MODELO DE SEGURIDAD PARA PLATAFORMAS IAAS DE LA EMPRESA VIRGIN MOBILE

ANDRES ARTURO APONTE AGUDELO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA D.C

2018

MODELO DE SEGURIDAD PARA PLATAFORMAS IAAS DE LA EMPRESA VIRGIN MOBILE

ANDRES ARTURO APONTE AGUDELO

Trabajo de grado para optar el título de

Especialista en seguridad informática

Director de Proyecto

Jorge Enrique Ramírez Montañez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA D.C

2018

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, Octubre 2018

DEDICATORIA

Dedico este proyecto de grado a Dios, mi familia y a mi esposa por su dedicación y comprensión en este nuevo paso profesional que me llevara a alcanzar las metas plateadas en mi crecimiento académico.

A los profesores, tutores y directivos que con su apoyo se logró llevar a satisfacción este trabajo de grado y por su dedicación y entrega al compartir sus conocimientos.

AGRADECIMIENTOS

Agradezco a mi esposa por su apoyo, comprensión y amor durante este nuevo peldaño en mi crecimiento académico. A Dios por darme sabiduría y la oportunidad de alcanzar un logro más.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

1. INTRODUCCION

Con el desarrollo del siguiente trabajo se realizó la definición del modelo de seguridad para el modelo de infraestructura IaaS de la empresa *Virgin Mobile* como recomendación para los administradores IT, las cuales se encuentran en desarrollo a nivel mundial, en las cuales durante la creación de un servidor virtual se crean usuarios genéricos dependiendo del sistema operativo con que se hayan creado.

Al crear un servidor con cualquier Sistema Operativo de distribución *Unix* tiene un único usuario *root* de nombre genérico, lo mismo sucede al crear un servidor con Sistema Operativo Windows el cual se crea un usuario con permisos de administrador local llamado "*Administrator*"

Estas son brechas de seguridad que deben solucionarse de inmediato por parte del administrador de los servidores en el momento en que sea habilitado un servidor y que se recomienda sean aplicadas por las empresas que se encuentran en la búsqueda de modernizar sus modelos de negocios relacionados a su infraestructura enfocada a sus equipos que soportan sus plataformas y que opten por la implementación IaaS.

Adicional a esto también se diseñó los procedimientos estándar necesarios para regular, proteger y asegurar los niveles y permisos requeridos en cuanto a los

accesos por parte de los empleados de la empresa *Virgin Mobile*, esto será evidenciado realizando un análisis inicial, previo al inicio del diseño de los procedimientos nombrados con anterioridad del nivel de seguridad el cual permita dar con un hallazgo y evidenciar las falencias.

Luego de realizar este análisis previo se dio el enfoque adicional para fortalecer estas fallas de controles en los procedimientos con el fin de entregar un documento apto que refleje un estado óptimo de control y una correcta ejecución de un óptimo nivel de seguridad frente una auditoria.

Frente a la falencia y debilidades de los niveles de seguridad, se utilizó un servidor con distribución Linux Ubuntu el cual será empleado como servidor de desarrollo, siendo esta distribución la más empleada en los servidores de la empresa *Virgin Mobile* para dar un enfoque más cercano y apropiado, de esta forma se evidenciaran las fallas y fortalezas que se encontraran y sobre estas fallas se iniciara a trabajar en el documento que constara de los controles necesarios para la mejora de la seguridad en los servidores de producción y desarrollo de la empresa *Virgin Mobile*.

Durante el desarrollo del presente documento se buscó, la creación del diseño de una serie de pasos tomados desde el análisis previo que entregue como resultado un documento de soporte que evidencia claramente las correcciones necesarias para asegurar la estabilidad y confiabilidad del nivel de acceso y seguridad a los servidores de la empresa *Virgin Mobile*.

También compartir los conocimientos adquiridos durante la especialización de seguridad informática para que sean utilizados como herramienta que conduzca hacia un resultado óptimo y que aumente el nivel de seguridad para la empresa *Virgin Mobile* Colombia en su infraestructura localizada en los servidores *Cloud* bajo la modalidad *IaaS*.

2. DEFINICION DEL PROBLEMA

En las organizaciones modernas y como proceso de evolución se busca la optimización de los espacios en las oficinas que son empleados como *datacenter*, *racks* y cuartos técnicos, han movido su infraestructura hacia soluciones más eficientes como lo es el servicio IaaS *(Infraestructure as a Service)*, donde se contrata con una empresa ya sea nacional o internacional unos recursos, este contrato no tiene límites de permanencia sino solamente un pago mensual por la renta y por la colocación de infraestructura en nubes privadas, donde se accede de forma remota a la administración de estos servidores o equipos de red, pero esta solución tiene el inconveniente que los niveles de seguridad ofrecidos son básicos con credenciales de uso regular, debido a que la administración de accesos y regulación de los controles hacen parte y van de la mano del administrador de la empresa contratante del servicio. Como lo reporta en su página INCIBE, (Instituto de Ciberseguridad de España) en su artículo "Riesgos y amenazas en *Cloud Computing*"[1] donde hablan de los riesgos de accesos no permitidos a causa de vulnerabilidades inherentes a esta modalidad de negocio.

[1]Disponible en Internet: Incibe.es. (2018). [online] Available at: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf [Accessed 13 Sep. 2018].

2.1. DESCRIPCIÓN DEL PROBLEMA

Al habilitar un servidor virtual en nube vienen con usuarios genéricos según el sistema operativo con que se hayan creado, por ejemplo:

- Al habilitar un servidor con Sistema Operativo Ubuntu tiene un único usuario *root* llamado "*Ubuntu*".
- Al habilitar un Servidor con Sistema Operativo Debian se crea un usuario con permisos de *root* llamado "*admin*".
- Al habilitar un Servidor con Sistema Operativo *Windows* se crea un usuario con permisos de administrador local llamado "*Administrator*".

Adicional a esto no se tienen los procedimientos estándar necesarios para regular, proteger y asegurar los niveles y permisos requeridos en cuanto a los accesos por parte de los empleados de la empresa *Virgin Mobile*, esto será evidenciado realizando un análisis inicial, previo al inicio del diseño de los procedimientos nombrados con anterioridad del nivel de seguridad el cual permita dar con un hallazgo y evidenciar las falencias.

2.2. FORMULACIÓN DEL PROBLEMA

¿Cómo se puede mejorar los niveles de seguridad en las plataformas IaaS de la empresa *Virgin Mobile*?.

3. JUSTIFICACION

La justificación de este trabajo se fundamenta en el hecho que día a día es mayor la migración de empresas al modelo de negocios en *Cloud*, por todos los beneficios que trae, como lo son la disminución en la renta de espacios para la ubicación de sus instalaciones, además de esta ventaja se debe contemplar que los costos en la escalabilidad ascendente o descendente son mucho menores a la compra, implementación y puesta en marcha de estos mismos recursos en un *datacenter* bajo la responsabilidad de la empresa, otro motivo que está llevando a las empresas a esta migración es la disminución de costos en su mantenimiento físico y soporte anual, ya que estos servidores no lo requieren por parte de las empresas contratantes, pero todas estas ventajas traen por supuesto unas desventajas en paralelo, pues se convierten en foco de ataques por parte de ciberdelincuentes que buscan lucrarse, con el robo de información de las empresas que luego pueden ser vendidas a la competencia, también con el daño en la infraestructura, contratados por empresas rivales que busquen el retraso o daño de la imagen empresarial de sus competidores, o simplemente de atacantes que busquen llamar la atención mostrando su grado de habilidades y destrezas en el campo de las actividades ilícitas y cibercrimen. El motivo que nos impulsa a la realización de este proyecto se centra en la necesidad que mejorar el nivel de seguridad de los servidores de la empresa *Virgin Mobile* los cuales a la fecha anterior a este proyecto no cuenta con ninguna mejora en su seguridad.

Además que se ha detectado a una falencia que radica en que no se tiene ningún control que evidencie los roles y permisos específicos que regulen los accesos para los empleados de la empresa que tienen ingreso a los servidores, debido a esto se busca proponer un aumento de la seguridad de los servidores de la empresa *Virgin Mobile* y la creación de un procedimiento de control de acceso que evidencie los permisos requeridos y otro de mejora en la seguridad de ingreso a los servidores enfocado a sus usuarios, contraseñas y demás procesos que se encuentren débiles en la primera revisión previa al inicio de la ejecución del modelo de seguridad para plataformas IaaS. Una serie de recomendaciones realizadas por el Ministerio de las Tecnologías de la Información y las Comunicaciones de Colombia sobre medidas de seguridad en plataformas *Cloud* en el artículo "Seguridad y Privacidad de la Información"[2] y un ejemplo de la implementación de plataformas en nube por parte de la Universidad de Santander[3] nos permiten ver que hallazgos fueron detectados y que nos ratifican los cambios requeridos.

Además, se tendrá meta la entrega de estos procedimientos que garanticen por parte de las áreas o cargos responsables el resguardo de estos activos de

[2] Disponible en Internet: Anon, (2018). [online] Available at: https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf Disponible en Internet: http://www.udi.edu.co/revistainvestigaciones/index.php/ID/article/download/41/38 [Accessed 10 Aug. 2018].
[3] Disponible en Internet: Anon, (2018). [online] Available at: http://www.udi.edu.co/revistainvestigaciones/index.php/ID/article/download/41/38 [Accessed 8 Jul. 2018].

información de la empresa y brinden las herramientas que permitan mantener a salvo y apoyar de la continuidad del negocio.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Diseñar procedimientos estándar de acceso para las plataformas IaaS virtualizadas de la empresa *Virgin Mobile*, por medio de un análisis de los accesos empleados por los usuarios de la plataforma en *Cloud* en búsqueda de vulnerabilidades latentes.

4.2. OBJETIVOS ESPECÍFICOS

- Realizar un análisis previo de los niveles de seguridad de la información en la configuración de acceso a los servidores, para conocer del estado inicial de la infraestructura de la empresa *Virgin Mobile*.
- Analizar el estado actual de la seguridad de la información en los procedimientos de autorización para los accesos a los servidores de la empresa *Virgin Mobile*.
- Realizar un análisis de brechas de seguridad en los accesos de los empleados a los servidores de la empresa *Virgin Mobile* en búsqueda de fallas procedimentales.

- Definir las acciones de mejora en cuanto al nivel de seguridad en la configuración de acceso a los servidores y equipos *Cloud* con el fin de proteger de vulnerabilidades y amenazas de origen externo e interno hacia los servidores de la empresa Virgin Mobile.

5. MARCO REFERENCIAL

Las empresas que hoy en día se encuentran en el mercado deben buscar estar a la vanguardia de los avances tecnológicos existentes enfocados a la seguridad de sus activos de información sobre los cuales soportan su modelo de negocios y que les aseguran la estabilidad del mismo y para dar una correcta ejecución de este principio deben conocer sus activos y clasificarlos, pero dar el foco a este tema será objeto de análisis los servidores existentes en las plataformas IaaS[4], en este caso de estudio se recordara que en la norma ISO 27001[5], en el ítem A.11 nos habla del tema relacionado al control de accesos, donde hace alusión a que los empleados de las empresas solo requieren tener los accesos necesarios para poder realizar su trabajo y así evitar que tengan privilegios superiores a los necesarios.

