que está sujeta a la protección de varias informaciones como los datos personales como cuentas bancarias, tarjetas de crédito, etc….. (Incibe, 2017)

Si esta información deja la institución mediante el uso de portátiles, móviles o varios dispositivos externos como discos duros, usb, etc… Que se pierden o se usan para la obtención, la información tiene un alto grado de gravedad si no se tiene control sobre los dispositivos que están permitidos como los byod y sobre dicha información que se puede copiar, la mejora seria si se pudiera controlar qué datos puede copiarse en estos dispositivos, está el caso debe ir de manera o/u otra cifrada a por medio de los correos electrónicos corporativos como también las cuentas de correo gratuitos se puede enviar información a consecuencia de un engaño o de manera voluntaria. Mejoraran do con concienciación el uso del correo electrónico y si se tiene un control la información que se puede enviar por estos medios y en cuales de los casos debe ir de manera cifrada. (Incibe, 2017)

Cuando se están utilizando redes inalámbricas sin ningún tipo de protección, como la de los hoteles, entre otros, por lo que los trabajadores de viaje sin tener una mínima cuenta de que se transmiten y quién puede estar escuchando, mejorar la conciencia a los trabajadores de en qué caso hacer uso de estos tipos de redes, se controla cual información o aplicaciones se pueden usar por fuera de la oficina o si se les proporciona una un punto de red privado para tener acceso desde el exterior de la organización. (Incibe, 2017)

La utilización aplicaciones por cierta empresa de una manera no controlada, para almacenamiento de la información en la nube como el uso de dropbox, google drive, mega, también como son las herramientas de colaboración como la mensajería instantánea o multiconferencia como skype, hangouts, line, viver y entre otras para uso compartidos de archivos como en P2P eMule, uTorrent, se mejoraría si establecen unas ciertas políticas del uso de un software permitido, haciendo el uso de algún bloqueo, instalación o desinstalando. (Incibe, 2017)

Haciendo publicaciones en redes sociales información de manera alguna manera inadecuada, esto es algo que no se tendrían que estar publicándose, cuando se corresponde al usuario sin control. Si de echo se resulta infectados por algún malware que hurta datos troyanos, spyware, keyloggers, stealers y ransomware esta información dejara las instalaciones donde se tenía almacenado o dejará de estar disponible varias veces sin que nadie se dé cuenta . (Incibe, 2017)

Ante la fuga de datos nos hacemos las siguientes preguntas, dónde queda toda la reputación empresarial o/u organizacional, cuáles son aquellos costes cuando ocurre estos tipos de incidentes en la seguridad de los datos, La seguridad de los datos es aquel aspecto que de manera crítica se evita una mala imagen en la que se puede proyectar en la organización la que puede ser incapaz de contener dichos ataques y una fuga de datos. Detrás de los incidentes la

fuga de información se puede esconder un millar de motivo, sean personales, económicas, o simplemente errores. (ARANTXA CALVO MOYANO, s.f.)

Ante esta cuestión fomentada cuáles son esas aquellas políticas de seguridad de los datos que se tiene un manejo de una manera tradicional en varias definiciones y en todas ellas tienen algo en común como el carácter, a la medida que se limitan la actuación de los empleados durante una operación general del mismo sistema y en su alto nivel de abstracción, de una manera que vienen a ser una declaración de intención, un asentamiento de bases que se debe definir y delimitar muchas responsabilidades en las distintas forma que se actúa que requirieren en caso de amenaza u/o ataque. En todo los casos ciertas políticas tiene concreción en toda serie de norma, protocolo, reglamento, en las que, principalmente, se fija el modo de comunicación entre los empleados. (de, 2017)

dichas brechas de seguridad, el verdadero problema es cuando esta información que de una manera u otra son de manera confidenciales que pasan y pasan a manos de terceros ajenos a la empresa, esto ocasiona una manera a otra un mayor incidente en la seguridad para la compañía o/u organización, tiene un mayor golpe en la reputación, tal como le ocurrió a la empresa Sony que en el 2011 sufrió uno de los ataques más escandalosos en la historia. Se dio un cálculo de que el agujero que tuvo en su seguridad pudo ocasionar una pérdida que esta superaría ampliamente los 1.000 millones de dólares. (ARANTXA CALVO MOYANO, s.f.)

