ANÁLISIS Y GESTIÓN DEL RIESGO DE LA INFORMACIÓN EN LOS SISTEMAS DE INFORMACIÓN MISIONALES DE UNA ENTIDAD DEL ESTADO, ENFOCADO EN UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

HINA LUZ GARAVITO ROBLES

UNIVERSIDAD ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2015

ANÁLISIS Y GESTIÓN DEL RIESGO DE LA INFORMACIÓN EN LOS SISTEMAS DE INFORMACIÓN MISIONALES DE UNA ENTIDAD DEL ESTADO, ENFOCADO EN UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

HINA LUZ GARAVITO ROBLES

Tesis de grado para optar por el título:
Especialista En Seguridad Informática

Director de Proyecto:
John Freddy Quintero Tamayo. MS (c)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2015

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, 31 de marzo de 2015

Dedicatoria

Este proyecto de Tesis está dedicado a mi hija Valeria Gómez Garavito, una niña de 3 años que es mi universo y es mi motivación para alcanzar mis metas.

Agradecimientos

Mis agradecimientos al profesor John Freddy Quintero Tamayo por su constante apoyo y por la motivación que me brindo para realizar este proyecto.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

Hoy en día con el alcance de la tecnología y la dependencia de ella para todas las actividades tanto cotidianas como de la empresa. Se presentan situaciones en que hay mucha información en los sistemas, se debe velar por su confidencialidad, integridad y disponibilidad de los datos.

Porque así como hay personas con una alta ética profesional y personal también las hay sin escrúpulos que quiere sacar provecho de la información privada de las empresas, vemos casos como el *Phishing* (suplantación de identidad), la captura de información para fines fraudulentos, como también casos donde se hace daño a la integridad de los datos de una empresa o a los sistemas de información, con el fin de perjudicar a la Entidad.

Por esta razón la empresa en estudio que es una entidad del estado y por motivos de seguridad no se revela el nombre en este documento se ve en la responsabilidad de involucrar implantar un SGSI iniciando para ello con el Análisis del Riesgo que se planteará en este documento.

1. FORMULACIÓN DEL PROBLEMA

La entidad estatal caso de estudio manifiesta la urgente necesidad de proteger su activo más valioso ña informaciónò y esto se ve agravado con el constante incremento de la información en la entidad como también de los sistemas de información en la web que son necesarios para la gestión de información en sus diferentes centros de servicio a nivel nacional.

Como también manifiesta la preocupación de haber sido objetivo de ataques de interceptación a la información confidencial en sus sistemas de información y recalca la gran importancia que tiene para la Entidad velar por la seguridad de sus Sistemas de Información Misional.

Se evidencia que no existen procedimientos definidos de seguridad de la información como tampoco existen controles y políticas de contingencia que permitan mitigar un posible evento negativo y continuidad del negocio.

Desde el punto de vista de la Entidad que maneja los datos, existen amenazas de origen externo, como las agresiones técnicas (cibercriminales), naturales o humanas y de origen interno por la negligencia del propio personal o fallas en las condiciones técnicas de procesos operativos internos.

Otro tipo de amenazas que no están en primer lugar pero igual son alarmantes y que se debe tomar en consideración son:

- Falta de Backups de datos
- Perdida de información por rotación, salida de personal
- Abuso de conocimientos internos (no consultado en encuesta de organizaciones sociales)
- Mal manejo de equipos y programas
- Acceso non-autorizado

2. JUSTIFICACIÓN

La entidad manifiesta carencias en seguridad de la información con el propósito de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos. Se hace necesario establecer políticas y controles de mejoramiento de los procesos de seguridad de la información.

Debido a la existencia de las amenazas externas: técnicas (cibercriminales), naturales; de tipo interno (los mismos empleados) y otras como: Falta de Backups de datos, perdida de información por rotación, salida de personal, abuso de conocimientos internos (no consultado en encuesta de organizaciones sociales), mal manejo de equipos y programas, Acceso no autorizado. Se hace necesario ejecutar acciones (controles) para mitigar las amenazas de la información que se puedan presentar en la entidad, preverlas, implementar medidas de protección para evitar o minimizar los daños en caso de que se realice una amenaza.

De ahí la importancia que en la Entidad tome conciencia que debe contrastar los riesgos a la que están sometida sus activos. Y entender que la evaluación, análisis y tratamiento del riesgo permite llevar ese nivel a valores aceptables. Y así poder organizar la defensa concienzuda y prudente de la Entidad, evitando situaciones difíciles y estando preparados para contrarrestar emergencias; permitiendo que esta sobreviva a los incidentes y siga operando en las mejores condiciones. Como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección de la Entidad asume.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un análisis de seguridad informática para determinar, y gestionar los posibles riesgos de la entidad enfocados en su Sistemas de Información Misional.

3.2 OBJETIVOS ESPECIFICOS

- Valorar los activos que tiene la Entidad relacionados con el Sistema de Información Misional y estimar el impacto que puede causar en la empresa su daño o perdida

- Estudiar los riesgos asociados al Sistema de Información Misional de la Entidad y a su entorno.

- Listar las amenazas existentes sobre cada uno de los activos estudiados permitiendo realizar la valoración del riesgo

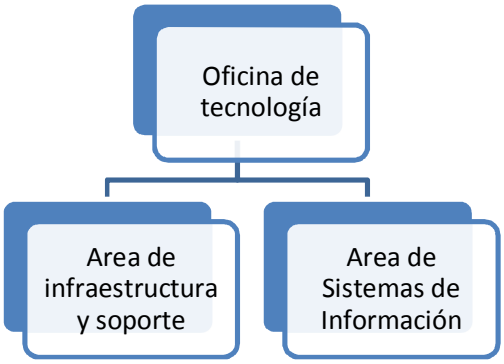
- Recomendar las medidas necesarias y selección de controles para conocer, prevenir, impedir, reducir o controlar los riesgos estudiados.

4. MARCO REFERENCIA

La entidad estatal para la cual se va a realizar el análisis y gestión del riesgo está encargada de coordinar, asesorar y ejecutar con otras entidades públicas y privadas a personas de un grupo específico de la sociedad. Adicionalmente diseña, implementa y evalúa la política de Estado dirigida a la reintegración social y económica de un grupo determinado de la sociedad.

El área de informática o departamento de sistemas de la entidad tiene el nombre de ñOficina de Tecnologíaò que está constituida por 2 subáreas: El área de infraestructura y soporte y el Área de sistemas de información, ver Figura 6.

Figura 1. Áreas de la Oficina de Tecnología.



Fuente Autor.

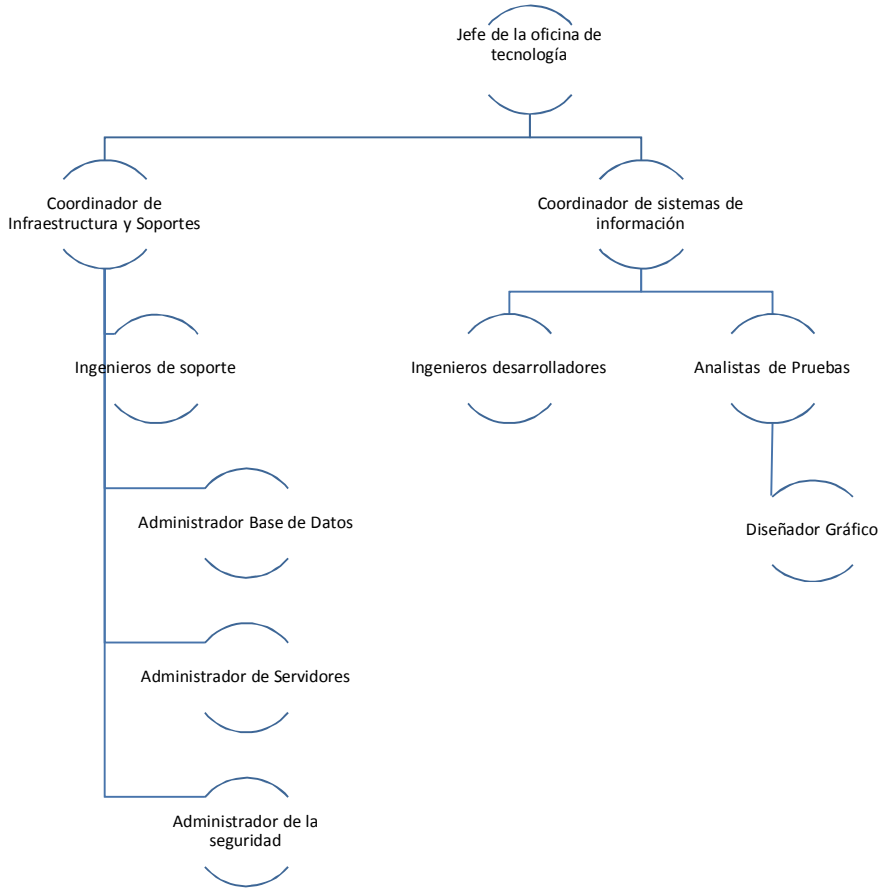
Cada Área tiene sus funciones específicas y brinda soporte a grupos de determinados usuarios.
El Área de Infraestructura y Soporte: Es un grupo constituido por 10 ingenieros de sistemas con diferentes especialidades encargados de monitorear la red de comunicación de la empresa, dar soporte a los equipos de cómputo de los usuarios finales, administrar los servidores.

El Área de Sistemas de Información: Está constituida por 11 ingenieros de sistemas en su mayoría desarrolladores de Software encargados de realizar desarrollos a la medida para el Sistemas de Información Misional de la entidad y dar soporte al usuario respecto a los sistemas.

4. 1 DESCRIPCION DEL RECURSO HUMANO

El perfil del recurso humano está clasificado de acuerdo a la subárea de tecnología que pertenece como se puede evidenciar en la Figura 2.

Figura 2. Estructura Organizacional de la oficina de Tecnología



Fuente Autor.

4.1.1 Funciones del recurso humano del área de infraestructura y soporte. Son las siguientes:

- Proveer de servicios informáticos o tele-informáticos que sirven de base a la labor de la entidad. Con la responsabilidad de mantener en funcionamiento la infraestructura requerida para esto, sino también de coordinar un adecuado mantenimiento y renovación de equipos y sistemas computacionales de base.

- Soporte a usuarios, con habilidad para dar entrenamiento, soporte, resolver problemas operativos y técnicos a los usuarios de los sistemas de información.

4.1.2 Funciones del recurso humano del área de sistemas de información. Son las siguientes:

- Diseñar sistemas de información en función de los requerimientos estratégicos de la entidad.
- Implementar, mantener e innovar proyectos de productos de software con tecnologías web para apoyar el área Misional de la entidad.
- Implementar, mantener proyectos de software en tecnología móvil con el objetivo de apoyar el área Misional de la entidad
- Seleccionar las tecnologías de hardware, software y telecomunicaciones más adecuadas.
- Brindar soporte a los usuarios finales en el manejo de los sistemas de información

4.1.3 Los Sistemas de Información analizados. Son las siguientes:

- El Sistema de Información Misional de la entidad: Que se encarga de administrar la información personal de un grupo de determinado de personas, como también ciertos servicios que le ofrece la entidad a estas personas en educación, formación para el trabajo, asesoría psicológica. Como también lleva el registro de los aportes económicos que les suministra la entidad a estas personas.