También vale recordar que una vulnerabilidad es el mal uso de credenciales o explotación de privilegios elevados por parte un atacante que encuentra permisos en usuarios no controlados[6] y que pueden generar, desde robo de información hasta afectación directa en la operación normal de las plataformas de *core* de las empresas. Pero en este caso no solo existe esta posible vulnerabilidad, sino que también se puede estar frente a un ataque por acceso no permitidos debido a un

[4] Disponible en Internet: FayerWayer. (2018). El origen de: El Cómputo en la Nube. [online] Available at: https://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/ [Accessed 8 Feb. 2018].
5 Disponible en Intenet: Anon, (2018). [online] Available at: http://www.iso27000.es/ [Accessed 18 Feb. 2018].
[6] McClure, S., Scambray, J., & Kurtz, G. (2010). Hackers 6: secretos y soluciones de seguridad en redes. México: McGraw-Hill Interamericana

error o debilidad en la configuración de los servidores de acceso de la empresa *Virgin Mobile.*

En las plataformas IaaS que existen en la actualidad donde los proveedores más predominantes en el mercado son AWS (*Amazon Web Services*), Azure de Microsoft y GCP de *Google*, se plantean formas diferentes formas y ambientes de control cada uno enfocado a su arquitectura, por ejemplo los controles de acceso de en la nube de AZURE[7] van enfocados al uso de proyectos que son grupos e intercalaciones de reglas que son transversales únicamente a este proyecto y no afecta a los demás proyectos o infraestructuras creadas además que su administración es más rígida pues todo se realizar por CLI (*Command Line Interface)*, mientras que en AWS las políticas de accesos pueden ser compartidas entre diferentes arquitecturas, en GCP se maneja un sistema de control de accesos similar al de AZURE[8] pero es un poco más amigable e intuitiva pues se opera por la GUI (*Graphical User Interface*). Por esta razón los servidores alojados en la plataforma de *Amazon Web Services* deben ser tomados desde el análisis y las practicas correspondientes a este proveedor.

[7] Ellis, G. (2015). Microsoft Azure IaaS essentials. Birmingham, UK: Packt Publishing

[8] Ellis, G. (2015). Microsoft Azure IaaS essentials. Birmingham, UK: Packt Publishing

5.1. MARCO TEÓRICO:

- *Cloud:* La definición del término “nube” o “Cloud” en Ingles se toma como la representación de un escenario intangible o muy basto que no era fácil de graficar o limitar con un diseño especifico, lo que posteriormente se tomó como representación de la Internet[9].

- *Cloud Computing:* Para este concepto se tomó la iniciativa desde la virtualización como evolución de esta misma ya que se basa en la capacidad de implementar un sistema Operativo sobre una infraestructura que se puede reutilizar para soportar múltiples ambientes.

- *Informática*: El desarrollo de las computadoras10 actuales se remontan a la creación del Abaco y a la constante necesidad de mejorar haciendo las cosas más rápidas y eficientes de allí se dieron múltiples saltos hasta llegar a los computadores u ordenadores actuales que facilitan la vida y dan más herramientas que día a día son explotadas y con las cuales se interactúa en cualquier momento del día, estos saltos se pueden resumir en:

[9] Disponible en Internet: Disponible en Internet: FayerWayer. (2018). El origen de: El Cómputo en la Nube. [online] Available at: https://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/ [Accessed 8 Feb. 2018].

[10] Disponible en Internet: Cad.com.mx. (2018). Generaciones de las Computadoras. [online] Available at: http://www.cad.com.mx/generaciones_de_las_computadoras.htm [Accessed 18 Feb. 2018].

- Primera generación o salto: Inicio en la década[11] de los 50´s siendo computadores muy grandes que tenían como principal falla o desventaja su tamaño y la excesiva creación de calor a causa de los tubos de vacío con los cuales operaban.

- Segunda generación o salto: a finales de la década[12] de los 50´s con el invento de los transistores lo que permitió la reducción de tamaño de los computadores y por ende su falla de producción calor excesivo llego a su final y el inicio de la creación de discos magnéticos que permitían almacenar información en forma digital.

- Tercera generación o salto: a finales de la década[13] de los 60´s con el invento de los *microchips* que era a acumulación de múltiples transistores que permitía ahorrar espacio y con el invento de la multiprogramación basada en la ejecución de múltiples tareas al tiempo.

- Cuarta generación o salto: a finales de la década[14] de los 70´s con el invento de los microprocesadores permitió que fuera más barato estos ordenadores y su crecimiento y expansión fuera mayor a nivel mundial

[11] Disponible en Internet: Disponible en Internet: FayerWayer. (2018). El origen de: El Cómputo en la Nube. [online] Available at: https://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/ [Accessed 8 Feb. 2018].
[12] Disponible en Internet: Disponible en Internet: FayerWayer. (2018). El origen de: El Cómputo en la Nube. [online] Available at: https://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/ [Accessed 8 Feb. 2018].
[13] Disponible en Internet: Disponible en Internet: FayerWayer. (2018). El origen de: El Cómputo en la Nube. [online] Available at: https://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/ [Accessed 8 Feb. 2018].
[14] Disponible en Internet: Disponible en Internet: FayerWayer. (2018). El origen de: El Cómputo en la Nube. [online] Available at: https://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/ [Accessed 8 Feb. 2018].

- Quinta generación o salto hasta la fecha presente: a inicios de la década[15] de los 80´s ha evolucionado hasta las redes neuronales, los primeros pasos de la inteligencia artificial por medio de chatbots o también llamados sistemas expertos.

- Seguridad Informática: Tuvo sus inicios en la década[16] de los 90´s con la aparición de ataques cibernéticos a empresas de telecomunicaciones que causaron pérdidas del grado de millones de dólares lo que causo que se colocara en el panorama la protección contra este tipo de ataques ya si evitar que se presentaran nuevamente, pero en los últimos años estos ataques se han ido modernizando y sofisticando lo que ha dado cabida a una separación de atacantes como los son:

- Internos[17]: Estos realizan las actividades ilegales desde dentro de la red empresarial, estos atacantes son o fueron empleados de las empresas que por venganza o por acuerdo con terceros y con el fin de lucrarse realizan ataques u operan como puertas traseras "*backdoors*" para que se puedan realizar estas operaciones ilícitas.

---

[15] Disponible en Internet: Disponible en Internet: FayerWayer. (2018). El origen de: El Cómputo en la Nube. [online] Available at: https://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/ [Accessed 8 Feb. 2018]./

[16] Disponible en Internet: Disponible en Internet: FayerWayer. (2018). El origen de: El Cómputo en la Nube. [online] Available at: https://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/ [Accessed 8 Feb. 2018]./

[17] Disponible en Internet: Ibid., Cad.com.mx. (2017). Generaciones de las Computadoras. [online] Available at: http://www.cad.com.mx/generaciones_de_las_computadoras.htm [Accessed 08 Nov. 2017].

- Externos[18]: estos realizan las actividades ilegales desde fuera de la red empresarial, para lo que requieren herramientas más sofisticadas y especializadas además de conocimientos avanzados que les permitan llegar a lograr sus fines ilícitos.

Hoy en día estos ataques se han especializado hasta el punto de búsqueda de estas fallas de seguridad en las infraestructuras que permitan accesos no autorizados y que conllevan a daños catastróficos como lo son:

- Computadores con daños que acarrean inoperatividad de estos como robo, cambio o daño permanente o parcial de la información.

- Implantación de malware que busca la ejecución de programas no autorizados o el acceso por medio de puertas traseras "*backdoors*".

- Robo de credenciales, *passwords* o suplantación de identidades.

- Seguridad en Internet: Habilidad para el uso de elementos que brindan protección al momento de usar Internet.

[18] Disponible en Internet: Ceac. (2017). Tipos de seguridad informática. [online] Available at: https://www.ceac.es/blog/tipos-de-seguridad-informatica [Accessed 08 Nov. 2017].

- Virus[19]: Programa ilegal que se instala en ordenadores sin el permiso de su propietario o por medio de engaños que realiza operaciones maliciosas.

- *Hackers:* Calificativo dado a personas con habilidades y conocimientos específicos que les permites evaluar el nivel de seguridad de un sistema sin realizar ataques o daños a la información alcanzada.

- *Crackers:* Calificativo dado a personas que con malas intenciones o con fines de lucro ingresan a sistemas de manera ilegal para realizar alguna operación sin la autorización del propietario o administrador de la información[20].

Tipos de seguridad:

- Pasiva: Es un tipo de seguridad[21] reactiva pues espera a que suceda el evento para recuperarse por medio de *back ups* o respaldos.

[19] Disponible en Internet: Iingen.unam.mx. (2017). Virus informáticos. [online] Available at: http://www.iingen.unam.mx/es-mx/Publicaciones/GacetaElectronica/Febrero2015/Paginas/Virusinformaticos.aspx [Accessed 09 Nov. 2017].
[20] Disponible en Internet: Mastermagazine.info. (2017). Cracker. [online] Available at: https://www.mastermagazine.info/termino/4472.php [Accessed 09 Nov. 2017].
[21] Disponible en Internet: Iingen.unam.mx. (2017). Virus informáticos. [online] Available at: http://www.iingen.unam.mx/es-mx/Publicaciones/GacetaElectronica/Febrero2015/Paginas/Virusinformaticos.aspx [Accessed 09 Nov. 2017].

- Activa: Se ejecuta[22] con el fin evitar que el suceso o ataque llegue a un término positivo para el atacante y que afecte la continuidad del negocio, o por el contrario busca minimizar este daño.

- Riesgo: Es la probabilidad[23] de que suceda un evento con consecuencias negativas para el ambiente, el individuo, etc.

- Amenaza: Posibilidad[24] de un hecho que puede suceder en un momento no predecible con una magnitud y duración predecible.

- Análisis de riesgos: Es una herramienta[25] que facilita la detección de riesgos que una empresa puede hacer frente y como tomar medidas contra estos.

- Matriz de evaluación riesgos: Es la organización[26] de la información relacionada con los riesgos que una entidad puede presentar y que genera como resultado una calificación a la cual se le aplican medidas de control y corrección.

---

[22] Disponible en Internet: Ibid., Iingen.unam.mx. (2017). Virus informáticos. [online] Available at: http://www.iingen.unam.mx/es-mx/Publicaciones/GacetaElectronica/Febrero2015/Paginas/Virusinformaticos.aspx [Accessed 09 Nov. 2017].

[23] Disponible en Internet: Epn.gov.co. (2018). 1.3. Riesgo, Amenaza y Vulnerabilidad. [online] Available at: http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_riesgo_amenaza_y_vulnerabilidad.html [Accessed 18 Feb. 2018].

[24] Disponible en Internet: Epn.gov.co. (2018). 1.3. Riesgo, Amenaza y Vulnerabilidad. [online] Available at: http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_riesgo_amenaza_y_vulnerabilidad.html [Accessed 18 Feb. 2018].

[25] Disponible en Internet: Huerta, A. (2018). Introducción al análisis de riesgos - Metodologías (I) - Security Art Work. [online] Security Art Work. Available at: https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/ [Accessed 6 Apr. 2018].

[26] Disponible en Internet: Sigweb.cl. (2018). Sigweb. [online] Available at: http://www.sigweb.cl/informacion-tecnica/matrices-de-riesgos/ [Accessed 9 Mar. 2018].

- Matriz de clasificación de riesgos: Es una herramienta[27] usada para clasificar los riesgos según su impacto y el riesgo existente detectado.

- Norma ISO 27001[28]: Norma internacional que cubre el análisis y tratamiento de la seguridad de la información como elemento de control que se enfoca en una serie de ítems que buscan mejorar los niveles de seguridad frente a riesgos en un ambiente corporativo, se complementa con la Norma ISO 27002.

- Norma ISO 27002[29]: Norma internacional compuesta por 14 capítulos y 144 componentes que dan como resultado una serie de recomendaciones de buenas prácticas que se integran con el análisis y tratamiento de riesgos de la norma ISO 27001.

5.2. MARCO CONCEPTUAL

Este proyecto se ejecutó a nivel nacional con mayor exactitud, sobre los servidores de la empresa *Virgin Mobile* bajo su aprobación, con un alcance a nivel nacional pues lo servidores son accedidos desde múltiples lugares del territorio nacional en especial

[27] Disponible en Internet: Sigweb.cl. (2018). *Sigweb.* [online] Available at: http://www.sigweb.cl/informacion-tecnica/matrices-de-riesgos [Accessed 6 Apr. 2018].
[28] Disponible en Intenet: Anon, (2018). [online] Available at: http://www.iso27000.es/ [Accessed 18 Feb. 2018].
[29] Disponible en Intenet: Anon, (2018). [online] Available at: http://www.iso27000.es/ [Accessed 18 Feb. 2018].

los servidores de desarrollo por parte de empresas contratistas o terceros con el fin de desarrollar o probar mejoras a los servicios que se encuentran en el ambiente de desarrollo y al cual no es posible la realización de pruebas en los servidores que se encuentran en el ambiente de producción. Pero al ser un ambiente exógeno a las instalaciones de la compañía se debe asegurar que las medidas de seguridad sean confiables tanto en el ambiente procedimental de la entrega de accesos y los niveles de privilegios que tengas dichos accesos según los roles de los empleados[30].