“En el escenario los conceptos como reputación corporativa u/o riesgo reputacional van tomado de la mano teniendo relevancia en el ámbito empresarial o/u organizacional propiciando ataques a grandes firmas uniendo al endurecimiento de ciertas normativas”. (ARANTXA CALVO MOYANO, s.f.)

Sin duda alguna, el costo para la organización es una mala reputación. Considerando los riesgos en la reputación de la empresa equivale a proteger la reputación, esto radica la importancia de abordar de forma adecuada todos los riesgos, tomando conciencia de que proteger la reputación de una organización u/o empresa en hacerla mucha mejor. (ARANTXA CALVO MOYANO, s.f.)

Como alega (Deutsch, 2016) "Por eso, a un corto plazo, las empresas que son más afectadas por la fuga de información de forma grave son las más pequeñas. Éstas son un objetivo más fácil para estos delincuentes, tienen menos formas de reacción, no cuentan con mecanismos de defensa ante los problemas legales o las sanciones".

Como afirma (incibe, 2016)"Este tipo de problemas siempre han existido en las empresas o/u organizaciones pero con el uso diario de estas nuevas tecnologías, el proceso y almacenamiento de mayores volúmenes de datos, da un mayor impacto en una filtración. Por otro lado, se encentra con el aumento de una utilización de los dispositivos móviles personales, corporativos para acceder a la red de la empresa, es un riesgo que se le añade a la seguridad de la información una fuga de datos se puede producir de forma accidental, el simple extravió de una portátil, el envío de información de forma errónea, etc…. También se trata de algún incidente provocado, de ejemplo, el descontento de algún trabajar que sustraiga información o por varias técnicas, como ataques que los lleva a cabo un ciberdelincuentes, o de la utilización de ingeniería social, que estas hayan propiciado el hurto de la información para provocar muchos daños a la reputación de la empresa o/u organizaciones con fines económicos".

En las empresas del sector público se manejan muchos tipos de datos llamativos para un atacante, además sensibles al manejo de personal interno y externo de la misma institución. Se presentan muchos tipos de amenazas para la información ya sean físicas o virtuales entre ellas se enumerarán a continuación una lista que debe ser tenida en cuenta cuando se proceda a realizar la evaluación de las vulnerabilidades asociadas el riesgo. En el sector público existen sin número de vulnerabilidades, la vulnerabilidad es la capacidad y posibilidad de un sistema de reaccionar a una amenaza o de recuperarse de un daño, las vulnerabilidades se interrelacionan con las amenazas, estas se basan en un contexto que puede ser Ambiental, Física, Económica, Social, Educativa, Institucional, Política y tecnológica. Por ser un control tecnológico nos podemos encontrar con vulnerabilidades, tales como: Uso no especificado de camuflaje de archivos. Se debe evitar el establecimiento de reglas innecesarias sobre el DLP. No saber que se monitorea o donde se encuentra la información. Incompatibilidad del DLP con otros agentes existentes y que se encuentran en operación. Ejemplo: Antivirus Symantec con Agente DLP McAfee. Se debe alinear la política de actualizaciones de la compañía, con la política de actualizaciones sobre el aplicativo DLP, tanto para los agentes de las maquinas como para servidores. Esto con el fin de evitar alguna falla sobre los clientes que tienen el agente instalado y puedan saltarse el control por falta de actualizaciones. El caso que los usuarios de la maquina tengan permisos para deshabilitar el agente. Los usuarios no deben tener privilegios sobre la carpeta donde quedan las evidencias de DLP. Más que una vulnerabilidad y limitante es que la mayoría solo funcionan en sistemas Operativos Windows.

(http://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_threat_sp.pdf, 2014)

Para para una mitigación el riesgo de una fuga de información se debe fomentar una cultura consciente de seguridad en la que la protección de la información sea una parte normal y natural del trabajo de cada empleado, y no una tarea adicional percibida como una carga o en conflicto con otros objetivos.

Proporcionar herramientas y la educación que los empleados necesitan para mantener la información segura, comenzando por la capacitación de empleados nuevos y luego mediante reforzamiento verbal en vez de por correos electrónicos que pueden perderse o ser ignorados.