- El portal Web de la entidad: Donde se visualiza la misión y visión de la entidad como también las noticias referentes a ella y se publican información de interés a la población en general y ofrecer servicios de atención al ciudadano.

- Sistemas de Encuestas: Tiene como finalidad permitir a la entidad realizar preguntas sobre un tema específico a la población que tiene relación con la entidad. Este sistema permite recolectar información y utilizarla para la toma de decisiones.

5. DISEÑO METOLÓGICO PRELIMINAR

Existen instrumentos que estando alineados con estos estándares ISO 27001 y que facilitan a una empresa enfocarse en implementar herramientas y metodologías que satisfagan los requerimientos básicos de la administración de riesgos en sus sistemas de información tales como la metodología Magerit para realizar el análisis y gestión del riesgo enfatizando en las políticas y controles de seguridad por cada capa o capitulación del compendio de ISO 27001.

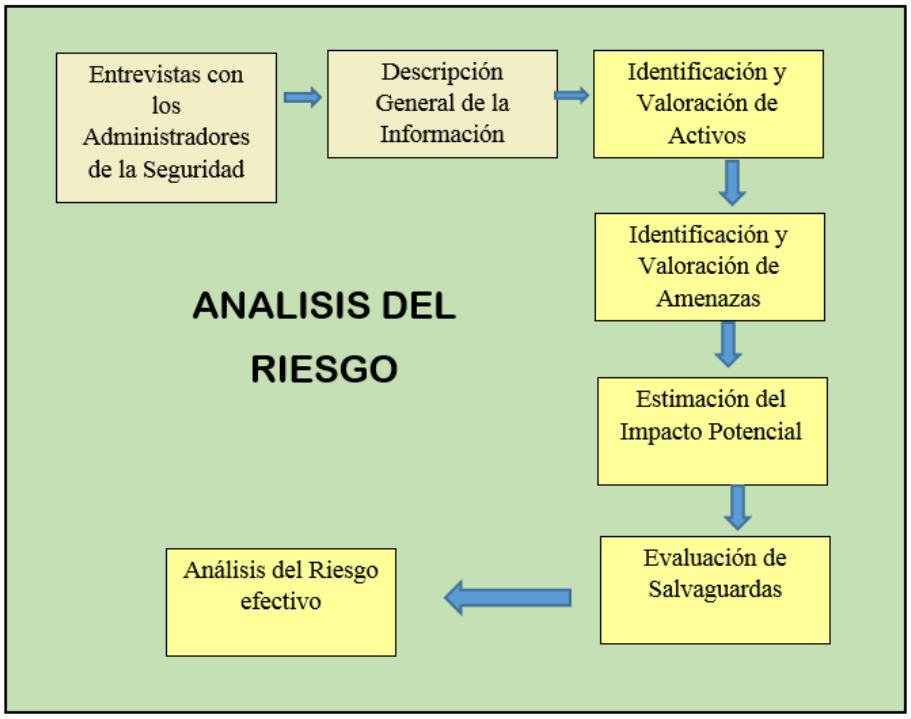
La norma ISO/IEC 27001 estipula que debe utilizarse un método de análisis de riesgo, pero esto no es una parte del estándar, y no se propone ningún método específico, aparte de la integración del proceso recursivo PDCA (*Plan, Do, Check, Act*) del modelo definido para la creación del SGSI.[1]

La norma ISO 27001 define estándares y controles para la gestión del riesgo y estos se logran definir después de un estudio de valoración del riesgo que se trabaja con la metodología Magerit.

Magerit fue elaborada por el Consejo Superior de Administración Electrónica con el objetivo de minimizar los riesgos de implantación y uso de las TIC en las Administraciones Públicas. Aunque existen varias herramientas que permiten llevar a cabo el análisis con mayor automatización (PILAR), llevarlo a cabo a mano no es especialmente complejo. [1] Se trata de un proceso de varias fases que se detallará a continuación en la Figura 3.

[1] Pablo Casto, septiembre 2014, Metodología Magerit. En línea: http://gr2dest.org/metodologia-de-analisis-de-riesgos-magerit/

Figura 3. Etapas de la metodología de análisis de riesgos.



Fuente: Autor

5.1 ETAPAS DE LA METODOLOGIA

La metodología Magerit está conformada por varias etapas que se describen a continuación:

- Identificación y Valoración de Activos: Se realiza el análisis de riesgo el primer paso es identificar los activos que existen en la entidad y determinar el tipo y su valor en la dimensiones de seguridad (Integridad, Autenticidad, Confidencialidad, Disponibilidad). Dentro de esta etapa se realizan Entrevistas con los responsables de los activos, se tabula la información recolectada.

- Identificación y Valoración de Amenazas: Se identifican las amenazas en los activos y determinar el nivel de exposición en la que se encuentra cada activo de información en la entidad. Después se realiza la valoración de las vulnerabilidades en cada uno de los activos, es decir, determinar que amenazas los puede afectar, con qué frecuencia se puede presentar la amenaza y que dimensión de seguridad puede ser afectada.

- Estimación del Impacto Potencial: Es resultado desmaterializarse las amenazas consideradas en cada activo.

- Establecimiento de Salvaguardas
  Está relacionado con la determinación de controles que se deben implementar para mitigar el riesgo

- Análisis del riesgo efectivo: Que es el riesgo que se estima después de aplicar los salvaguardas en la empresa

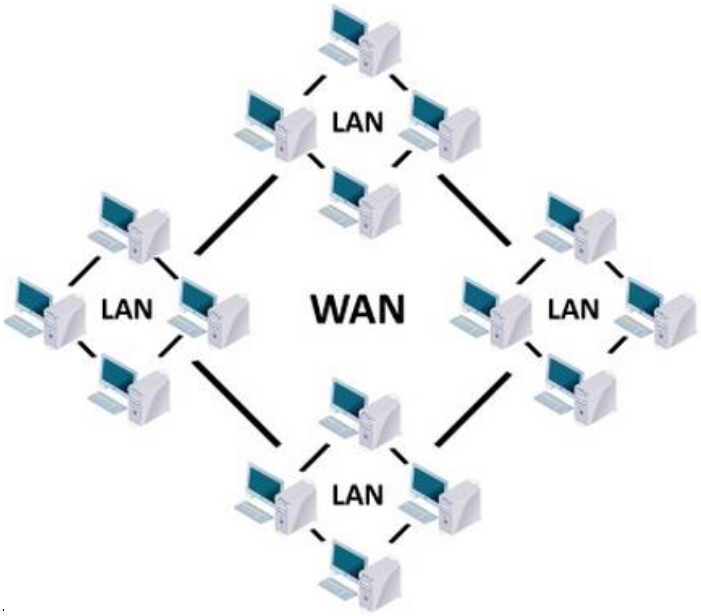
6. ANÁLISIS DE LA INFRAESTRUCTURA TECNOLOGIA DE LA ENTIDAD

La infraestructura tecnológica de la entidad está conformada por su red de comunicaciones y sus sistemas de información.

6.1. DESCRIPCIÓN DE LA RED

La Entidad caso de estudio tiene un tipo de red WAN (MPLS): Es una red que da cobertura en un área geográfica extensa, proporcionando capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y satelital, ver ñFigura 4ò

Figura 4. Estructura WAN (MPLS).



Fuente http://www.ebrahma.com/2012/07/remote-connectivity-wan-options-in-brief

La red WAN (MPLS) es más amplia que la rede un área local y cubre áreas mayores que en algunos casos no se limitan a un entorno metropolitano sino que pueden

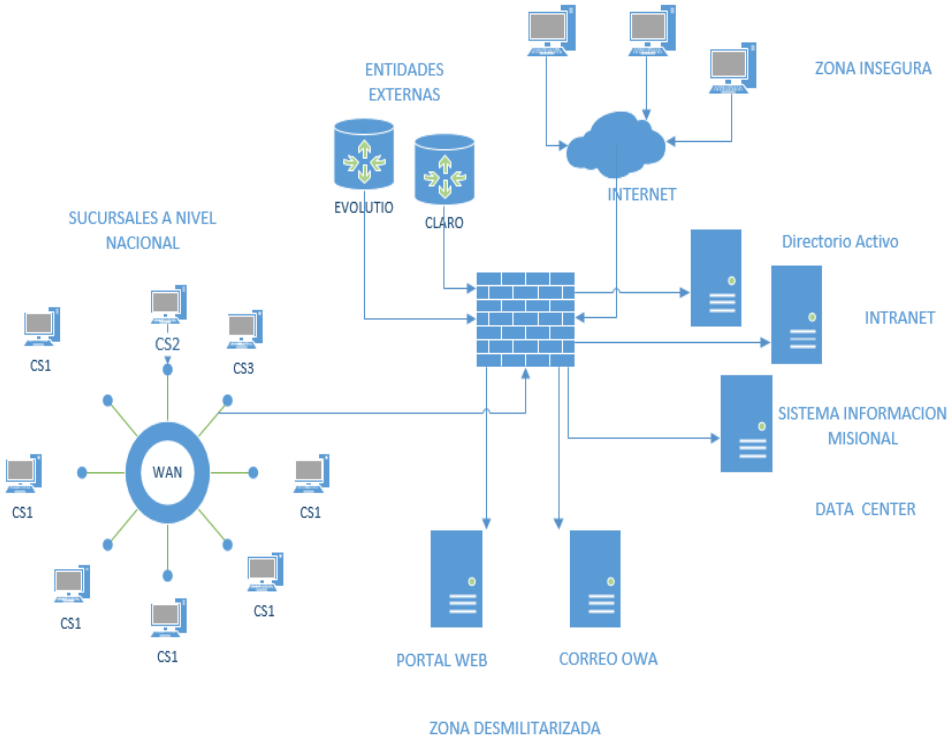
llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana. [2]

Los servicios basados en MPLS mejoran la recuperación ante desastres de diversas maneras. En primer lugar, permiten conectar los centros de datos y otros emplazamientos clave mediante múltiples conexiones redundantes a la nube MPLS y, a través de ella, a otros sitios de la red. Además, los sitios remotos pueden ser reconectados fácil y rápidamente a las localizaciones de backup en caso de necesidad; a diferencia de lo que ocurre con las redes ATM y Frame Relay, en las cuales se requieren circuitos virtuales de Backup permanentes o conmutados. Esta flexibilidad para la recuperación del negocio es precisamente una de las principales razones por la que la Entidad escogió esta tecnología.[3]

6.1.1 Estructura de la red de la Entidad. La estructura de Red está compuesta por: Una zona desmilitarizada, zona insegura, Sucursales a nivel nacional, Data Center, Entidades Externas (ver Figura 5). A continuación describiremos cada zona:

[2] Red MAM. En línea: http://definicion.de/red-man/
[3] Network world, diciembre 2007, Migración a MPLS. En línea: http://www.networkworld.es/networking/migracion-a-mpls-por-que-cuando-como

Figura 5. Estructura de la red de la entidad.