Esta empresa se encuentra en operación sobre la modalidad de pago por demanda de la infraestructura bajo la modalidad IaaS (*Infrastructure as a Service*) con el servicio contratado con el proveedor *Amazon Web Services*, por ende, se debe contar con cambios en las configuraciones y buenas prácticas en seguridad que son diferentes a cada una de las nubes o proveedores de este modelo de negocio y que proveen esta solución a nivel de infraestructura[31], para preservar la seguridad de los servidores accedidos por los empleados donde se soportan plataformas de los ambientes de operación de Producción, Desarrollo y Pruebas de la empresa *Virgin Mobile* Colombia. Debemos recordar que unas buenas prácticas llevaran a mejorar el nivel de seguridad en los controles de acceso a los servidores de la compañía, además de asegurar que solo los usuarios que requieren tener los accesos necesarios los tengan, estas buenas prácticas serán soportadas sobre el uso de la

30 Disponible en Internet : Marzoasesores.es. (2018). Medidas de seguridad en el Cloud Computing |. [online] Available at: http://www.marzoasesores.es/medidas-de-seguridad-en-el-cloud-computing/ [Accessed 18 May 2018].

31 Disponible en Internet: Docs.microsoft.com. (2018). *Procedimientos recomendados de seguridad de la red de Azure*. [online] Available at: https://docs.microsoft.com/es-es/azure/security/azure-security-network-security-best-practices [Accessed 14 Jun. 2018].

norma ISO 27002[32] la cual brinda una serie de recomendaciones apoyadas en la norma ISO 27001

Este proyecto tuvo un tiempo de 4 meses y fue llevado en los servidores de desarrollo y producción de la empresa *Virgin Mobile,* el tiempo total de estudio estuvo comprendido en el primer semestre del año 2018, para lograr tener visibilidad de los riesgos latentes, se utilizó un análisis de riesgos que fue compuesto por una matriz de evaluación de riesgos y el análisis de la calificación que fue tomado desde una matriz de clasificación de riesgos, lo cual nos llevó a tomar medidas que protejan la integridad de los servidores y aumentar el nivel de seguridad de la empresa en *Virgin Mobile.*

[32] Disponible en Intenet: Anon, (2018). [online] Available at: http://www.iso27000.es/ [Accessed 18 Feb. 2018].

6. MARCO METODOLOGICO

En la figura 1 se observa cual fue el flujo de los ítems sobre los cuales se soportan los pasos a seguir durante la elaboración de este documento dando una introducción a los 9 componentes.

Figura 1 Flujo de Metodología

Fuente: autor

6.1. INVESTIGACIÓN DE CAMPO

Esta fase estuvo basada en encuestas de preguntas con respuestas cerradas que se realizaron a los administradores de plataformas para reunir la información del estado inicial y hallar las falencias existentes de los servidores y así vislumbrar en un inicio el nivel de seguridad durante la primera fase de este proyecto.

6.2. INVESTIGACIÓN DOCUMENTAL

Se realizó la revisión de los procedimientos existentes para evaluar el grado de carencia en cuanto a los permisos y roles de acceso que deben tener los empleados de la empresa *Virgin Mobile*.

6.3. TRATAMIENTO CUALITATIVO

Con el cual se buscó realizar un modelo o evaluación previa que evidencio las fallas que fueron tratas y usadas como base para la realización de una primera propuesta con las correcciones sugeridas que serán evaluada por personal aprobador de *Virgin Mobile*.

6.4. ANALISIS DE ESTADO ACTUAL

Se procedió a realizar una revisión del estado inicial de seguridad en cuanto los controles de acceso a los servidores, enfocados a como los empleados consiguen sus credenciales de acceso y una vez obtenidos que registros quedan de sus entregas.

6.5. ANALISIS DE LA INFORMACION RECOLECTADA

Luego de la recolección de la información por medio del análisis se buscó encontrar las brechas de seguridad que representaban un riesgo en cuanto a la entrega de accesos a los empleados, además de la falta de personalización o aseguramiento en las configuraciones de acceso a los servidores.

6.6. ANALISIS DE LOS RIESGOS HALLADOS

Se procedió por medio del análisis de los riegos hallados a la implementación de una seria de medidas que mitiguen el impacto frente a estas brechas de seguridad.

6.7. CREACION DE DOCUMENTOS DE SOPORTE

Se creó un par de formatos para la solicitud y la entrega de credenciales que tendrán como objetivo esclarecer quienes y que accesos poseen a los servidores en los ambientes de producción, pruebas y desarrollo.

6.8. CREACION DE PROCEDIMIENTO DE CAMBIOS EN LOS SERVIDORES

Se creó un procedimiento que debe ser ejecutado por los administradores de los servidores con el fin de aumentar la seguridad en los accesos de los empleados y eliminando las configuraciones estándar en los servidores que son de conocimiento público.

7. ESTABLECER UN ANALISIS DEL GRADO DE SEGURIDAD ACTUAL

Se realizó una encuesta para conocer el grado de seguridad percibido por los usuarios con el fin de buscar posibles vulnerabilidades que afecten la operación normal de los servidores o brechas de seguridad explotables por atacantes malintencionados y evidenciar los orígenes de las credenciales que se emplean en el día a día, los datos para realizar esta encuesta fueron:

- Población de 12 personas integrantes del área de Tecnología.
- Desarrolladores y administradores de los servidores que sirven como plataformas de desarrollo y producción de la empresa *Virgin Mobile.*

Se realizó una revisión previa del estado de configuración en los ambientes de producción, desarrollo y pruebas de los servidores encontrando que todos usan el mismo puerto y las mismas configuraciones de acceso, el cual es el estándar entregado al momento de la creación de un servidor en la plataforma del proveedor *Amazon Web Services.*

7.1. ENCUESTA

Se busca realizar una encuesta básica enfocada a las personas que utilizan los servidores desde los roles de administradores y programadores para evaluar su grado de seguridad y evidenciar las falencias en cuanto a los procedimientos existentes por medio de una encuesta.

A continuación, se anexan el formato de la encuesta realizada:

Tabla 1 Encuesta

2.1. Nombre completo de la Empresa u Organización:
2.2. Ubicación (Localidad – Departamento):
2.3. Nombre de la persona encuestada:
2.4. Cuál es su antigüedad en la empresa? Marque con una x una de las siguientes categorías:
( ) 1. Más de 5 años ( ) 2. Más de 4 años ( ) 3. Más de 3 años ( ) 4. Más de 2 años ( ) 5. Más de 1 año ( ) 6. Más de 6 meses

Tabla 1 (Continuación)

3. ¿Existe evidencia de la entrega de sus credenciales de acceso al momento de su ingreso a la empresa?	Marque con una x una de las siguientes categorías:
( ) 1. Si ( ) 2. No	
4. ¿Realiza algún cambio periódico de sus contraseñas?	
( ) 1. Si ( ) 2. No	
4.1. Si su respuesta fue afirmativa, complete las siguientes opciones:	
4.1.1. ¿Ud Realiza el cambio con que periodicidad?:	
( ) 1. Cada semana ( ) 2. Cada 2 semanas ( ) 3. Cada mes ( ) 4. Cada 2 meses ( ) 5. Cada 6 meses	
4.2. ¿Existe alguna medida que le exija hace el cambio de contraseñas?:	
( ) 1. Si (x) 2. No	
4.2.1. ¿Para realizar su trabajo requiere acceso físico al datacenter?:	
( ) 1. Si ( ) 2. No	

Tabla 1 (Continuación)

5. Cuando requiere un acceso nuevo a quien lo solicita?
( ) 1. Compañero de trabajo ( ) 2. Jefe directo
5.1. ¿Queda algún registro de esta entrega de credenciales?
( ) 1. Si ( ) 2. No
5.2. Sabe si existe algún formato para la solicitud de credenciales y accesos?
( ) 1. Si ( ) 2. No
5.3. ¿Sabe si existe alguna política de seguridad?
( ) 1. Si ( ) 2. No

Tabla 1 (Continuación)

6. ¿Existe algún control de acceso físico?
( ) 1. Si ( ) 2. No

7.2. CONFIGURACION GENERAL DE LOS SERVIDORES

Luego de la creación de los servidores se constató que la configuración de acceso fue:

- Acceso por el puerto 22 el cual es estándar para todos los servidores creados empleando el protocolo SSH.

- Las claves de acceso para los usuarios *root* es la misma para todos los servidores, pues se emplea llave genérica.

- Se cuenta con un tiempo de gracia de 60 segundos o "*LoginGraceTime*" para que el usuario digite sus credenciales.

- Se cuenta con intentos ilimitados o “*MaxAuthTries*” al momento de fallar la contraseña ingresada.

- Puede usar máximo 10 sesiones abiertas o “*MaxStartups*” en el servidor en simultáneo.

- Todas las IP’s tiene autorización a conexión por medio del parámetro “*AllowUsers*”

7.3. ANALISIS DE LA ENCUESTA

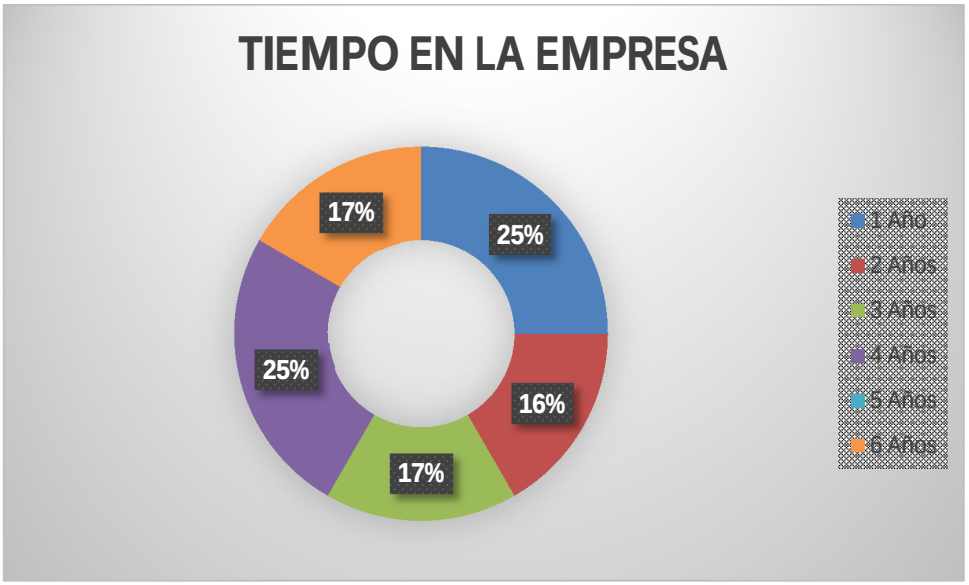
A continuación, se analizó la información recolectada para evaluar según las respuestas de las encuestas donde se encuentran las fallas más generales y proceder a la generación de medidas correctivas.

- **¿Cuál es su antigüedad en la empresa?:** Las personas encuestadas respondieron que cuentan con una antigüedad en la empresa con los porcentajes presentados a continuación y observados en la Figura 2:

    - El 25 % es mayor al quinto año.
    - El 16.6 % es mayor al cuarto año.

- El 16.6 % es mayor al tercer año.
- El 25 % es mayor al segundo año.
- El 16.6 % es mayor al sexto mes.