Evaluar la conducta de los empleados y los riesgos asociados basándose en factores tales como el país y el panorama de amenazas. Luego de acuerdo con dicha evaluación, diseñe planes de educación sobre amenazas, capacitación en seguridad y procesos comerciales.

Analizar continuamente los riesgos de cada interacción entre usuarios y redes, puntos terminales, aplicaciones, datos y, por supuesto, otros usuarios para siempre tener presente el entorno de amenazas.

Formular, divulgar y hacer cumplir políticas de seguridad sensatas. Simplifique el cumplimiento creando un número limitado de políticas de seguridad fáciles de comprender que estén integradas en los procesos comerciales y concuerden con los requisitos laborales.

Proporcionar un liderazgo claro mediante el compromiso y el ejemplo de la plana ejecutiva, para que los empleados vean que los ejecutivos están comprometidos y se hacen responsables.

Fijar expectativas en relación con la seguridad.

Para una prevención con garantía de muchos tipos de incidentes, se debe mantener en cuenta el tipo de valor en la información a proteger, teniendo una manera objetiva en cuenta le sea posible el impacto que se pueda ocasionar en la organización el robo u/o la pérdida, ya que

puede tener varias consecuencias en función al tipo de información u/o tipo de organización. (incibe, 2016)

Por lo tanto, siempre se debe conocer que información se gestiona en la organización. Esto debe hacerse a mediante entrevistas u/o reuniones con el personal de dicha organización. Clasificarla según un criterio razonable u/o unificado. Determinar el grado de seguridad mediante unas preguntas como, es mayor el riesgo de una pérdida de información, y el de fuga o el hurto de información, puede tener alteraciones sin autorización, Establecer ciertas medidas de manera necesarias para mayor mejora en la seguridad. (incibe, 2016)

El uso de soluciones DLP o la implementación de esta da como resultado mostrar los puntos de vulnerabilidad, posibilitando el establecimiento de un conjunto de soluciones para tener un dominio del ambiente, estos son pasos para la búsqueda de implementar una solución y evitar pérdidas de datos en el ambiente de la institución. Es una manera de reducir riesgos que involucran datos de los usuarios es la implementación de normas y medidas para la protección de la información en el GAD Municipal (JUJAN).

El uso de la norma ISO27001:2013, "Sistema de Gestión de Seguridad de la Información, da resultado para mejorar de forma apropiada y lograr determinar varias amenazas, fijando estrategias y controles necesarios resguardar la información." (Excellence, 2015)

El uso o implementación de un monitoreo de redes, con esto se puede optimizar las instalaciones y componentes de la misma. En si se podrá saber cuándo se necesita más hardware y cuando están sobredimensionados. Con esto se podrá obtener detecciones de cuellos de botella en la red cual pueda ser la causa y como puedan solucionarlo, siempre anticipándose a los problemas y que eviten que lleguen más.

afirma (Marqueting, 2017) “Pandora FMS, En su versión libre es capaz de realizar monitoreo a más de 10,000 nodos y llega a cubrir sin limitaciones monitorización en las redes, de los servidores y de las aplicaciones. Tiene muchas funcionalidades completas para informes, alertas, integraciones, etc…”. Y también “Nagios, Es probablemente una de las herramientas libres más conocidas que nos ofrece un potente sistema de monitorización de código abierto que les permite una monitorización a toda una infraestructura (Information Technology), para correcto aseguramiento en los sistemas, aplicaciones, servicios u/o procesos de negocio que funcionen de manera adecuada”.