Fuente: Autor

6.1.1.1 Zona desmilitarizada. En seguridad informática, una zona desmilitarizada (conocida también como DMZ, sigla en inglés de demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de la entidad y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa - los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.[4]

[4] Wikipedia, 9 de enero de 2015, Zona desmilitarizada. En línea: http://es.wikipedia.org/wiki/Zona_desmilitarizada_%28inform%C3%A1tica%29

Una DMZ se crea a menudo a través de las opciones de configuración del firewall, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall).

6.1.1.2 Zona Insegura. Es la zona perteneciente al internet.

6.1.1.3 Sucursales a nivel Nacional. La Entidad tiene sucursales a nivel nacional en las diferentes ciudades del país.

6.1.1.4 Data Center. Es donde se encuentra el Portal y El Sistema de Información Misional de la entidad.

6.1.1.5 Entidades Externas. Son los proveedores que prestan el servicio de internet.

6.2 RESUMEN INFORMATICO Y FUNCIONAL DE LOS SISTEMAS DE INFORMACION SENSIBLES

Los sistemas de información de la entidad están conformados por un Portal web, un Sistema Web de Encuestas y su Sistema de Información Misional y los describiremos a continuación.

6.2.1 El Portal Web. Tiene como objetivo informar a la comunidad acerca de la Entidad y está conformado por las siguientes sesiones:

- Información sobre la entidad, sus funciones, sus políticas.
- Información sobre sus trámites y servicios
- La sesión de notificaciones al usuario: Que tiene implícita una sesión de autenticación para que el sistema pueda mostrar las notificaciones relacionadas a las personas vinculadas a la entidad.
- La sesión Peticiones, Quejas, Reclamos, Sugerencias y Denuncias que permite al ciudadano registrarse y crear Peticiones, quejas, reclamos y sugerencias.

El portal esta realizado con la tecnología ASP.Net y base de datos Sql server.

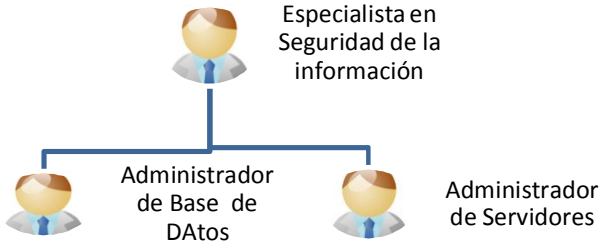
6.2.2 El Sistema Web de Encuestas. Es un sistema que permite a la Entidad realizar encuestas son temas definidos para la entidad y que recogen información necesaria para tomar decisiones en la entidad a cerca de sus vinculados.

6.2.3 El Sistema de Información Misional. Es el sistema de información que permite gestionar todos los datos de las personas vinculadas a la Entidad. Está relacionado con los servicios que le presta la Entidad a todos sus vinculados. Este Sistema es manejado solo por los funcionarios de la entidad y es utilizado a través de la intranet. Esta realizado en .Net y con Base de Datos Sql Server.

6.3 ESTRUCTURA ORGANIZACIONAL DE LA SEGURIDAD EN LA ENTIDAD

Esta estructura de la entidad (ver ñFigura 6ò) está conformada por un Especialista en Seguridad que sirve como asesor en los temas de seguridad al Administrador de Base de Datos y Administrador de Servidores, los cuales gestionan temas de seguridad en las áreas que administran, ver Figura 6.

Figura 6. Administradores de la seguridad en la entidad.



Fuente: Autor

6.4 POLITICAS DE SEGURIDAD INFORMATICA EXISTENTES EN LA ENTIDAD

A continuación se exponen las políticas de seguridad que estipuladas actualmente en la entidad sobre diferentes directrices:

6.4.1 Del Uso del Servicio de Internet. El servicio de Internet en la entidad, es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios, por lo tanto, su utilización debe observar y cumplir las directrices que a continuación se enlistan:

- El uso del Servicio de Internet está limitado exclusivamente para propósitos laborales.
- Los servicios a los que un determinado usuario pueda acceder desde la Internet dependerán del rol que desempeña el usuario en la entidad y para los cuales este formal y expresamente autorizado.
- Todo usuario es responsable de informar de contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones dentro de la entidad.
- Está expresamente prohibido el envío y/o descarga y/o visualización páginas de contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido el acceso a páginas web, portales, sitios web y/o aplicaciones web que no hayan sido autorizadas por la entidad.
- Está expresamente prohibido el envío y/o descarga de cualquier tipo de software o archivos de fuentes externas y/o de procedencia desconocida.
- Está expresamente prohibido la propagación de virus o cualquier tipo de código malicioso.
- Está expresamente prohibido acceder a páginas que agredan la ética y el buen comportamiento.
- La entidad se reserva el derecho de monitorear los accesos y por tanto uso del Servicio de Internet de todos sus colaboradores, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines institucionales.

6.4.2 Del Uso del Correo Electrónico. El servicio de correo electrónico Institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios de la, en tal virtud, su uso debe sujetarse a las siguientes directrices:

- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de orden institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Entidad

- Se debe preferir el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan, cumpliendo con la Directiva Presidencial No.03 Cero Papel
- Está prohibido el uso de correos masivos tanto internos como externos, salvo a través del correo institucional, el cuál es administrado por el grupo de comunicaciones.
- Todo mensaje SPAM o CADENA debe ser inmediatamente reportado al correo de soporte de la entidad, eliminado y nunca respondido. No está permitido el envío y/o renvío de mensajes en cadena.
- Todo mensaje sospechoso respecto de su remitente o contenido debe ser inmediatamente reportado al correo de soporte de la entidad y posteriormente eliminado, ya que puede ser contentivo de virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, tengan explícitas referencias eróticas o alusiones a personajes famosos.

6.4.3 Del Manejo de la Información. Es lo relacionado a la gestión de la información perteneciente a la Entidad. Su uso debe sujetarse a las siguientes directrices:

- La copia de información RESERVADA o CONFIDENCIAL, deberá ser autorizada por el Propietario de la información.
- El almacenamiento de información RESERVADA o CONFIDENCIAL no deberá realizarse en el disco duro u otro componente del computador personal.
- La información RESERVADA solo podrá ser almacenada en las bases de datos de los sistemas de información dispuestos para este fin, para garantizar su seguridad y respaldo.
- La información CONFIDENCIAL y de USO INTERNO deberá ser almacenada en los discos de red para garantizar su seguridad y respaldo.
- El acceso a la información RESERVADA y/o CONFIDENCIAL solo podrá ser autorizado por el propietario de la información.
- Los acuerdos de No-Divulgación de Información que se suscriban con terceros deberán incluir cláusulas referentes al uso de la información y su destrucción posterior.

6.5 HERRAMIENTAS Y CONTROLES ACTUALES DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD

Herramientas y controles actuales de seguridad de la información en la entidad se utiliza SOLAR WIND para el monitoreo de red y para el registro de log se trabajan con la herramienta SIEM de SOLAR WIND que maneja el Log de operaciones del sistema operativo Windows, junto con un Firewall Perimetral utilizado para bloquear las posibles intrusiones, como también controlar la navegación en internet, controla los accesos a internet por VPN y protege la red interna y la zona desmilitarizada de las posibles intrusiones. Además también se cuenta con otra herramienta IPS (Sistema de Prevención de Intrusos) se previenen las intrusiones y se pone fin a ataques maliciosos. A continuación describiremos las funciones de cada herramienta y como se utilizan en la entidad.

6.5.1 Firewall Perimetral Redundante (H.A) La entidad posee un Firewall Perimetral tipo UTM (Gestión Unificada de Amenazas). Es un sistema que puede detectar y eliminar virus, gusanos y otras amenazas basadas en contenido, sin afectar el rendimiento de la red, incluso para aplicaciones que están funcionando en tiempo real. Algunas de estos servicios son: Inspección de paquetes, función VPN, Anti Spam (para evitar los correos no deseados o spam), Anti Phishing, Antispyware, Filtrado de contenidos (para el bloqueo de sitios no permitidos mediante categorías), Antivirus de perímetro (evitar la infección de virus informáticos en computadoras clientes y servidores), Detección/Prevención de Intrusos (IDS/IPS).[5]

La herramienta en la Entidad se utiliza para controlar la navegación de los usuarios en internet, generar reportes de la navegación de los usuarios. También se controla con el firewall la conexión de acceso remoto VPN.

En firewall en la mayoría de los casos se utiliza para proteger la red interna y la zona desmilitarizada de la red, como también se utiliza para controlar el acceso en la red inalámbrica

[5] New Visión SoftLan, La Solución de Seguridad Definitiva para Redes. En Línea:http://www.newvisionsoftlan.com/infraestructuras.html

6.5.2 Herramienta De Monitoreo De Red (Solar Winds). Esta herramienta permite a través del Network Performance Monitor (NPM), proveer una completa plataforma para la administración de fallas y monitorización de desempeño que permite al área de Tecnologías de la información recolectar información y ver la disponibilidad de cada uno de los componentes de su infraestructura tecnológica en tiempo real y los históricos de estadísticas desde un Web Browser, mientras se monitorea, se recolectan y analizan datos de enrutadores, switches, firewalls, servidores y cualquier otro dispositivo con el protocolo SNMP habilitado.[6]

La herramienta en la Entidad se utiliza para:

- Se utiliza para realizar un escaneo o analices de la red permitiendo la detección, el diagnóstico y la resolución de problemas de la red antes de que se produzca un corte del servicio.

- También es utilizado por el administrador de la red para hacer seguimiento del tiempo de respuesta, tiempo de actividad y para analizar la disponibilidad (routers, los conmutadores y otros dispositivos con SNMP habilitado) de los dispositivos y elementos que componen la infraestructura del área Tecnológica.

- Para analizar la capacidad y utilización de ancho de banda de switches, enrutadores e interfaces de red.

- Para monitorear la red en busca de trafico excesivo o inusual que llega al sistema

6.5.3 SIEM - Correlacionador de Eventos- Lem (Solar Winds). SolarWinds LEM permite el Análisis proactivo de registros de los dispositivos de la red, como también es correlación de eventos de la red, sistemas, aplicaciones, máquinas virtuales e infraestructura de almacenamiento con casi 700 reglas de correlación incorporadas y un constructor de reglas personalizable para crear y compartir reglas con otros ad ministradores de TI. [7]

La herramienta en la entidad se utiliza para efectuar el registro de los *Log* en los servidores, si hay una alerta critica envía un correo notificando. Las alertas críticas en la entidad son aquellas que están relacionadas con la caída de un servicio, el

[6] SolarWind. SolarWind El poder de Administrar por completo. En línea: http://www.solarwinds.com/es/
[7] SolarWind, Julio 2011. SolarWinds Log & Event Manager. En línea: http://www.marketwired.com/press-release/solarwinds-completa-adquisicion-de-trigeo-y-presenta-solarwinds-log-event-manager-1537527.htm

llenado de un disco duro, problemas de memoria, alta ocupación de procesadores; como también notifica acerca de intrusiones de seguridad en el caso de ingresos de usuarios no autorizados.