Figura 2 Tiempo en la empresa



Fuente: el autor

- **¿Existe evidencia de la entrega de sus credenciales de acceso al momento de su ingreso a la empresa?:** Las personas encuestadas respondieron sobre la evidencia de entrega de sus credenciales con los porcentajes presentados a continuación observados en la figura 3:

  - No: 100%
  - Si: 0 %

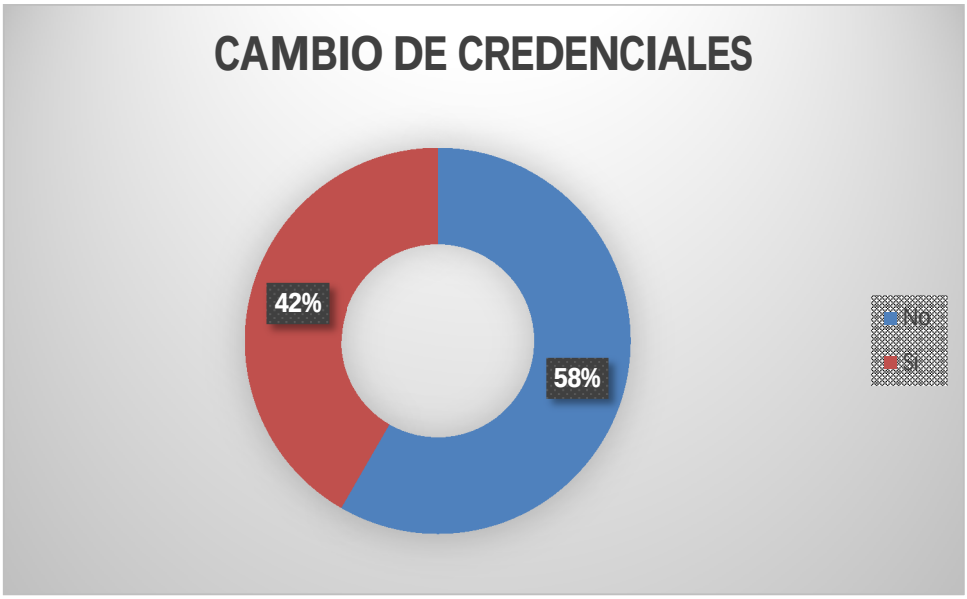
Figura 3 Evidencia de entrega de credenciales

Fuente: el autor

- **¿Realiza algún cambio periódico de sus contraseñas?:** Las personas encuestadas respondieron que realizan los cambios con una regularidad observados en la figura 4:

  - No: 58,3%
  - Si: 41,7 %

Figura 4 Cambio de credenciales

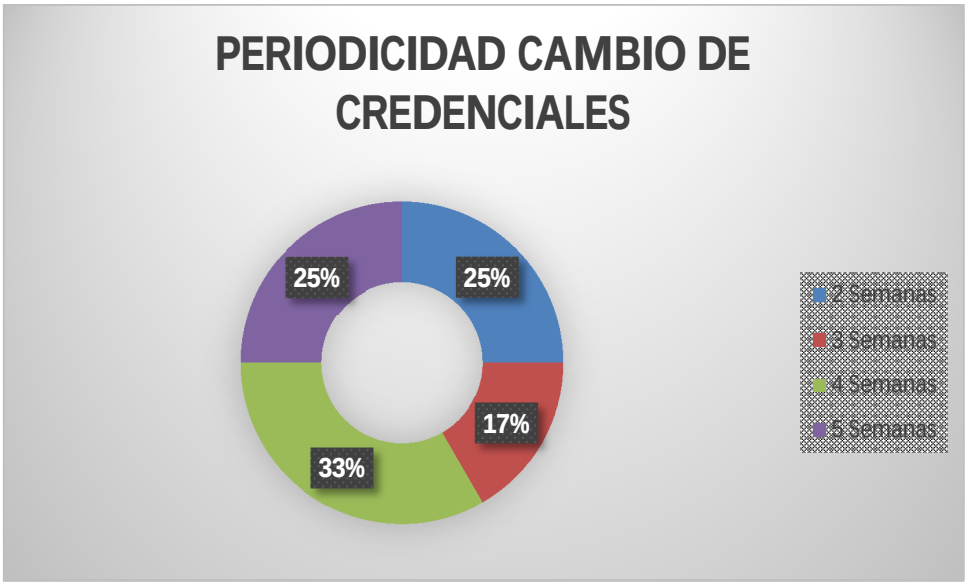


Fuente: el autor

1. Si la respuesta fue “Si” en la pregunta anterior:

- **¿Usted Realiza el cambio con que periodicidad?:** Las personas encuestadas respondieron con qué frecuencia realizan el cambio de credenciales y se observan en la figura 5:
  - El 25 % cada 2 semanas
  - El 17 % cada 3 semanas
  - El 33 % cada 4 semanas
  - El 25 % cada 5 semanas

Figura 5 Periodicidad Cambio de credenciales

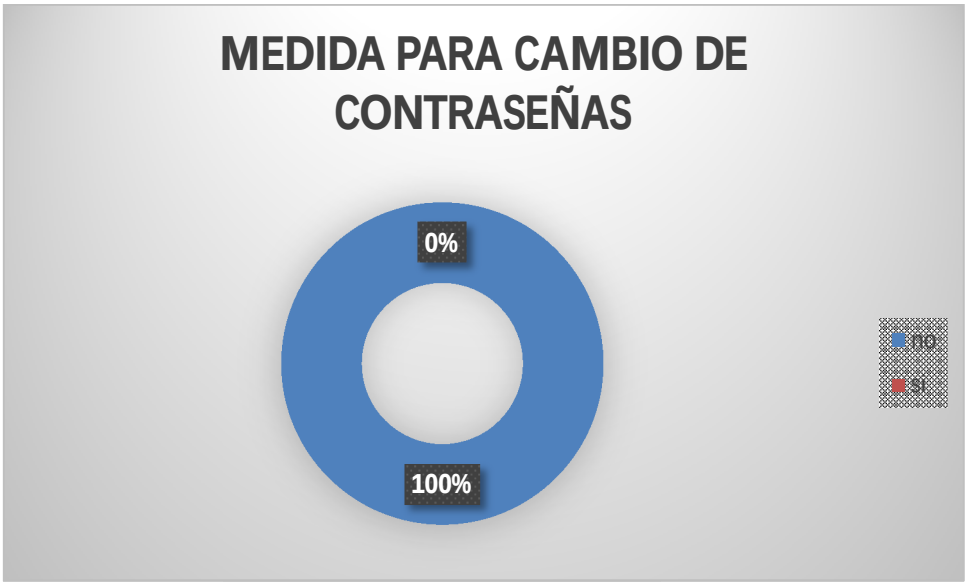


Fuente: el autor

- **¿Existe alguna medida que le exija hace el cambio de contraseñas?:** Las personas encuestadas respondieron si les han exigido realizar algún cambio en sus credenciales y se observa en la figura 6:

  - No: 100%
  - Si: 0 %

Figura 6 Medida para cambio de contraseñas

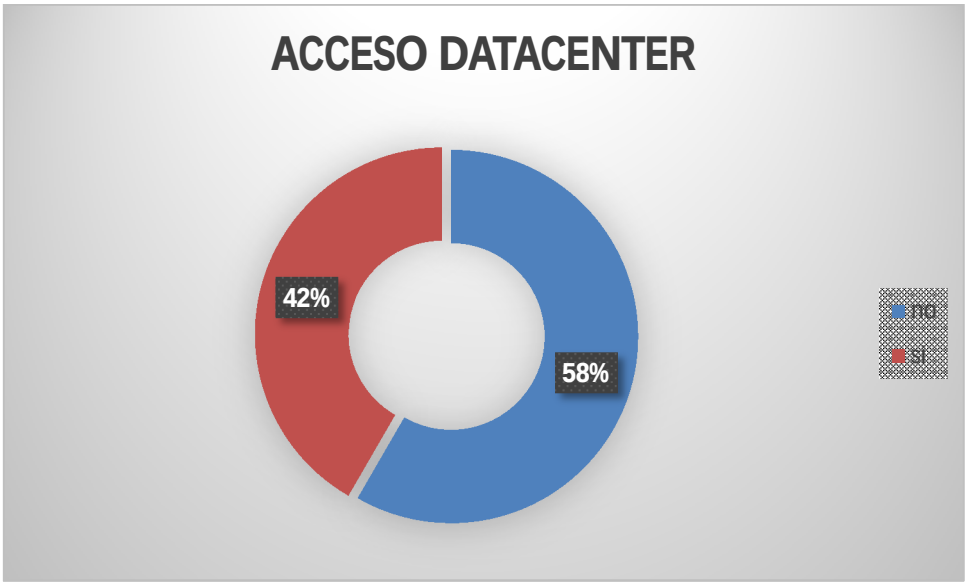


Fuente: el autor

- **¿Para realizar su trabajo requiere acceso físico al *datacenter*?:** Las personas encuestadas respondieron que para realizar sus labores requieren acceso físico al *datacenter*, esta información se puede observar en la figura 7:

  - No: 58.3%
  - Si: 41.6 %

Figura 7 Medida para acceso al *datacenter*

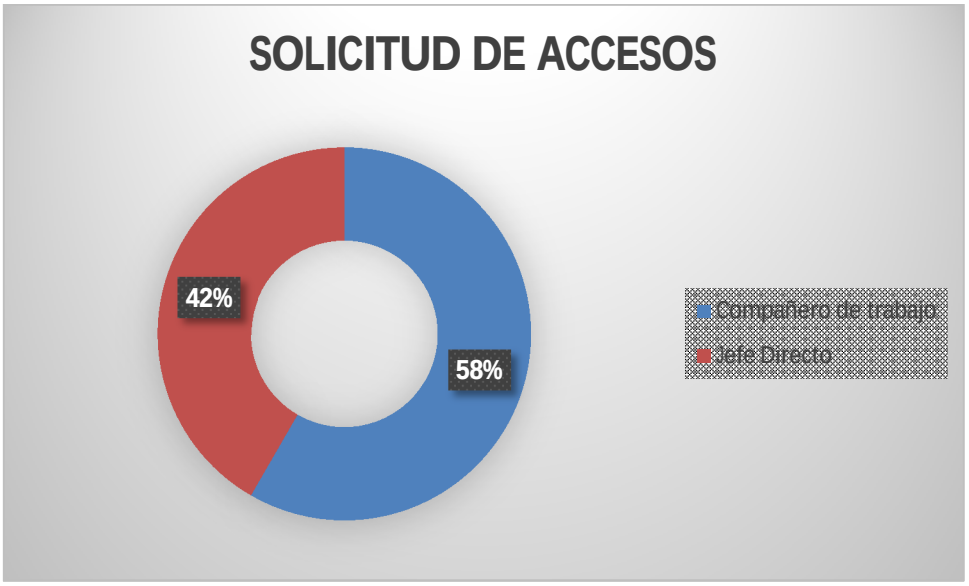


Fuente: el autor

- **¿Cuándo requiere un acceso nuevo a quien lo solicita?:** Las personas encuestadas respondieron que debían solicitar los accesos a compañeros de trabajo y jefe en diferentes porcentajes que son observados en la figura 8:

    - Compañero de trabajo: 58.3%
    - Jefe directo: 41.6%

Figura 8 Solicitud de Accesos

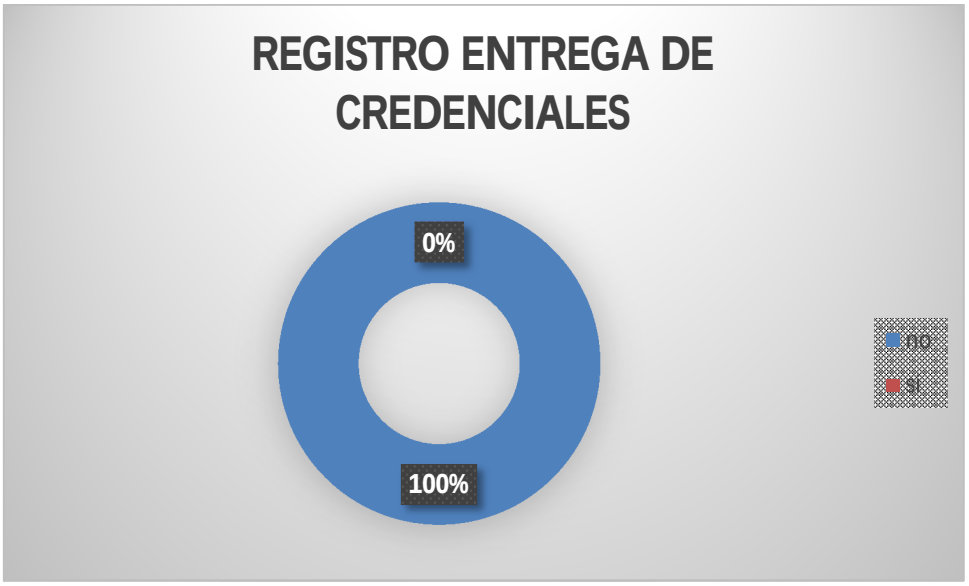


Fuente: el autor

- **¿Queda algún registro de esta entrega de credenciales?:** Las personas encuestadas indicaron que no quedan registros físicos de la entrega de las credenciales como se observa en figura 9:

  - No: 100%
  - Si: 0 %

Figura 9 Registro entrega de credenciales

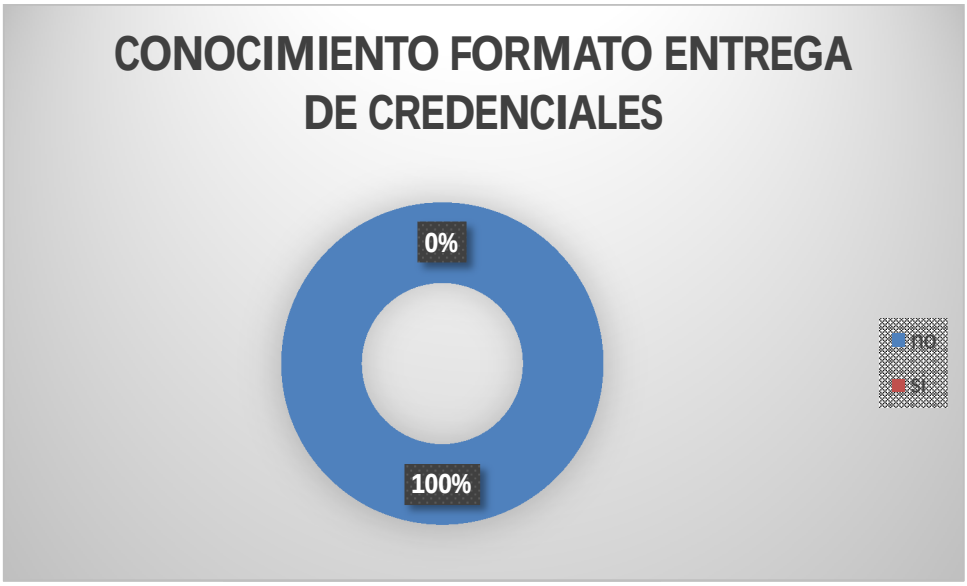


Fuente: el autor

- **¿Sabe si existe algún formato para la solicitud de credenciales y accesos?:** Las personas encuestadas indicaron que no conocen ningún formato o procedimientos para solicitar nuevos accesos como se observa en figura 10:

  - No: 100%
  - Si: 0 %

Figura 10 Conocimiento del formato entrega de credenciales

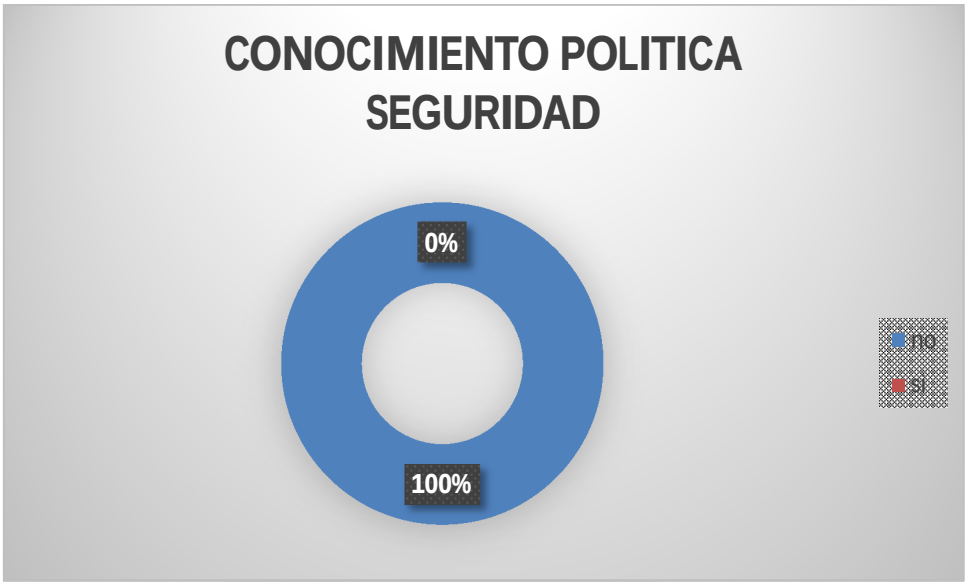


Fuente: el autor

- **¿Sabe si existe alguna política de seguridad?:** Las personas encuestadas indicaron que no conocen ninguna política de seguridad como se observa en la figura 11:

  - No: 100%
  - Si: 0 %

Figura 11 Conocimiento de la política de seguridad

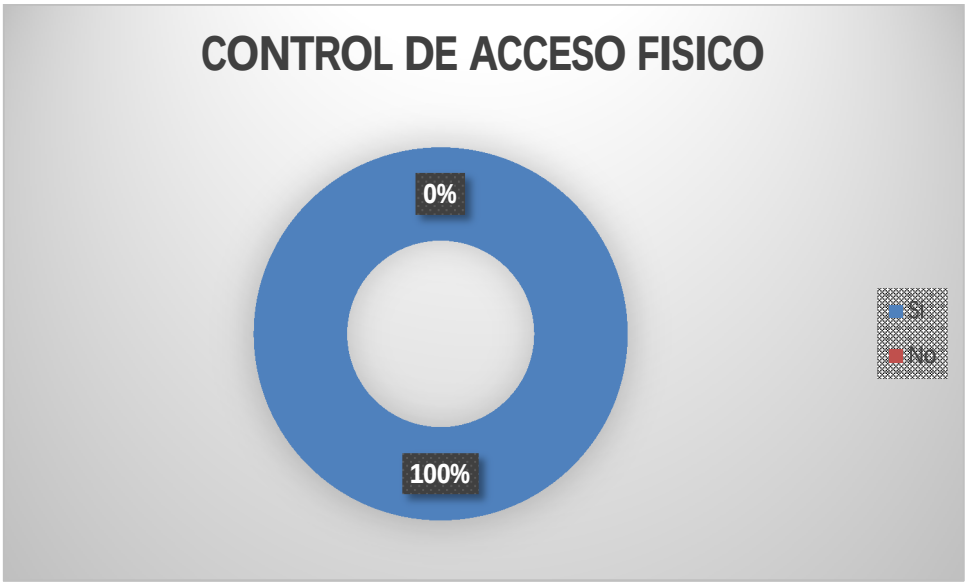


Fuente: el autor

- **¿Existe algún control de acceso físico?:** Las personas encuestadas indicaron que los accesos físicos si son controlados como se observa en la figura 12:

  - No: 0%
  - Si: 100 %

Figura 12 Control de acceso físico



Fuente: el autor

Luego de revisar estas respuestas podemos determinar 2 grandes hallazgos que son:

- La norma ISO 27001 en su numeral A.11[33] nos habla del control de accesos donde hace mención que solo los empleados deben tener privilegios necesarios para realizar su trabajo pero durante este análisis se observa que la mayoría de personas son antigua en la empresa con un tiempo mayor a 3, 4 y 5 años, que no se manejan registros de ninguna clase en las entregas de credenciales, que más de la mayoría no suele tener la precaución de cambiar

[33] Disponible en: Google.com. (2018). [online] Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjDpKbU4qnbAhXLuFkKHU8GDYsQFggnMAA&url=http%3A%2F%2Fwww.iso27000.es%2Fdownload%2FISO-27001_Los-controles_Parte_II.pdf&usg=AOvVaw0VinIOt8_dcGsGaxsBSVZe [Accessed 26 Mar. 2018].

sus contraseñas y quienes si lo hacen lo hacen en tiempo prudentes, no hay medidas de control q exijan los cambios de contraseñas periódicos, no hay una persona o administrador que entregue las credenciales de acceso de forma unificada, no hay formatos divulgados para la solicitud de accesos nuevos, no existe una política de seguridad vigente pero se resalta que existen controles de accesos físicos y en operación.

- Se evidencia una brecha de seguridad muy grande al no tener registro de control en las entregas de credenciales de acceso a los servidores de la empresa *Virgin Mobile*, por ende, es necesario plantear formatos de solicitud y entregas que deben ser almacenado en físico y digital con el fin de asegurar su disponibilidad como evidencia de entrega, la norma ISO 27001 nos habla en su numeral A.11 que se debe regular una administración de acceso de los usuarios apoyado en un procedimiento que garantice el registro y revocación de los privilegios obtenidos.[34]

[34] Disponible en: Google.com. (2018). [online] Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjDpKbU4qnbAhXLuFkKHU8GDYsQFggnMAA&url=http%3A%2F%2Fwww.iso27000.es%2Fdownload%2FISO-27001_Los-controles_Parte_II.pdf&usg=AOvVaw0VinIOt8_dcGsGaxsBSVZe [Accessed 26 Mar. 2018].

8. ANALISIS Y EVALUACION DE RIESGOS

Luego de la realización de la encuesta su tabulación y posterior análisis se determinaron una serie de riesgos que al ser cotejados con la norma ISO 27001 e ISO 27002 donde se dará comienzo con la visualización y presentación de las vulnerabilidades encontradas por medio una matriz del análisis y la evaluación de los riesgos detectados:

Se interpretó parámetros como:

- Probabilidad**:** Donde se tiene una escala de 1 a 4, siendo 1 muy baja probabilidad de presentarse el evento y 4 la probabilidad más alta.

- Impacto: Donde se tiene una escala de 1 a 4, siendo 1 el impacto más bajo y 4 el impacto más alto sobre los activos o servidores de la empresa *Virgin Mobile* y su respectiva operación normal.

- Calculo del riesgo total: Se toma los valores de la probabilidad y el impacto y son multiplicados para lograr un valor del riesgo en la escala de 1 a 16.