CONCLUSIONES Y RECOMENDACIONES

- Todas las entidades incluyendo las del sector público como el GAD Municipal (JUJAN), son vulnerables en algún grado a las amenazas constantes que se presentan contra la información importante y que pueden comprometer cualquiera de sus principales propiedades: Confidencialidad, Integridad y Disponibilidad. Para poder establecer de forma adecuada un sistema DLP de manera que proteja correctamente la información confidencial de la compañía, es necesario que se conozca de manera adecuada cual es la que contiene información sensible de la Organización (Metodología propuesta), quién es el responsable de dicha información, el valor de la información.
- Con la propuesta de este caso de estudio, el cual consiste en proponer un modelo de seguridad para la implementación de soluciones, políticas, buenas-mejores prácticas, protección y control de acceso lógico orientados a la prevención de pérdida de datos en la organización, se cumpla de forma satisfactoria.
- Esta metodología toma el ciclo de vida de los datos electrónicos dentro de la organización, iniciando desde la etapa de creación, almacenamiento, tratamiento, identificación, movimiento y la disposición final de esos datos hasta su destrucción.
- Cuando se inicie un plan de implementación de un sistema DLP, en una empresa del sector público, se deben tener presente los principales, riesgos, amenazas y vulnerabilidades a las que se están expuestas y como se beneficiará, una entidad de este sector cuando se culmine dicho proyecto.

Bibliografía

ARANTXA CALVO MOYANO, D. D. (s.f.). *redseguridad*. Obtenido de redseguridad: http://www.redseguridad.com/especialidades-tic/dlp-y-fraude/fuga-de-informacion-la-mayor-amenaza-para-la-reputacion-corporativa

de, s. (01 de septiembre de 2017). *seguro de* . Obtenido de seguro de : https://www.segurode.com/noticias/ciberriesgos/valor-politicas-seguridad-informatica

Deutsch, V. E. (30 de marzo de 2016). *blogthinkbig.com*. Obtenido de blogthinkbig.com: https://aunclicdelastic.blogthinkbig.com/el-caso-guillaume-y-la-gestion-de-las-fugas-de-informacion/

Excellence, I. (23 de abril de 2015). *ISOTools Excellence*. Obtenido de ISOTools Excellence: https://www.pmg-ssi.com/2015/04/la-importancia-de-la-norma-iso-27001/

Hoyos, Ó. I. (2016). *Metodología para la elaboración de estudios de caso en responsabilidad social.* Colombia. Obtenido de https://books.google.com.ec/books?id=TlUeDQAAQBAJ&pg=PP7&dq=metodologia+cualitativa+de+un+caso+de+estudio&hl=es&sa=X&ved=0ahUKEwjWzvrX_JPUAhWI6yYKHeOvD0YQ6AEIQjAH#v=onepage&q=metodologia%20cualitativa%20de%20un%20caso%20de%20estudio&f=false

http://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_threat_sp.pdf. (2014). *Fuga de datos a nivel mundial: El elevado costo de las amenazas internas.* cisco.

incibe. (05 de mayo de 2016). *incibe_ instituto nacional de ciberseguridad*. Obtenido de incibe_ instituto nacional de ciberseguridad: https://www.incibe.es/protege-tu-empresa/blog/como-puedo-prevenir-fuga-informacion-dentro-empresa

Incibe. (18 de enero de 2017). *incibe-Insituto Nacional de Ciberseguridad*. Obtenido de incibe-Insituto Nacional de Ciberseguridad: https://www.incibe.es/protege-tu-empresa/blog/estas-preparado-hacer-frente-fuga-datos

Marqueting. (10 de marzo de 2017). *APEN25 solutions globals D'informatica I tecnologia*. Obtenido de APEN25 solutions globals D'informatica I tecnologia: https://apen.es/2017/03/10/las-10-mejores-herramientas-de-monitoreo-de-redes-del-2017/

Sociales, C. G. (s.f.). *incibe_instituto nacional de ciberseguridad.* Obtenido de incibe_instituto nacional de ciberseguridad: http://graduadosocial.org/docs/Gestion-fuga-informacion-Graduado_Social.pdf

Anexos

Cuestionario utilizado para la entrevista.

Preguntas

¿Conoce sobre alguna política de seguridad informática existente en el GAD Municipal (JUJAN)?

¿Cree que se mantiene la confidencialidad de la información en la red del GAD Municipal(JUJAN)?

¿Tiene usted algún tipo de conocimiento acerca de los dispositivos electronicos que tiene el GAD Municipal (JUJAN)?

¿El GAD Municipal(JUJAN) tiene algún programa de capacitación en dispositivos electronicos?

¿El GAD Municipal(JUJAN) tiene conexión permanente a internet?

¿Cómo mantienen protegido la información del servidor del GAD Municipal(JUJAN)?

¿Qué información manejan el GAD Municipal(JUJAN)?