6.5.4 Ips(Sistema de Prevención de Intrusos). Es una tecnología de software más que hardware que ejerce el control de acceso en una red de computadores para protegerla de ataques y abusos. La tecnología de Prevención de Intrusos (IPS) es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías de firewalls que lo complementan.[8]

Esta herramienta en la Entidad se utiliza como complemento para el Firewall como sistema de prevención de intrusos para poner fin a ataques maliciosos entre diferentes zonas de estructura de la red.

6.5.5 Arcserve Backup- Computer Associates. Arcserve es una de soluciones de software de protección de datos que permite a las organizaciones gestionar las copias de seguridad de su información, como también replicar y recuperar datos críticos no estructurados y de misión a través de un híbrido de los entornos de almacenamiento y recuperación complejas(ARCserve, Unificado de Protección de Datos), combina la copia de seguridad, recuperación, replicación y tecnologías de alta disponibilidad en un interfaz de usuario consolidada, lo que elimina la necesidad de los clientes gestionar múltiples interfaces.[9]

CA ARCserve proporciona la flexibilidad para utilizar el cifrado de proteger los datos sensibles durante las diversas etapas de la proceso de copia de seguridad. Utiliza AES (Advanced Encryption Standard) para encriptar los datos. Puede cifrar los datos en una tarea de respaldo con una de las tres opciones:

- Cifrado en el agente
- Cifrado en el servidor de CA ARCserve Backup durante el reserva
- Cifrado en el servidor de CA ARCserve Backup durante migración (por tarea de almacenamiento intermedio)

[8] Ditech. Prevención de Intrusos IPS. En línea: http://ditech.com.co/soluciones-integrales/seguridad-informatica-en-redes/revencion-de-intrusos-ips/

[9] ArcServer, En línea: http://www.isoftland.com/docs/caarcserve/Replication/CA_Arcserve_Replication_es.pdf

Esta herramienta se utiliza en la Entidad para realizar copias de seguridad en la entidad de las base de datos y de los archivos de misión crítica.

6.5.6 Un servicio de Token de Seguridad (STS). Es un software basado en proveedor de identidad responsable de emitir tokens de seguridad, especialmente los identificadores de software, como parte de una identidad basada en notificaciones del sistema.

En un escenario de uso típico, un cliente solicita el acceso a una aplicación de software seguro, a menudo llamada la parte que confía. En lugar de la aplicación autenticación del cliente, el cliente es redirigido a un STS. El STS autentica el cliente y emite una señal de seguridad. Por último, el cliente se redirige de nuevo a la parte que confía en que se presenta la señal de seguridad. El token es el registro de datos en la que las reclamaciones se embalan y se protege de la manipulación con la criptografía fuerte. La aplicación de software verifica que el token se originó a partir de un STS de confianza por él y, a continuación, toma decisiones de autorización en consecuencia. El token es la creación de una cadena de confianza entre los STS y la aplicación de software que consumen las reivindicaciones. Este proceso se ilustra en la aserción de seguridad Markup Language (SAML) de casos de uso, lo que demuestra cómo puede utilizar un único inicio de sesión para acceder a los servicios web.

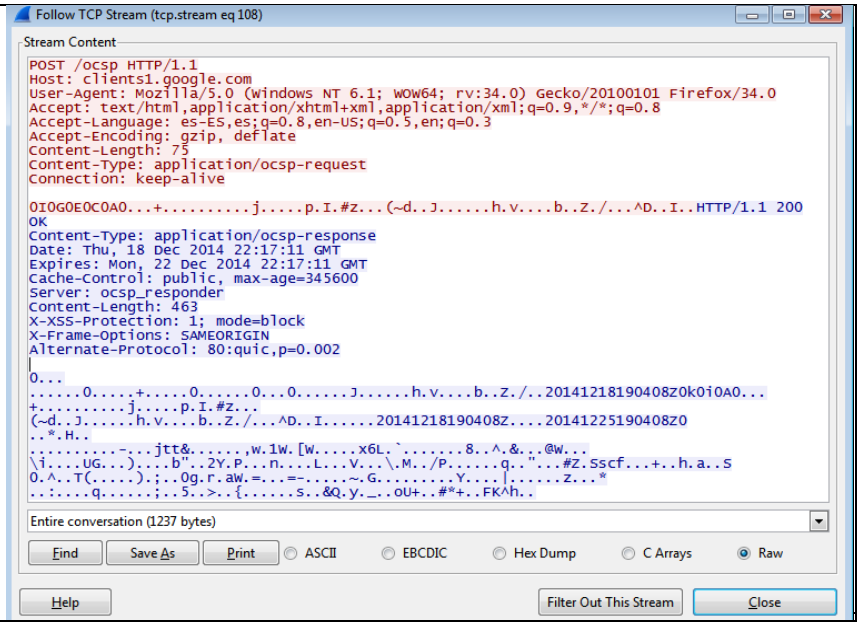
Servicios de tokens de seguridad se pueden ofrecer como servicios web, mediante el uso de interfaces de programación de aplicaciones (API), o para aplicaciones nativas en conjunción con Software Development Kits (SDKs).

La entidad incorpora en sus comunicaciones STS en la autenticación de las aplicaciones. Se utiliza en la autenticación del Portal Web y en El Sistema de Información Misional.

7. ETHICAL HACKING- ANÁLISIS DE VULNERABILIDADES

Tabla 1. Escaneo y Sniffer del Portal Web de la Entidad

Descripción de Prueba efectuada	Escaneo y Sniffer en el Portal Web: Se hace con la finalidad de interceptar datos confidenciales de los sistemas en la red. Se realiza con la herramienta Wireshark, al efectuar el usuario el logue en una sección del Portal
Vulnerabilidad	No se encontró vulnerabilidad.
Activo de Información	Portal de la Entidad
Vectores de Ataque	• Capturar información usuarios y claves. • Conocer información interna de la aplicación. • Obtener acceso a información no autorizada.
Atacante	• Anónimo desde Internet • Anónimo desde intranet
Fecha de realización	Febrero 2015
Encargado de la prueba	Hina Luz Garavito
Resultados y Evidencia	Investigando la arquitectura del Portal Web se conoce que trabaja con encriptación en sus comunicaciones con TSL Security Token Service Aplication

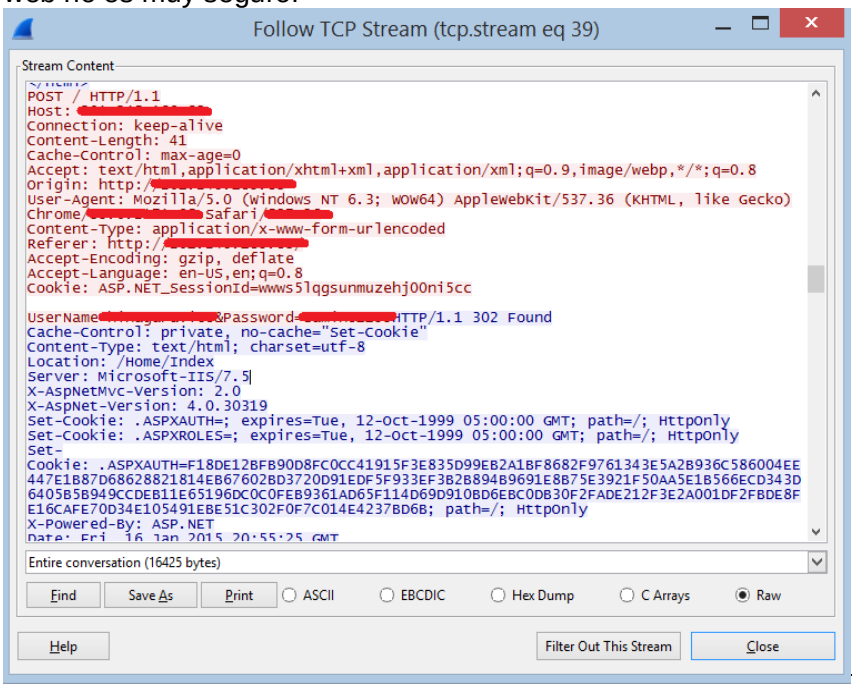


Fuente Autor

Tabla 2. Escaneo y Sniffer en Aplicativos de la Entidad con Wireshark.

Descripción de Prueba efectuada	Escaneo y Sniffer en Aplicativos de la entidad: Se realizó escaneo en el momento de realizar la autenticación el usuario en un sistema web ñAplicativo de Encuestasòy el aplicativo ARCserve para realizar Backups; con la finalidad de interceptar usuarios y claves. Se trabajó con la herramienta Wireshark y herramientas de escaneo en Kali Linux
Vulnerabilidad	Información sensible como credenciales de usuario o información administrada por los clientes es transmitida a través de un canal inseguro de información.
Activo de Información	• Aplicativo para diligenciar encuestas. • Aplicativo para realizar Backups ARCserve.
Vectores de Ataque	• Capturar información usuarios y claves. • Extraer información no permitida del sistema
Atacante	Anónimo desde Internet
Fecha de realización	Febrero 2015
Encargado de la prueba	Hina Luz Garavito

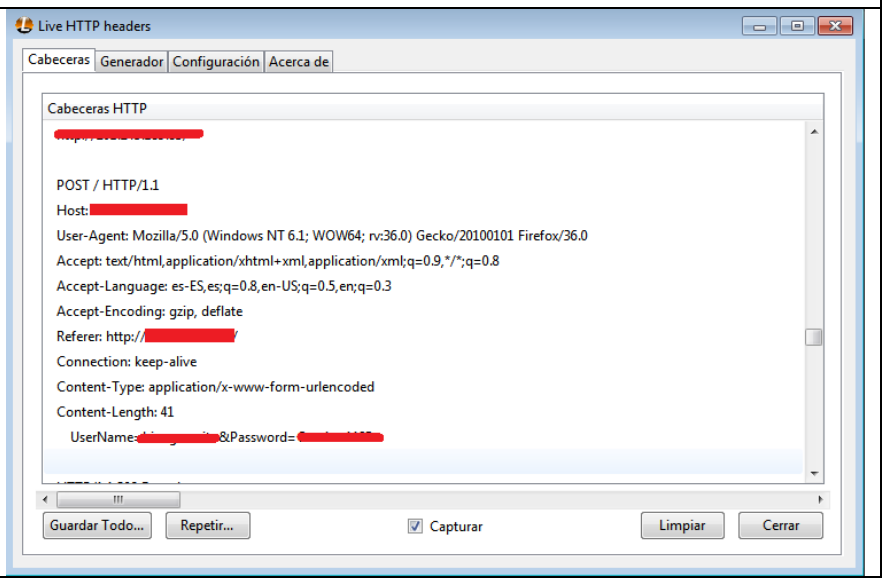
Resultados y Evidencia	Se pudo capturar un usuario y la contraseña en el Aplicativo de Encuestas, se concluyo que la información de claves no esta encriptada y es facilmente capturable. Por tal motivo el aplicativo web no es muy seguro.



Captura de contraseñas en aplicativo ARCserve Backup

Fuente Autor.