Tabla 2 Matriz evaluación del riesgo

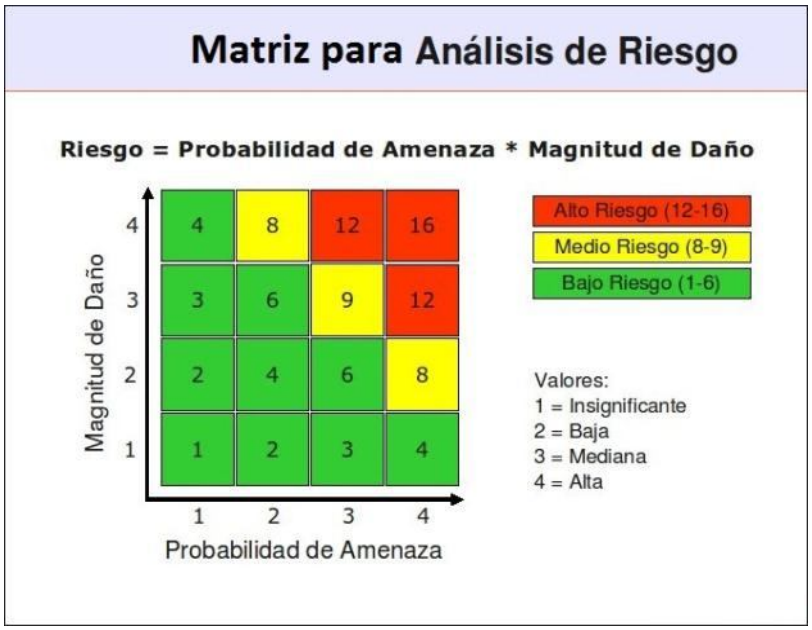
Campo	Ítem	Vulnerabilidades	Amenaza	Riesgo	Probabilidad				Impacto				Valoración Total del Riesgo
					1	2	3	4	1	2	3	4	
Acceso Servidores	**1**	No existe un registro o evidencia de la entrega de credenciales de acceso a los empleados	Ingreso no autorizado por parte de personal no autorizado o con elevación de privilegios.	Manipulación de la información sensible sin autorización.				**X**				**X**	**16**
	2	No existe un procedimiento de solicitud de credenciales que sea soportado por una validación por parte de	Uso inapropiado de los accesos entregados.	Perdida o daño de la información.			**X**					**X**	**12**

		algún cargo empresarial con rol de aprobador.											
	3	No existe un método que exija el cambio de las contraseñas a los empleados.	Robo de contraseñas.	Suplantación o robo de identidades con fines maliciosos.			**X**				**X**		**6**
	4	No se controlan los cambios necesarios para aumentar la seguridad de acceso a los servidores.	Accesos no autorizados por atacantes con fines maliciosos.	Perdida o daño de la información.			**X**				**X**		**9**

8.1. MATRIZ DE CLASIFICACION DE RIESGOS

La matriz de calificación de riesgos se emplea para clasificar y determinar el nivel de tratamiento que se debe dar a cada una de las vulnerabilidades detectadas y analizadas en el punto anterior dándoles un enfoque hacia la norma ISO 27002 la cual tiene como función las buenas prácticas en el ámbito de la seguridad de la información y los pasos que la componen son:

Figura 13 Matriz para análisis de riesgo

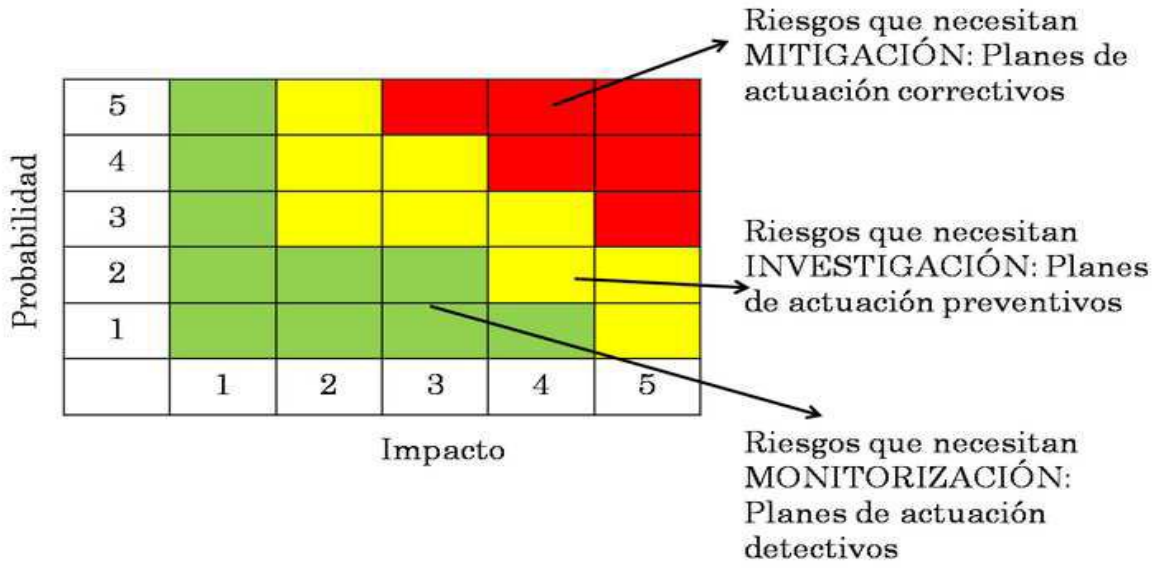


Fuente: ERB, M. (2008). *Gestión de Riesgo en la Seguridad Informática*

La evaluación se llevó a cabo teniendo en cuenta la magnitud del daño contra la probabilidad de que llegara a suceder el incidente, aplicado a cada uno de los numerales que se encuentran en la tabla 2.

En la figura 13 se observa el mapa de calor de la matriz de riesgos donde se calcula el riesgo dependiendo de la probabilidad que suceda un evento por la magnitud del del daño.

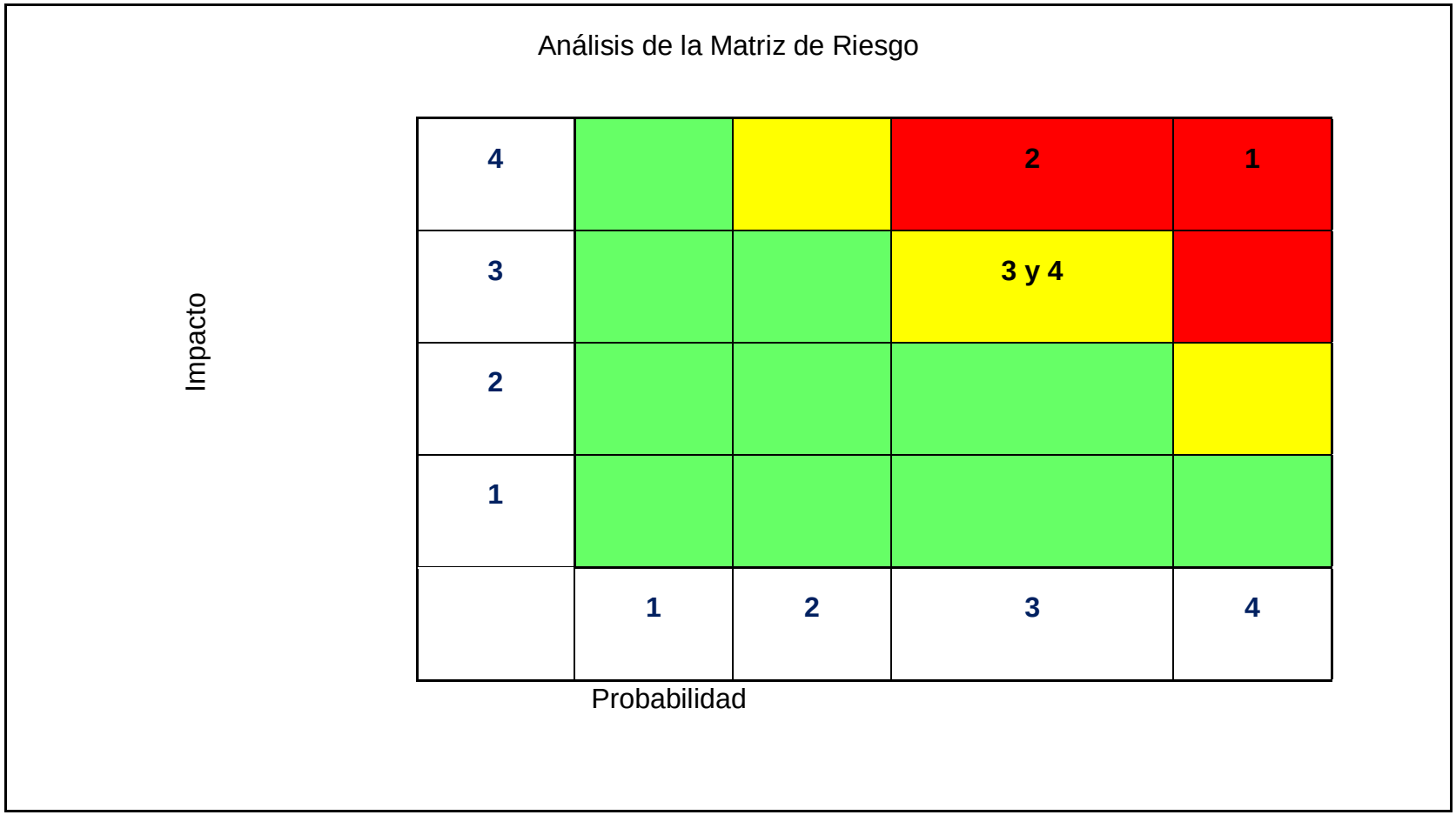
Figura 14 Interpretación de la matriz para análisis de riesgo



Fuente: ERB, M. (2008). Gestión de Riesgo en la Seguridad Informática.

En la figura 14 se observa el mapa de calor de la gestión que se hará de riesgos donde se puede interpretar los valores hallados según el método de control ya se por monitoreo, mitigación o si requiere investigación.

Figura 15 Matriz análisis del riesgo



Fuente: autor

Luego de evaluar los riesgos en la figura 14, se colocan en cada tabla los ítems de la figura 15, es posible realizar una segmentación según su clasificación como se verá en la tabla 3 :

Tabla 3 Clasificación del riesgo

Ítem	Riesgo	Clasificación del riesgo
3	Suplantación o robo de identidades con fines maliciosos.	Riesgos que necesitan Investigación: Planes de actuación Preventivos. Mejorar condición.
4	Perdida o daño de la información.	
1	Manipulación de la información sensible sin autorización..	Riesgos que necesitan Mitigación: Planes de actuación correctivos, Gestión Urgente
2	Perdida o daño de la información.	

Fuente: autor

8.2. TRATAMIENTO DE RIESGOS

Para la realización del tratamiento de riesgos, se empleó la Norma ISO 27002, la cual nos referencia y nos da las pautas para las buenas prácticas y el tratamiento de riesgos en seguridad de la información y se integra con la Norma ISO 2700135 enfocándose en una seria de ítems los cuales son 14 capítulos que a su vez están compuestos por 114 controles, que en su esencia no es necesario cubriros todos sino dar énfasis a los que sea aplicados a la organización y al análisis de riesgo encontrado.

Para iniciar con el tratamiento de riesgos se realizó una indagación en búsqueda de si existía algún tipo de documento oficial o medio regulado y auditable que funcione como soporte o evidencia para la solicitud y entrega de credenciales y/o accesos en la empresa Virgin Mobile y que nos diera un control a estos riesgos, lo cual no se encontró ningún documento en el área de Tecnología que lo respaldara como lo exige la norma ISO 27001, por este motivo se plantearan una serie de medidas ejemplificadas en la tabla 16:

[35] Disponible en Intenet: Anon, (2018). [online] Available at: http://www.iso27000.es/ [Accessed 18 Feb. 2018].

Tabla 4 Tratamiento de riesgos

Ítem	Riesgo	Clasificación del riesgo	Control de Mitigación de Riesgo	Detalle del control – técnica y mecanismo	Justificación- referente, quien lo implementa, cuando, y costo
3	Suplantación o robo de identidades con fines maliciosos.	**Riesgos que necesitan Investigación: Planes de actuación Preventivos. Mejorar condición.**	**Dominio: 9**. Control de Accesos. **Objetivo de Control: 9.4: Control** de acceso a sistemas y aplicaciones. **Control: 9.4.3:** Gestión de Contraseña de usuario.	Implementación de políticas de cambios de contraseñas por medio de GPO (*Group Policy Objet)* por el Directorio Activo para forzar el cambio de contraseñas cada 2 semanas en los computadores locales.	De esta forma se aumenta el nivel de seguridad al minimizar el riesgo de suplantación de identidad además de protección ante equipos desatendidos y el atacante pueda emplear las credenciales robadas, será implementado por el administrador del sistema y no

Ítem	Riesgo	Clasificación del riesgo	Control de Mitigación de Riesgo	Detalle del control – técnica y mecanismo	Justificación- referente, quien lo implementa, cuando, y costo
					presentara ningún costo.
4	Perdida o daño de la información.		**Dominio: 12**. Seguridad en la Operativa.	Cambios en la configuración de seguridad de accesos en los servidores por medio un procedimiento aprobado por las directivas de Tecnología.	Se desarrolló un procedimiento que dicta el paso a paso para generar estos cambios en la configuración, que deben ser realizados por los administradores de los servidores lo cual no genera ningún costo adicional.
			Objetivo de Control:12.1: Responsabilidad y procedimientos en la operación		
			Control: 12.1.2: Gestión de Cambios		

Ítem	Riesgo	Clasificación del riesgo	Control de Mitigación de Riesgo	Detalle del control – técnica y mecanismo	Justificación- referente, quien lo implementa, cuando, y costo
1	Manipulación de la información sensible sin autorización.	**Riesgos que necesitan Mitigación: Planes de actuación correctivos, Gestión Urgente**	**Dominio: 9**. Control de Accesos. **Objetivo de Control:9.1:** Requisitos de negocio para el control de accesos **Control: 9.1.1:** Política de Control de Accesos	Se plantea un procedimiento de solicitud y entrega de credenciales ya aprobados.	La puesta en práctica del procedimiento generará transparencia en la entrega, solicitud y aprobación de las credenciales asignadas para los usuarios que las requieran por parte de los administradores de los servidores sin costos adicionales para la empresa.