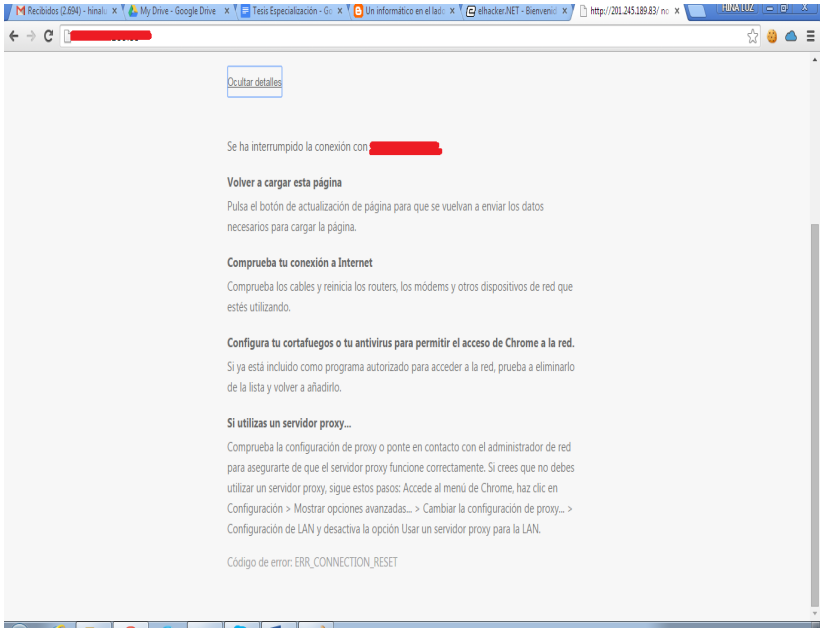
Tabla 3. Escaneo y Sniffer de Aplicativos de la Entidad con Live HTTP Headers

Descripción de Prueba efectuada	Escaneo y Sniffer de Aplicativos de la Entidad con Live HTTP Headers
Vulnerabilidad	Información de usuarios y claves es transportada por un canal inseguro, además de eso se puede presentar por desconocimiento del usuario al ver ventana activa de Live HTTP Headers e ignorarla.
Activo de Información	Aplicativo para diligenciar encuestas
Vectores de Ataque	Obtener información no permitida del sistema
Atacante	• Anónimo desde Internet • Anónimo desde intranet
Fecha de realización	Febrero 2015
Encargado de la prueba	Hina Luz Garavito
Resultados y Evidencias	

Fuente Autor.

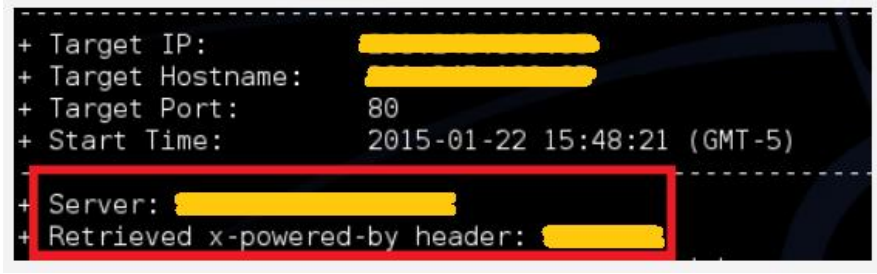
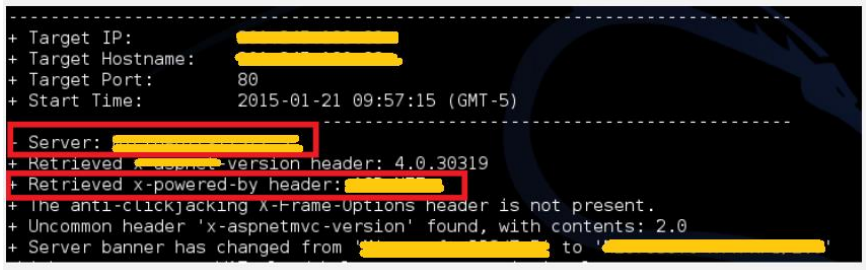
Tabla 4. Injection Sql en Aplicativos de la entidad.

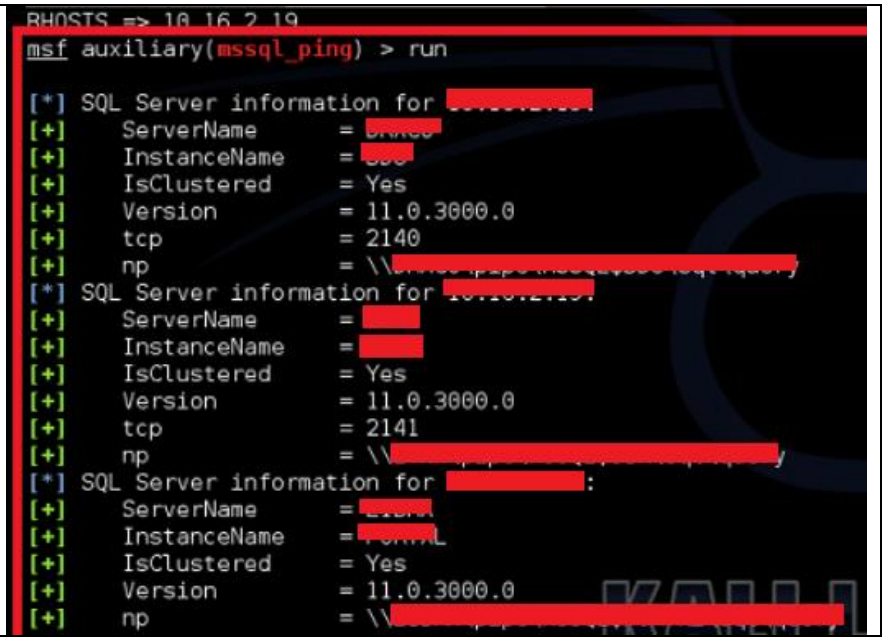
Descripción de Prueba efectuada	Se realizaron pruebas de Injection Sql en Aplicativos de la entidad: Con la finalidad de saber información acerca de las bases de datos: Se trabajaron con sentencias como: • " or "x"="x • " or "a"="a

Vulnerabilidad	No se encontró vulnerabilidad
Activo de Información	Aplicativo para diligenciar encuestas
Vectores de Ataque	Obtener información no permitida del sistema
Atacante	• Anónimo desde Internet • Anónimo desde intranet
Fecha de realización	Febrero 2015
Encargado de la prueba	Hina Luz Garavito
Resultados y Evidencia	No se pudo capturar información en la prueba de Injection Sql 

Fuente Autor

Tabla 5. Escaneo y Sniffer de servidores.

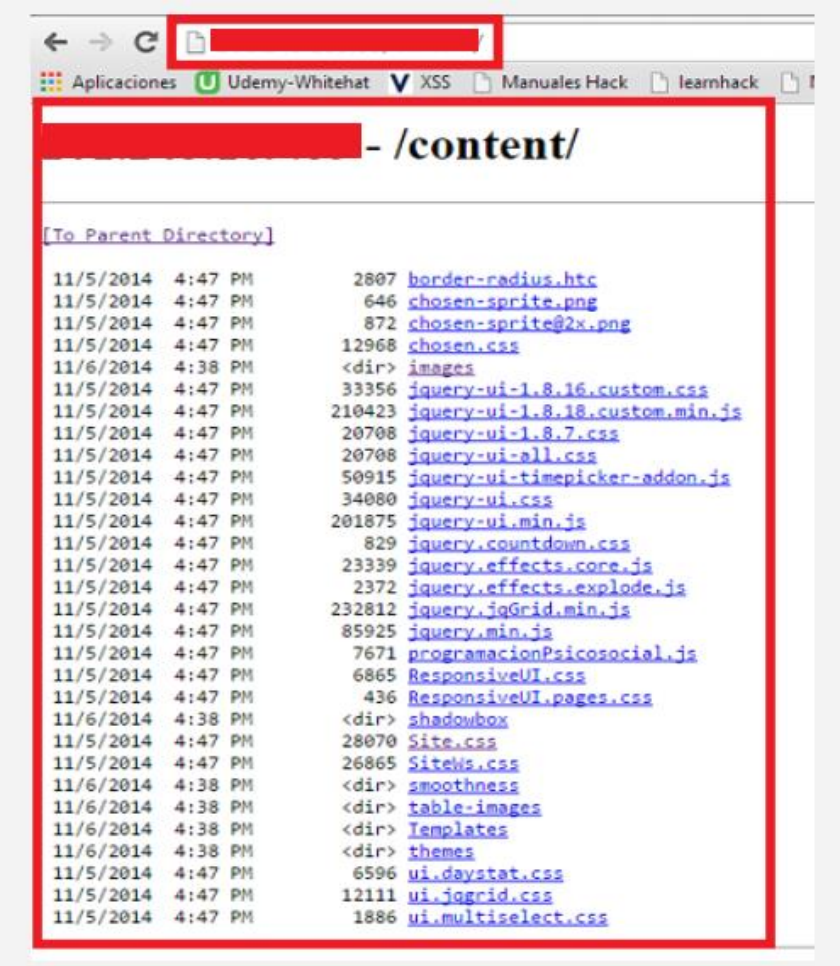
Descripción de Prueba efectuada	Escaneo y Sniffer de servidores utilizando la herramienta Kali Linux
Vulnerabilidad	Es posible conocer información técnica de los diferentes componentes tecnológicos que soportan la operación de la entidad con el fin de perfilar ataques más sofisticados.
Activo de Información	• Servidores • Aplicaciones
Vectores de Ataque	• Conocer información interna de la aplicación • Obtener acceso a información no autorizada
Atacante	• Anónimo desde Internet • Anónimo desde intranet
Fecha y duración	Febrero de 2015
Encargado de la prueba	Entidad contratada por la entidad para hacer Ethical Hacking
Resultados y Evidencia	Información de versiones de tecnologías usadas:   Información técnica sobre el servidor de base de datos, se puede visualizar las instancias creadas en las bases de datos



Fuente Autor

Tabla 6. Revisión de directorios en servidores.

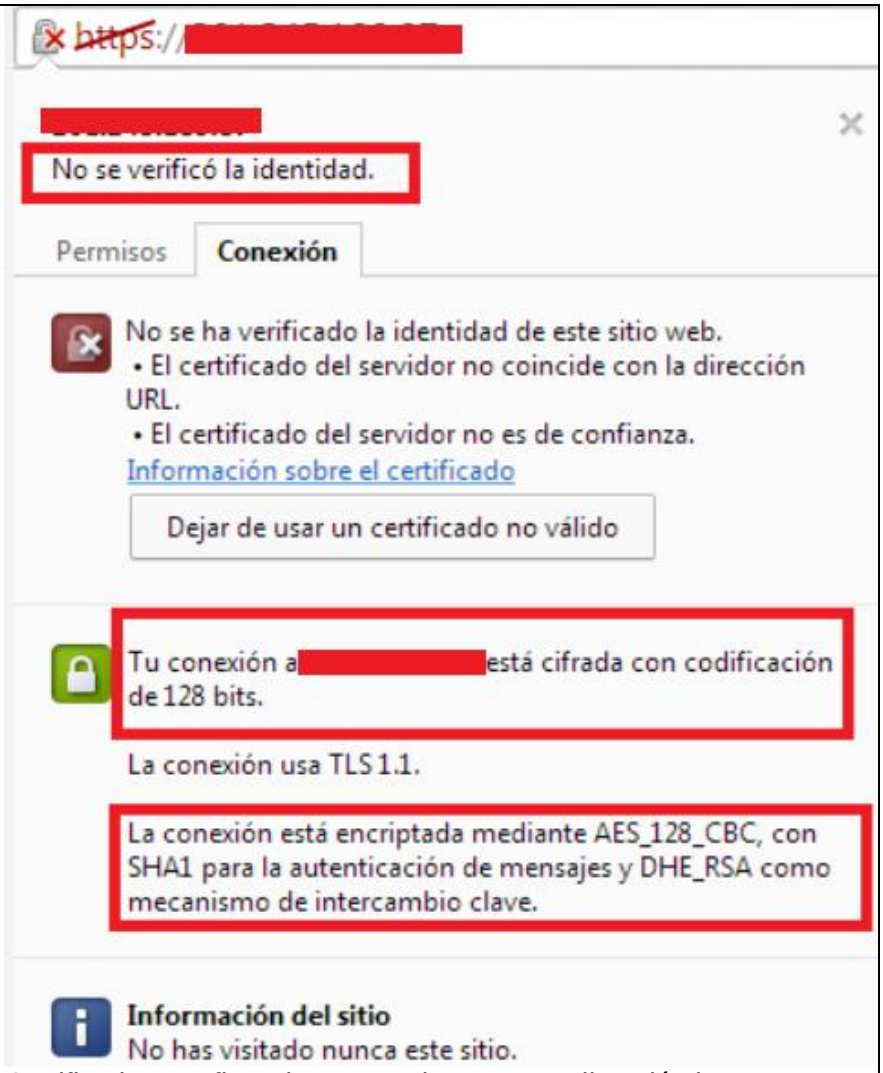
Descripción de Prueba efectuada	Revisión de directorios en servidores
Vulnerabilidad	Es posible para un atacante visualizar y acceder a directorios expuestos en el servidor
Activo de Información	Información Servidores WEB
Vectores de Ataque	• Conocer funcionamiento interno de la aplicación • Extraer información no permitida del sistema
Atacante	Anónimo desde Internet
Fecha de realización	Febrero 2015
Encargado de la prueba	Entidad contratada por la entidad para hacer Ethical Hacking

Resultados y Evidencia	Contenido en directorio almacenado en el servidor: 

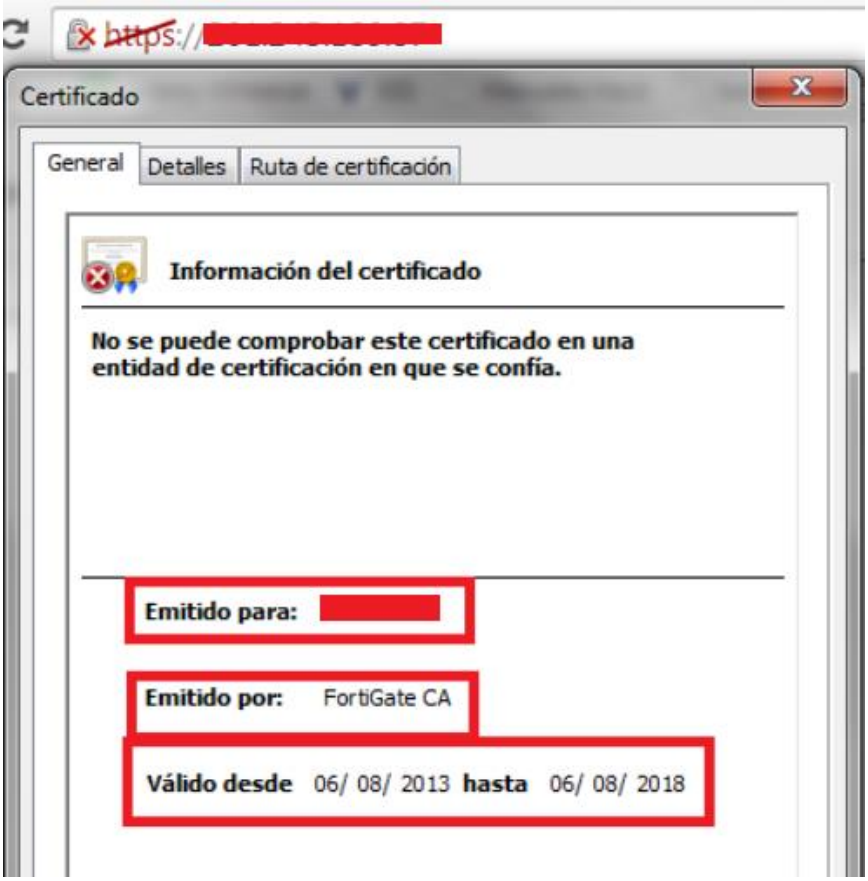
Fuente Autor.

Tabla 7. Verificación de Url de Sitios Web.

Descripción de Prueba efectuada	Verificación de Url de Sitios Web
Vulnerabilidad	Posibilidad de que un tercero pueda suplantar los sitios web afectados sin levantar sospecha en los usuarios
Activo de Información	Información Servidor WEB
Vectores de Ataque	Interceptar información sensible que transita por la red
Atacante	• Anónimo desde Internet • Anónimo desde intranet
Fecha de realización	Febrero 2015
Encargado de la prueba	Entidad contratada por la entidad para hacer Ethical Hacking
Resultados y Evidencia	Certificado con algoritmo débil y la URL no coincide con los datos validados por el certificado.

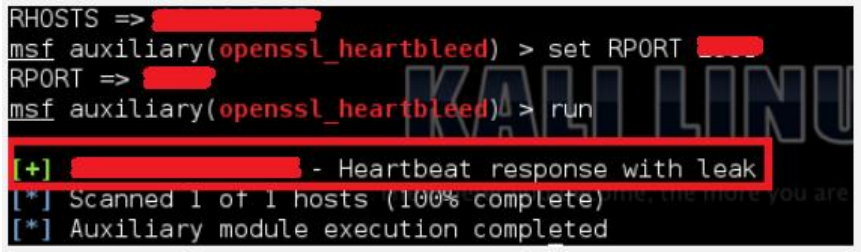


Certificado auto firmado, generado para una dirección interna y con una validez superior a 1 año



Fuente Autor.

Tabla 8. Escaneo de servidores de aplicación.

Descripción de Prueba efectuada	Escaneo de servidores de aplicación
Vulnerabilidad	La versión del protocolo TLS/SSL implementada es vulnerable ataques Change Cipher Spec injection y Heartbleed, lo cual permite a un atacante realizar ataques de Hombre en el Medio para poder secuestrar sesiones y/o obtener información sensible
Activo de Información	Información en servidores de aplicación
Vectores de Ataque	• Obtener acceso a información no autorizada • Interceptar información sensible que transita por la red
Atacante	Anónimo desde intranet
Fecha de realización	Febrero 2015
Encargado de la prueba	Entidad contratada por la entidad para hacer Ethical Hacking
Resultados y Evidencia	

Fuente Autor.

Tabla 9. Revisión de Seguridad del Sistema de Información Misional.

Descripción de Prueba efectuada	Revisión de Código Fuente en El Sistema de Información Misional para detectar vulnerabilidades
Vulnerabilidad	Se encontraron varios puntos para mejorar
Activo de Información	Sistema de Información Misional
Vectores de Ataque	• Capturar información usuarios y claves. • Conocer información interna de la aplicación • Obtener acceso a información no autorizada • Obtener información no permitida del sistema
Atacante	Anónimo desde intranet
Fecha de realización	Febrero 2015
Encargado de la prueba	Hina Luz Garavito
Resultados y Evidencia	• No hay terminación de sesión en el Sistema de Información Misional • Separación de funciones: Existe un usuario administrador en el sistema que tiene un acceso total al sistema, tiene los privilegios de funciones administrativas y además puede crear, actualizar y registrar información en los diferentes módulos • Manipulación de la información: La aplicación en algunos módulos envía información al usuario, como tasas de interés o periodos que son obtenibles de la aplicación misma, el sistema debería asegúrese que toda la información personalmente identificable no esté disponible o alcanzable desde el sistema; porque un atacante podría valerse de ello para cambiar cualquier información entregada a ellos, y por lo tanto pueden cambiar validación del lado del cliente, datos GET y POST, cookies, cabeceras HTTP, y más. • Caída del sistema por agotamiento de recursos: Se evidencia en el sistema que alguno módulos que utiliza muchos usuarios son un poco demorados al cargar o al efectuar operaciones esto se debe a que se realizan cálculos complejos, búsquedas pesadas, o consultas largas • No Existe en el sistema un módulo que permita llevar una trazabilidad de las operaciones importantes que hace el usuario es decir un módulo para realizar auditorías en el sistema.

Fuente Autor.

8. ANÁLISIS DE RESULTADOS DE LA ENCUESTA REALIZADA A LOS ENCARGADOS DE SEGURIDAD DE INFORMACION

Se realizó una encuesta de seguridad de la información a algunos empleados de la entidad: Especialista en seguridad de la información, Administrador de base de datos y Administrador de servidores. Con el objetivo de indagar e investigar cómo está la empresa a nivel de seguridad de la información en varios aspectos; el formulario respondido se encuentra en el ñAnexo A: Encuesta de análisis de seguridad de la información en la entidadò

9. ANÁLISIS DE RESULTADOS DE LA ENCUESTA DE EVALUACION DEL USO DE LA TECNOLOGÍA Y DE LOS SISTEMAS DE INFORMACIÓN A LOS EMPLEADOS DE LA ENTIDAD

Se realizó encuesta a los empleados de la entidad para evaluar que conocimientos tiene acerca de la seguridad informática en la entidad y para saber que vulnerabilidades se pueden presentar por parte de los empleados en la entidad. Se realizará análisis de estadístico de los resultados encontrados. Esta encuesta se puede visualizar en el ñAnexo Bò. A continuación describiremos lo que se deduce de las gráficas estadísticas que arroja los resultados de la encuesta:

- En la gráfica estadística de la pregunta ñA su correo institucional han llegado correos masivos de remitentes externos a la entidad?ò(ver Anexo D), se evidencia que el 52% de los Funcionarios de la Entidad reciben correos masivos de remitentes externos y el 48% no los recibe. Aspecto que afecta el buen uso de la tecnología.

- En la gráfica estadística de la pregunta ñUsted cierra la sesión de sus sistema cada vez que se levanta de su equipo?ò(ver ñAnexo Fò), se evidencia que el 52% de los Funcionarios cierra sesión en su computador de oficina y el 48% no lo hace. Este aspecto afecta el buen uso de la tecnología.