Ítem	Riesgo	Clasificación del riesgo	Control de Mitigación de Riesgo	Detalle del control – técnica y mecanismo	Justificación- referente, quien lo implementa, cuando, y costo
2	Perdida o daño de la información.		**Dominio: 12**. Seguridad en la Operativa. **Objetivo de Control:12.1:** Responsabilidad y procedimientos en la operación **Control: 12.1.2:** Gestión de Cambios	Se plantea un par de formatos para solicitud y entrega de credenciales que ya fueron aprobados por las directivas del are de tecnología.	Se desarrollaron los formatos de solicitud y entrega de credenciales que garantizan un seguimiento y trazabilidad de las entregas de las credenciales dando un soporte que fueron aprobados y entregados a su usuario final, estos formatos serán desarrollados por el administrador

Ítem	Riesgo	Clasificación del riesgo	Control de Mitigación de Riesgo	Detalle del control – técnica y mecanismo	Justificación- referente, quien lo implementa, cuando, y costo
					del sistema sin costo alguno.

9. DEFINICION DE LOS PROCEDIMIENTOS

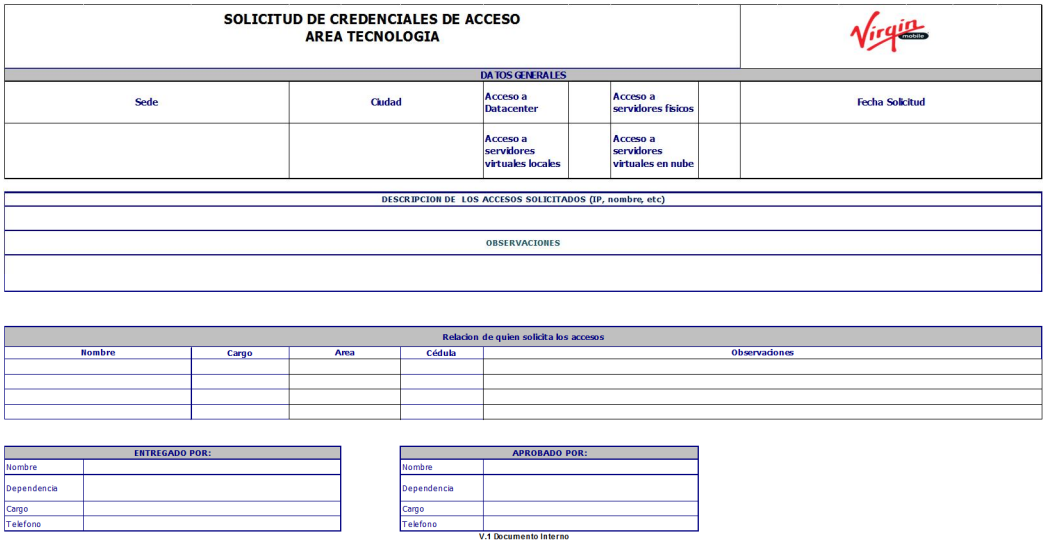
Como se observó en los análisis previos se determinó el desarrollo de los 2 procedimientos uno para la solicitud y entrega de credenciales otro para los cambios de configuración de seguridad en los servidores además de un par de formatos, uno donde se plasma la solicitud y otro para la entrega de credenciales.

El formato de solicitud de credenciales se creó con el fin de mitigar el riesgo encontrado en el ítem 1 de la figura16 (Manipulación de la información sensible sin autorización.) y el ítem 2 de la figura 16 (Pérdida o daño de la información).

9.1. FORMATO DE SOLICITUD DE CREDENCIALES

Este formato de solicitud debe ir aprobado por el jefe directo quien da la aprobación para continuar con este requerimiento:

Figura 16 Formato Solicitud de Accesos



SOLICITUD DE CREDENCIALES DE ACCESO
AREA TECNOLOGIA

DATOS GENERALES						
Sede	Ciudad	Acceso a Datacenter		Acceso a servidores físicos		Fecha Solicitud
		Acceso a servidores virtuales locales		Acceso a servidores virtuales en nube		

DESCRIPCION DE LOS ACCESOS SOLICITADOS (IP, nombre, etc)
OBSERVACIONES

Relacion de quien solicita los accesos				
Nombre	Cargo	Area	Cédula	Observaciones

ENTREGADO POR:	
Nombre	
Dependencia	
Cargo	
Telefono	

APROBADO POR:	
Nombre	
Dependencia	
Cargo	
Telefono	

V.1 Documento Interno

9.2. FORMATO DE ENTREGA DE CREDENCIALES

Se acordó que solo serán entregadas 2 credenciales por formato para rigurosidad y control en la asignación de los permisos, por ende, el formato de entrega de accesos quedo así:

Figura 17 Formato Entrega de Accesos

ENTREGA DE CREDENCIALES DE ACCESO
AREA TECNOLOGIA

DATOS GENERALES						
Sede	Ciudad	Acceso a Datacenter		Acceso a servidores fisicos		Fecha Entrega
		Acceso a servidores virtuales locales		Acceso a servidores virtuales en nube		

DESCRIPCION DE LOS ACCESOS SOLICITADOS (IP, nombre, etc)

Relacion de quien solicita los accesos				
Nombre	Cargo	Area	Cédula	Observaciones

Credenciales Entregadas	
Acceso 1:	Acceso 2:

ENTREGADO POR:	
Nombre	
Dependencia	
Cargo	
Telefono	

APROBADO POR:	
Nombre	
Dependencia	
Cargo	
Telefono	

V.1 Documento Interno

10. CAMBIOS PLANTEADOS EN LOS SERVIDORES

Se recomienda realizar cambios en los accesos a los servidores en la nube como lo son:

- Cambio del puerto 22 empleado por el protocolo SSH por *default* y usar un puerto más alto para asegurar que solo las personas notificadas puedan tener el acceso al servidor. Figura 18

Figura 18 Puertos

- Implementar el uso de claves cifradas para el acceso acompañadas por palabras claves mayores a 8 dígitos, aumentando así su nivel de seguridad.

- Cambiar "*LoginGraceTime*" el cual regula el tiempo de espera que tiene el usuario para digitar la palabra clave. Figura 19

Figura 19 LoginGraceTime

- Disminuir a 2 el "*MaxAuthTries*" la cual es la opción que mantiene la sesión abierta luego de digitar mal los datos de acceso. Figura 20

Figura 20 MaxAuthTries

- Cambiar el parámetro "*MaxStartups*" para limitar a 2 la máxima cantidad de sesiones abiertas desde la misma IP o terminal hacia los servidores en la nube. Figura 21

Figura 21 MaxStartups

- Editar el parámetro "*AllowUsers*" que se encarga de autorizar el acceso desde las IP´s seleccionadas las cuales serían desde los PC´s permitidos. Figura 22

Figura 22 AllowUser

11. PROCEDIMIENTO APROBADO DE ENTREGA Y SOLICITUD DE ACCESOS

Luego de realizar la presentación a las directivas de tecnología y algunos cambios solicitados se realizó la aprobación del procedimiento que fue divulgado dentro de las áreas interesadas y se envió al área de Calidad para su corrección en formato y control de versiones, para ser agregado a los procedimientos internos del Sistema de Gestión.

11.1. DOCUMENTACIÓN DEL PROCEDIMIENTO:

11.1.1. Control de revisiones y aprobaciones

Figura 18 Formato de control de revisiones y aprobaciones

Revisiones	Nombre	Cargo	Fecha	Firma
Elaborado por:	Andrés Aponte	Senior IT Analyst	27 – 02 - 2018	

Figura 18 (Continuación)

Revisado por:	Aprobador	Manager IT	18 - 04 - 2018	
Aprobado por:	Aprobador	Manager IT	15 – 05 – 2018	

11.1.2. Control de versiones:

Figura 19 Formato de control de versiones

Número de Versión	Fecha de inicio	Fecha de terminación	Observaciones
1	27/02/18	15-05-2018	Versión # 1

11.1.3. Objeto:

Estandarizar, documentar y comunicar las actividades para la gestión de la solicitud y entrega de accesos a las plataformas pertenecientes a la compañía controlada por parte del área de IT hacia las demás áreas de la compañía.

11.1.4. Alcance:

El procedimiento abarca las áreas que necesitan interacción con las plataformas de gestión de acceso a los servidores de producción o desarrollo en el área de IT o tecnología.

11.1.5. Glosario:

a. **IT**: TI, o más conocida como IT por su significado en inglés: information technology, es la aplicación de ordenadores y

equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas.

b. **Acceso Específico**: Servidor al cual se requiere puntualmente tener acceso.

11.1.6. Desarrollo:

Descripción detallada de las actividades del proceso.

11.2. PROCEDIMIENTO DE SOLICITUD

1. El solicitante enviara un correo electrónico a su jefe directo con la solicitud de los accesos a los servidores requeridos con el acceso especifico

2. El jefe de área evaluara con su subalterno si es requiere de los accesos solicitados y procederá a presentar formalmente la solicitud de acceso con el formato aprobado de solicitud de credenciales de acceso.

3. El jefe de área diligenciara el formato correspondiente a la solicitud de

credenciales de accesos y será enviado al encargado de crear los accesos según sea su administrador.

4. El administrador del servidor o los servidores a los cuales se solicitó el acceso por parte del respectivo jefe de área, deberá generar las credenciales solo para quienes estén relacionados en el formato de solicitud de credenciales de acceso.

5. Estas credenciales deben requerir que sean cambiadas en su primer acceso por parte del solicitante para asegurar que se deban cambiar obligatoriamente por nivel mínimo de seguridad.

11.3. PROCEDIMIENTO DE ENTREGA

1. El administrador deberá relacionar en el formato de entrega de credenciales de acceso, entregando como máximo 2 credenciales por requerimiento.

2. Este formato será enviado al jefe de área quien realizo el requerimiento, él será el encargado de realizar la entrega formal de las credenciales, como entrega formal se requiere que sea impreso y firmado por ambas partes el jefe de área como responsable de la entrega y el solicitante

como aprobador de los accesos que fueron requeridos.

3. Es responsabilidad del jefe de área asegurar la entrega de la copia física firmada por ambas partes al área de recepción quien la archivara en su respectivo lugar seleccionado por esta área.

4. Es responsabilidad del jefe de área asegurar la copia digital en el drive de nube donde se almacenarán las evidencias de las entregas de credenciales y propinar al solicitante una copia del documento si este lo solicita; además de reenviar la copia digital firmada al Manager IT para garantizar que se cumplió el procedimiento y operar como veedor de transparencia.

12. PROCEDIMIENTO CAMBIOS EN LOS SERVIDORES

Luego de realizar la presentación a las directivas de tecnología y algunos cambios solicitados se realizó la aprobación del procedimiento con los cambios en los servidores el cual fue comunicado en el área de IT y se envió al área de Calidad para su corrección en formato e iniciar el control de versiones, con el fin de ser agregado a los procedimientos internos del Sistema de Gestión.