- En la gráfica estadística de la pregunta ñCómo define sus contraseñas?ò (ver ñAnexo Gò), se evidencia que el 61% de los Funcionarios define sus contraseñas como debe ser (Utiliza como mínimo 8 caracteres, que contenga letras, números y símbolos) y 39% elige una palabra corta. Lo que indica que la mayoría de los funcionarios tienen un nivel de seguridad medio en la definición de sus contraseñas.

- En la gráfica estadística de la pregunta ñEn su memoria USB, en su celular u otro dispositivo portable acostumbra a llevar copias de la información de la Oficina?ò (ver ñAnexo Hò), se evidencia que el 61% respondió ñAlgunas vecesò y el 32% ñNuncaò Este aspecto indica una mala práctica en el uso de la tecnología.

- En la gráfica estadística de la pregunta ñSi a Usted le solicitan conservar la información a través de medios que garanticen su preservación (hacer copias de seguridad de la información gestionada en la entidad), prefiere?ò(ver ñAnexo Iò), se evidencia que el 61% respondió que lo guarda en otro medio (USB, celular)

y el 29% en discos de red o carpetas compartidas. Este aspecto indica una mala práctica en el manejo de la información en la Entidad

- En la gráfica estadísticas de la pregunta ñSi crea copias de seguridad de la información de la Entidad en medios físicos como DVD, CD, USB. Donde las ubica?ò(ver ñAnexo Jò), se evidencia que el 35% prefiere guardar información en su casa y el 32% en un archivo especial destinado para ello. Este aspecto manifiesta una mala práctica en el manejo de la información perteneciente a la Entidad.

- En la gráfica estadísticas de la preguntaò Usted mantiene la información de naturaleza confidencial de la entidad en:ò(ver ñAnexo Pò) se evidencia que solo un 29% elige la carpeta Mis Documentos. Esto manifiesta una mala práctica en el uso de la tecnología en la Entidad.

10. ANÁLISIS Y EVALUACIÓN DEL RIESGO BASADO MAGERIT

10.1 DESCRIPCION DE LOS ACTIVOS

Son todos los elementos que la Entidad posee para el tratamiento de la información. Magerit diferencia los activos agrupándolos en varios tipos de acuerdo a la función que ejercen en el tratamiento de la información. A continuación describiremos los activos de la Entidad que vamos analizar en el estudio de análisis del riesgo.

10.1.1 [D] Datos / Información. Los datos que se gestionan son los del grupo de personas con el que se trabaja en la entidad y todos los servicios que se prestan, información que gestiona El Sistemas de Información Misionales:

- Base de Datos del Sistema de Información Misional
- código fuente, código ejecutable de los sistemas de información misionales
- datos de prueba de las aplicaciones

10.1.2 [HW] Equipos Informáticos. Conformado por:

- Equipos de oficina (PC, portátiles, servidores, dispositivos móviles, etc.)
- Se cuenta con los siguientes servidores de aplicaciones:
    - Servidor Sistema de Información Misional de la entidad
    - Servidor Portal
    - Servidor de BD

10.1.3 [SW] Software / Aplicativos. Programas, aplicativos, desarrollos, que han sido desarrollados para su desempeño por un equipo informático, entre ellos están: Aplicaciones propias de carácter misional, desarrollo a medida (subcontratado), estándar, el portal Web. Como también aplicaciones de software utilizadas para el desarrollo de sus sistemas tales como:

- El Portal Web de la entidad
- Sistemas de Información Misional
- Sistema de Encuestas
- Herramientas de gestión de BD*:* En la entidad se trabaja con SQL Server.
- *CA ARCserve Backup:* Aplicativo para realizar copias de seguridad

10.1.4 [Media] Soportes de información. Dispositivos físicos que permiten almacenar información de forma permanente o por largos periodos de tiempo. Ejemplo: CD-ROM, DVD, USB, Material Impreso.

10.1.5 [P] Personal. Personal relacionado con los sistemas de información; como:

- Personal interno y externo,
- Operadores,
- Administradores de sistemas
- Desarrolladores de sistemas
- Contratistas y proveedores
- Personal de soporte al usuario
- Personal de mantenimiento y soporte de los sistemas de información

10. 2 CARACTERIZACIÓN Y VALORACIÓN DE LOS ACTIVOS

La valoración de los activos debe ser lo más objetiva posible y debe involucrar en el proceso de valoración a todas las áreas de la entidad aunque no sean los encargados de realizar el Análisis del Riesgo.

El primer paso para realizar la valoración es identificar los activos de la entidad para así pasar a valorarlos. Se refiere al valor que se asigne a cada activo de acuerdo al grado de importancia en las cinco dimensiones de seguridad: la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

La metodología Magerit contempla dos tipos de valoraciones, cualitativa y cuantitativa. La primera hace referencia al de calcular un valor a través de una escala cualitativa donde se valora el activo de acuerdo al impacto que puede causar en la empresa su daño o perdida, en consecuencia la escala se refleja en:

Tabla 10. Valoración de Activos

Impacto	
Muy Alto (MA)	
Alto (A)	
Medio (M)	
Bajo (B)	
Muy bajo (MB)	

Fuente: Curso Sistema de Gestión de la Seguridad de Información SGSI, UNAD

Un punto importante para tener en cuenta en la valoración es poner en consideración las consecuencias que traería para entidad en el caso de que se materialice una amenaza para el activo.

10.2.1 Valoración Cualitativa y Cuantitativa de Activos. A continuación se realizará la valoración de los activos de la Entidad en las cinco dimensiones de seguridad (D: Disponibilidad, I: Integridad, C: Confiabilidad, A: Autenticidad, T: Trazabilidad) ver Tabla 11.

Tabla 11. Valoración Cuantitativa y Cualitativa de Activos de la Entidad

Activo	**D**	**I**	**C**	**A**	**T**
[D] Datos / Información					
Base de Datos del Sistemas de Información Misional	MA	MA	MA		
Código fuente, código ejecutable del Sistemas de Información Misional	MA	MA	MA	MA	
Datos de prueba de las aplicaciones	B	B	B	B	
[HW] Equipos Informáticos					
Servidores	MA	MA	MA		
Equipos de computo	A	A			
[SW] Software / Aplicativos					
Herramientas de gestión de BD	MA	MA	MA		
El Portal Web	MA	MA	MA	MA	
Sistemas de Información Misional	MA	MA	MA	MA	
Sistema de Encuestas	A	A	A	A	
CA ARCserve Backups		MA			
[Media] Soportes de información					
Discos, medios magnéticos		MA			
[P] Personal					
Personal de soporte al usuario	MA				
Personal de mantenimiento y soporte de los sistemas de información	MA	MA	MA		

Fuente Autor

10.3 IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

En este paso se equilibraran todas las posibles amenazas que pueden afectar en alguna de las dimensiones de seguridad un activo. Para hacer una valoración más exacta es necesario estimar la frecuencia de ocurrencia y el rango porcentual de impacto en los activos.

Tomando como base el listado de amenazas propuesto por la metodología Magerit, se procede a realizar la valoración de ellas en cada uno de los activos, es decir, determinar que amenazas los puede afectar, con qué frecuencia se puede presentar y que dimensión de seguridad puede ser afectada. Para valorar las amenazas es necesario que se estime una escala de valores que nos permita determinar el rango de frecuencia en que se puede presentar, la cual se realiza mediante estimaciones anuales, mensuales, y semanales, asignando un número de veces (ver Tabla 12).

Para valorar el nivel o frecuencia de la amenaza en cada activo, es necesario valorar también el impacto que sería en realidad el daño causado al activo en caso de materialización de una amenaza; Así mismo se podrá estimar en qué grado el activo es afectado sobre las dimensiones de seguridad que la metodología Magerit ha considerado como la Autenticidad (A), confidencialidad (C), integridad (I), disponibilidad (D) y la trazabilidad del servicio (T) (ver ñTabla 13ò).

Tabla 12. Valores de Frecuencia de Amenazas

Valor			**Criterio**
4	Muy frecuente	MF	A diario
3	Frecuente	F	Mensualmente
2	Norma	FN	Una vez al año
1	Poco frecuente	PF	Cada varios años

Fuente Magerit V.3 ï Libro II-Catálogo de Elementos

Tabla 13. Valores de degradación de amenaza.

Valor	**Criterio**	
100%	MA	Degradación MUY ALTA del activo
80%	A	Degradación ALTA considerable del activo
50%	M	Degradación MEDIANA del activo
10%	B	Degradación BAJA del activo
1%	MB	Degradación MUY BAJA del activo

Fuente Magerit V.3 ï Libro II ï Catálogo de Elementos.

10.3.1 Valoración de Amenazas. A continuación se efectuara la valoración del impacto que tendrían las amenazas para los activos de la Entidad en las cinco dimensiones de seguridad (Disponibilidad, I: Integridad, C: Confiabilidad, A: Autenticidad y T: Trazabilidad), teniendo en cuenta su frecuencia, ver Tabla 14.

Tabla 14. Valoración de amenazas de la Entidad.

Activo	**Frecuencia**	**D**	**I**	**C**	**A**	**T**
[D] Datos / Información						
Base de Datos del Sistemas de Información Misional						
[E.4] Errores de configuración	F					
[A.11] Acceso no autorizado	F					
[A.14] Interceptación de información (escucha)	F					
Código fuente, código ejecutable del Sistemas de Información Misional						
[E.21] Errores de mantenimiento / actualización de programas (software)	PF					
[HW] Equipos Informáticos						
Servidores						
[E.4] Errores de configuración	F					
[E.14] Escapes de información	F					
[A.4] Manipulación de la configuración	PF					
Equipos de computo						
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	PF					
[SW] Software/Aplicativos						
Sistemas de Información Misional						
[E.1] Errores de los usuarios	F					
[E.24] Caída del sistema por agotamiento de recursos	F					
[A.15] Modificación deliberada de la información						
Sistema de Encuestas						
[A.14] Interceptación de información(escucha)	F					
[A.11] Acceso no autorizado	F					
[Media] Soportes de información-Backups						
Discos, medios magnéticos						
[E.18] Destrucción de información	F					
[P] Personal						
Personal de soporte al usuario						

Personal de mantenimiento y soporte de los sistemas de información		
[A.30] Ingeniería social (picaresca)	F	

Fuente: Autor

10.3.1.1 Justificación de valoración de las Amenazas en Datos e Información. A continuación se menciona cada amenaza del activo y se explica el porqué de su valoración:

[E.4] Errores de configuración: En el estudio de Ethical Hacking se detectó que esta amenaza afectaba las bases de datos de la entidad, ya que debido a errores en la configuración se podía ver información técnica de ellas. En la valoración de la amenaza tiene una degradación MUY ALTA para las dimensiones de Integridad, Confidencialidad y Disponibilidad debido a que una mala configuración en los activos pertenecientes a las bases de datos de las aplicaciones informáticas llevaría a ataques como intrusión, denegación de servicios, robo de información.

[A.14] Interceptación de información (escucha): Con esta amenaza el atacante tiene acceso a información confidencial sin que la información en si misma se vea afecta en la Entidad por este motivo se le dio una valoración ALTA en la dimensión de Confidencialidad en la degradación del activo.