12.1. DOCUMENTACIÓN DEL PROCEDIMIENTO:

12.2. CONTROL DE REVISIONES Y APROBACIONES

Figura 20 Formato de control de revisiones y aprobaciones

Revisiones	Nombre	Cargo	Fecha	Firma
Elaborado por:	Andrés Aponte	Senior IT Analyst	25 – 04 - 2018	
Revisado por:	Aprobador	Manager IT	08 - 05 - 2018	
Aprobado por:	Aprobador	Manager IT	22 – 05 – 2018	

12.3. CONTROL DE VERSIONES:

Figura 21 Formato de control de versiones

Número de Versión	Fecha de inicio	Fecha de terminación	Observaciones
1	25-04-18	25-04-18	Versión # 1

12.4. OBJETO:

Estandarizar, documentar y comunicar las actividades para la gestión de los cambios necesarios en los servidores de la empresa Virgin Mobile con el fin de aumentar y personalizar las configuraciones de los equipos en las plataformas de pruebas, desarrollo y producción.

12.5. ALCANCE:

El procedimiento abarca las áreas que administran los servidores de la empresa Virgin Mobile, quienes realizaran los cambios requeridos.

12.6. GLOSARIO:

a. **IT**: TI, o más conocida como IT por su significado en inglés: information technology, es la aplicación de ordenadores y

equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas.

b. **Acceso Específico**: Servidor al cual se requiere puntualmente tener acceso.
c. **SSH**: Protocolo de comunicación por Consola.
d. **Claves Robustas**: contraseñas mayores a 8 caracteres alfanuméricas y con caracteres especiales.

12.7. DESARROLLO:

Descripción detallada de las actividades del proceso.

12.8. PROCEDIMIENTO DE CAMBIOS

Se debe ingresar únicamente por el administrador del servidor con autorización para ejecutar estos cambios y empleando un usuario con permisos “root” en los servidores con SO Ubuntu el cual es el estándar para el uso de la compañía.

- Se debe ingresar a la ruta: **/etc/ssh/sshd_config**

Se deben hacer los cambios en las siguientes líneas:

- Se hará el cambio en el puerto de acceso cambiando el “22” por el puerto que se acuerde entre el manager IT, en la línea que indica el puerto actual.

- En la línea “***LoginGraceTime”*** se debe cambiar el tiempo máximo que el usuario tiene para digitar la contraseña por **5 Segundos**.

- En la línea “***MaxAuthTries***” se debe cambiar el máximo número de intentos no exitosos por parte del usuario a **2 intentos** y luego cierra la sesión.e

- En la línea “***MaxStartups”*** se debe cambiar a máximo **3 sesiones** abiertas al tiempo en los servidores al mismo tiempo y habilitar esta opción si esta deshabilitada por default.

- En la linea *“**AllowUsers**”* se debe agregar las IP´s LAN con que los usuarios autorizados pueden tener acceso a los servidores.

- Luego reiniciar el servicio por medio por medio del comando: **service ssh restart.**

13. RESULTADOS Y AUDITORIAS

Luego de realizar los respectivos procedimientos, formatos y cambios en búsqueda de la mejora de los niveles de acceso a los servidores, se procede a crear un formato de auditoria como propuesta al área de calidad de la empresa con el cual se buscó por medio de preguntas que buscan presentar las evidencias de la ejecución de las mejoras planteadas.

13.1. FORMATO DE AUDITORIA INTERNA

Se diseñó un formato de lista de preguntas de chequeo que buscan auditar los procedimientos por medio de una serie de interrogantes que tienen como objetivo aclarar la cuestión si se están ejecutando los procedimientos, el documento se anexa a continuación:

13.1.1. Control de revisiones y aprobaciones

Figura 22 Formato de control de revisiones y aprobaciones

Revisiones	Nombre	Cargo	Fecha	Firma
Elaborado por:	Andrés Aponte	Senior IT Analyst	05 – 06 - 2018	
Revisado por:	Aprobador	Manager IT	05 - 06 - 2018	
Aprobado por:	Aprobador	Manager IT	05 – 06 – 2018	

13.1.2. Control De Versiones

Figura 23 Formato de control de versiones

Número de Versión	Fecha de inicio	Fecha de terminación	Observaciones
1	05/06/18	05/06/18	Versión # 1

13.1.3. Objeto

Auditar el estado actual de los procedimientos implementados para el

aseguramiento y mejora del nivel de seguridad.

13.1.4. Alcance

Verificar la correcta ejecución de los procedimientos estipulados y asegurar su ejecución.

DESARROLLO:

Descripción detallada de las actividades del proceso.

Figura 24 Formato de lista de verificación

LISTA DE VERIFICACIÓN		
Proceso o procedimiento de seguridad.	Solicitud de Credenciales	
Requisito o procedimiento para auditar.	**Pregunta**	**Anotaciones**

Figura 24 (Continuación])

Procedimiento solicitud de credenciales	**¿Existe un formato para solicitud de credenciales?**	**Se cuenta con un formato aprobado para la solicitud de credenciales.**
	¿Se están almacenando los formatos firmados?	**Se almacenan en físico y digital.**
	¿Quien realiza la aprobación de los requerimientos de solicitud?	**El personal encargado y responsable en el procedimiento.**
Proceso o procedimiento:	Entrega de Credenciales	
Requisito o procedimiento para auditar.	**Pregunta**	**Anotaciones**
Procedimiento entrega de credenciales	**Existe un formato para entrega de credenciales?**	**Se cuenta con un formato aprobado para la entrega de credenciales.**

Figura 24 (Continuación)

	¿Se están almacenando los formatos firmados?	**Se almacenan en físico y digital además de la entrega de una copia al solicitante.**
	¿Quién realiza la creación de las credenciales solicitadas?	**Son creadas por los administradores de los servidores bajo requerimiento aprobado del respectivo formato.**
Proceso o procedimiento:	Cambios configuración de acceso de servidores	
Requisito o procedimiento para auditar.	**Pregunta**	**Anotaciones**

Figura 25 (continuación)

Procedimiento cambios de configuración de acceso de servidores.	**¿Existe un procedimiento para el cambio de la configuración de acceso a los servidores?**	**Se cuenta con procedimiento para el cambio de la configuración de acceso a los servidores.**
	¿Quienes tienen la potestad para realizar estos cambios?	**Solo los administradores de los servidores.**
	¿Se puede verificar el cambio realizado?	**Se puede ingresar a cada servidor para validar que se realizaron los cambios en el archivo de configuración de accesos.**

14. CONCLUSIONES

- Se diseñaron los procedimientos estándar para los accesos a las plataformas en los diferentes ambientes en búsqueda de mitigar las vulnerabilidades latentes.

- Se crearon los formatos y procedimientos que soportaran las buenas prácticas de solicitud o entrega de credenciales al analizar la información recolectada con la encuesta a los empleados del área de tecnología.

- Se realizaron los cambios relacionados en el procedimiento de cambios en los servidores para asegurar un nivel óptimo en los accesos por parte de los empleados.

15. BIBLIOGRAFIA

McClure, S., Scambray, J., & Kurtz, G. (2010). Hackers 6: secretos y soluciones de seguridad en redes. México: McGraw-Hill Interamericana. Recuperado de: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10433876&tm=1465509236690

Sistema Operativo Ubuntu Server. [online] Available at: http://isft179-ubuntuserver.blogspot.com.co/ [Accessed 06 Nov. 2017].

Cañihua, F. R. (2007). Elaboración de una medida tecnológica que permita garantizar y proteger el adecuado tratamiento de los datos personales en el Internet de tercera generación/Ipv6. Chile: Universidad de Chile. Recuperado de: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10198466&tm=1465508433109

Duarte, E. (2017). Cómo Mejorar La Seguridad En Un Servidor Linux. [online] Información práctica sobre Redes, Linux, Seguridad y Hacking para profesionales de TI. Capacity Academy. Available at: http://blog.capacityacademy.com/2013/10/31/recomendaciones-de-seguridad-para-servidores-linux/ [Accessed 06 Nov. 2017].

Amazon Web Services, Inc. (2017). ¿Qué es AWS? – Amazon Web Services. [online] Available at: https://aws.amazon.com/es/what-is-aws/ [Accessed 08 Nov. 2017].

Chandrasekaran, K. (n.d.). Essentials of cloud computing.

Tiempo, C. (2017). Un nuevo ataque cibernético mundial afecta a varias multinacionales. [online] El Tiempo. Available at: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/nuevo-ataque-cibernetico-afecta-a-empresas-en-el-mundo-103092 [Accessed 14 Nov. 2017].

Abril, A., Pulido, J., & Bohada, J. A. (2013). Análisis de riesgos en seguridad de la información. Ciencia, Innovación y Tecnología, 39-53.

Cad.com.mx. (2017). Generaciones de las Computadoras. [online] Available at: http://www.cad.com.mx/generaciones_de_las_computadoras.htm [Accessed 08 Nov. 2017].

GLobalLogic Latinoamerica. (2017). Seguridad en el modelo IaaS | GLobalLogic Latinoamerica. [online] Available at: https://www.globallogic.com/latam/gl_news/seguridad-en-el-modelo-iaas/ [Accessed 14 Nov. 2017].

Ellis, G. (2015). Microsoft Azure IaaS essentials. Birmingham, UK: Packt Publishing.

Computación en La Nube. (2017). Casos de Exito. [online] Available at: http://cloudcomputinguq.wordpress.com/casos-de-exito/ [Accessed 10 Nov. 2017].

Sage One. (2017). 4 ventajas de los negocios escalables. [online] Available at: http://www.sageone.es/2014/09/10/4-ventajas-de-los-negocios-escalables/ [Accessed 08 Nov. 2017].

COLOBRAN HUGUET Miguel, (2008). Administración de sistemas operativos en red: Administración de servidores. Barcelona: Editorial UOC, 37 p. ISBN: 978-84-9788-760-1

Pacio, G. (2017). Estándares en el Data Center. [online] Datacentershoy.com. Available at: http://www.datacentershoy.com/2013/02/estandares-en-el-data-center.html [Accessed 02 Nov. 2017].

Doublehorn. (2017). Risks and Concerns about IaaS – Executive Perspective. [online] Available at: https://doublehorn.com/risks-and-concerns-about-iaas/ [Accessed 06 Nov. 2017].

Mather, T., Kumaraswamy, S. and Latif, S. (2009). Cloud security and privacy. Beijing: O'Reilly.

Hugos, M. and Hulitzky, D. (2011). Business in the cloud. New York: Wiley.

Brown, P. and Nuara, L. (2011). Cloud computing 2011. New York, N.Y.: Practising Law Institute.

Top de los 7 mejores y más veloces proveedores de internet en Colombia. (2017). Top de los 7 mejores y más veloces proveedores de internet en Colombia. [online] Available at: http://www.dinero.com/emprendimiento/articulo/los-mejores-proveedores-de-internet-en-colombia-segun-netflix/241512 [Accessed 07 Nov. 2017].

Interxion.com. (2017). Qué es el cloud computing y cuáles son sus beneficios en las empresas. [online] Available at: http://www.interxion.com/es/blogs/2014/03/que-es-el-cloud-computing-y-cuales-son-sus-beneficios-en-las-empresas/ [Accessed 08 Nov. 2017].

Ceac. (2017). Tipos de seguridad informática. [online] Available at: https://www.ceac.es/blog/tipos-de-seguridad-informatica [Accessed 08 Nov. 2017].

Iingen.unam.mx. (2017). Virus informáticos. [online] Available at: http://www.iingen.unam.mx/es-

mx/Publicaciones/GacetaElectronica/Febrero2015/Paginas/Virusinformaticos.aspx [Accessed 09 Nov. 2017].

Mastermagazine.info. (2017). Cracker. [online] Available at: https://www.mastermagazine.info/termino/4472.php [Accessed 09 Nov. 2017].

pensante, E. (2017). La investigación de campo – El pensante. [online] Educacion.elpensante.com. Available at: https://educacion.elpensante.com/la-investigacion-de-campo/ [Accessed 09 Nov. 2017].