[A.11] Acceso no autorizado: Es consecuencia de la presencia de las amenazas [E.4] Errores de configuración y [A.14] Interceptación de información. Y tiene una valoración MUY ALTA en las dimensiones de Confidencialidad e Integridad en la degradación del activo.

[E.21] Errores de mantenimiento / actualización de programas (software): Se presenta en la entidad debido a que se hacen ajustes de desarrollo de software en las aplicaciones que quedan con fallas en el proceso o que hizo falta tener en cuenta alguna validación. Esta amenaza tiene un impacto ALTO en la Integridad de los aplicativos; pero es POCO FRECUENTE.

10.3.1.2 Justificación de valoración de las Amenazas en Equipos Informáticos. A continuación se menciona cada amenaza del activo y se explica el porqué de su valoración:

[E.4] Errores de configuración: Se presenta en los servidores de las Aplicaciones, se evidencia en el estudio de Ethical Hacking que los servidores permiten visualizar información técnica y permite a usuarios no autorizados la visualización de sus archivos de las aplicaciones que hospedan. Tiene una valoración MUY ALTA en el impacto de las dimensiones de Integridad y Confidencialidad de las aplicaciones que soporta los servidores.

[E.14] Escapes de información*:* Esta amenaza se presenta porque la configuración de los servidores permite que se intercepte información sensible que transita por la red, debido a que se manejan protocolos de comunicación como TLS/SSL que no son tan seguros. Tiene una valoración MUY ALTA en las dimensiones de Integridad y Confidencialidad de los Servidores.

[A.4] Manipulación de la configuración: Es consecuencia de la presencia de las amenaza [E.4] Errores de configuración que permiten a un usuario no autorizado manipular la configuración de los servidores. Tiene una valoración MUY ALTA en la dimensión de Integridad de los Servidores.

[E.23] Errores de mantenimiento / actualización de equipos (hardware): Esta amenaza se puede presentar en los equipos de cada usuario, es POCO FRECUENTE. Tendría un impacto ALTO en la dimensión Disponibilidad de los Equipos Informáticos

10.3.1.3 Justificación de valoración de las Amenazas en Software y Aplicativos. A continuación se menciona cada amenaza del activo y se explica el porqué de su valoración:

[A.14] Interceptación de información (escucha): Se presenta porque algunos sistemas como el de Encuestas de la entidad no maneja un cifrado en él envió de sus claves de usuario. Por lo que se puede prestar para que una atacante intercepte esta información. Tiene una valoración MUY ALTA en la dimensión de Confidencialidad de la información que maneja el aplicativo.

[A.11] Acceso no autorizado: Es consecuencia de la presencia de la amenaza [A.14] Interceptación de información y tiene una valoración MUY ALTA en la dimensión

de Confidencialidad de la información que maneja el aplicativo de Encuestas de la entidad.

[E.24] Caída del sistema por agotamiento de recursos: Se presenta en el Sistema de Información Misional cuando se realizan procesos que son algo demorados y muchos usuarios lo utilizan. Tiene una valoración ALTA en la Dimensión de Disponibilidad del Sistema Información Misional

[E.1] Errores de los usuarios: Se presenta cuando los usuarios realizan ingreso de información incorrecta en el Sistema de Información Misional. Tiene una valoración MEDIA en la dimensión de Integridad del Sistema de Información Misional.

[A.15] Modificación deliberada de la información: Se presenta debido a que existen en el Sistema de Información Misional existen usuarios Administradores que tiene un acceso total al sistema, tiene los privilegios de funciones administrativas y además puede crear, actualizar y registrar información en los diferentes módulos. Tiene una valoración ALTA en la dimensión de Integridad del Sistema de Información Misional.

10.3.1.4 Justificación de valoración de las Amenazas en Soportes de Información. A continuación se menciona cada amenaza del activo y se explica el porqué de su valoración:

[E.18] Destrucción de información: Se presenta cuando hay destrucción o daño de la información de los Sistemas de Información y la copia de seguridad de esta información no se encuentra o no se puede recuperar y esto se puede presentar frecuentemente debido a que no hay procedimientos debidamente documentados de los procesos de realización y recuperación de Backups. Tiene una valoración MUY ALTA en las dimensiones de Integridad y Disponibilidad de la Información del Sistema de Información.

10.3.1.5 Justificación de valoración de las Amenazas en Personal. A continuación se menciona cada amenaza del activo y se explica el porqué de su valoración:

[A.30] Ingeniería social (picaresca): Tiene que ver por concientización del personal en las mejores prácticas de seguridad informática. Es POCO FRECUENTE pero tiene un valor MUY ALTO en las dimensiones de Confidencialidad con la Información de la entidad.

10.4 SALVAGUARDAS DE LOS ACTIVOS

En la evaluación de los salvaguardas se mide la eficacia de las salvaguardas existentes en relación al riesgo que afrontan y se identifican las dimensiones de seguridad afectadas ([A] Autenticidad, [C] Confiabilidad, [D] Disponibilidad, [T] Trazabilidad, [I] Integridad).

Tabla 15. Valoración de Salvaguardas Existentes en la Entidad.

Activo	Salvaguardas	Dimensión	Evaluación
[D] Datos / Información • Base de Datos del Sistemas de Información Misional • Código fuente, código ejecutable del Sistemas de Información Misional	SW.A Copias de seguridad (Backups)	[I], [D]	50%
[HW] Equipos Informáticos • Servidores • Equipos de computo	H.tools.IDS IDS/IPS: Herramienta de detección/prevención de intrusión	[I], [C], [D]	70%
	H.tools.TM Herramienta de monitorización de tráfico	[I], [C], [D]	70%
[SW] Software/Aplicativos • Sistemas de Información Misional • Sistema de Encuestas	COM Protección de las Comunicaciones	[I], [C], [D], [A]	60%
	SW.A Copias de seguridad (backup)	[I], [D]	50%
[Media] Soportes de información-Backups Discos, medios magnéticos	SW.A Copias de seguridad (backup)	[I], [D]	50%
[P] Personal	PS Gestión del Personal	[C]	40%

• Personal de soporte al usuario • Personal de mantenimiento y soporte de los sistemas de información

Fuente Autor.

10.4.1 Descripción salvaguardas activos Datos /Información. Actualmente en la Entidad se trabaja con la salvaguarda de SW.A Copia de seguridad (Backup) para el activo Datos e Información, realizando copias de seguridad Full semanales y diferenciales diariamente en la entidad. Sin embargo no existe documentación de los procedimientos para realizar y restaurar copias de seguridad; como tampoco se considera la posibilidad de encriptar la información de las cintas de copias de seguridad. Por estos motivos el procedimiento de copias de seguridad no está muy bien consolidado en la entidad y la evaluación como salvaguarda es baja.

10.4.2 Descripción salvaguardas de activos Equipos Informáticos. A continuación describiremos las salvaguardas que existen actualmente en la Entidad para el activo de Equipos Informáticos:

- H.tools.IDS IDS/IPS: Herramienta de detección/prevención de intrusión: En la entidad se maneja IPS(Controlador de Tráfico) que permite controlar el acceso en una red de computadores para protegerla de ataques y abusos. En la entidad tienen buenas herramientas para el control pero debe hacerse mejor uso de ellas o mejor configuración de ellas. Por tal motivo la evaluación como salvaguardas es aceptable.

- H.tools.TM Herramienta de monitorización de tráfico: En la entidad se trabaja con la herramienta de Monitoreo de red (Solar Winds) que provee de una completa plataforma para la administración de fallas y monitorización de desempeño que permite al área de Tecnologías de la información recolectar información y ver la disponibilidad de cada uno de los componentes de su infraestructura tecnológica. Sin embargo un eficiente manejo y configuración de la herramienta. Por tal motivo tiene una valoración aceptable como salvaguarda

10.4.3 Descripción salvaguardas de activos Software y Aplicativos. A continuación describiremos las salvaguardas que existen actualmente en la Entidad para el activo de Software y Aplicativos:

- COM Protección de las Comunicaciones: La seguridad en las comunicaciones de la entidad está basada en TLS/SSL Security Token Service. Pero esta tiene sus debilidades ya permite a un atacante obtener acceso a información no autorizada e interceptar información sensible que transita por la red. Por tal motivo tiene una evaluación como salvaguardas aceptable.

- SW.A Copias de seguridad (backup): En la entidad se maneja un (1) Backup del código fuente que es actualizado constantemente en un servidor más no en cintas de copias de seguridad. Por tal motivo la evaluación de la salvaguarda es aceptable

10.4.5 Descripción salvaguardas activos Soporte de Información- Backups. Actualmente en la entidad se trabaja con la salvaguarda SW.A Copias de Seguridad (Backup) para el activo de Soporte de Información-Backup, realizando copias de seguridad de las bases de datos y del código fuente de las aplicaciones. Sin embargo estos procedimientos no están bien definidos ni bien documentados, ni tampoco hay un plan de contingencia. Por tal motivo la evaluación de los salvaguardas es baja.

10.4.6 Descripción salvaguardas activos Personal. Actualmente en la Entidad se trabaja con la salvaguardas PS Gestión del Personal en el activo Personal, para la selección del ingreso del personal de trabajo se realiza un buen filtro con la finalidad de contratar personal con Ética Profesional. Sin embargo no se ha capacitado a las personas en los temas de seguridad informática. Por este motivo la evaluación de la salvaguarda es bajo.

10.5 ESTIMACIÓN DEL IMPACTO

El impacto es el daño que se origina sobre el activo derivado de la materialización de una amenaza. Teniendo la valoración de los activos y el porcentaje de degradación que causan las amenazas, se deriva el impacto que tienen sobre los

activos de la Entidad (ver Tabla 16). La estimación de impactos de estos porcentajes se hace en función de varios factores, como son:

- La ejecución de una amenaza puede de perjudicar a todo un recurso de información o solo a una parte del mismo.

- Ante la materialización de una amenaza perjudica a partes claves o partes dependientes del recurso de información

- Si la amenaza, una vez perpetrada, tiene consecuencias de forma temporal o de forma permanente hacia el recurso.

Las consecuencias indirectas que traen los impactos, pueden ser cualitativas o cuantitativas, como pérdidas económicas, pérdida de inversión en el mercado o que los posibles clientes tengan una imagen negativa de la empresa Se puede llegar a establecer una proporción entre las consecuencias de los ataques y la cantidad de salvaguardas necesarias.

Se debe tomar en cuenta, también, la posible frecuencia de ocurrencia de realización de las amenazas; esto es especialmente cuando el daño causado por un ataque pequeño, pero el efecto global de muchas ataques en el tiempo, puede dar lugar a considerables pérdidas o daños.

El Impacto Acumulado es el impacto potencial al que está expuesto el sistema tomando como base los valores obtenidos de los activos y valoración de las amenazas, sin tener en cuenta las salvaguardas actuales. Estos requieren atención inmediata.

El Impacto Residual es el resultado de combinar el valor de los activos, la valoración de las amenazas y la efectividad de las salvaguardas aplicadas; los activos con resultado muy bajo o bajo (o casillas en blanco), son riesgos con los que se puede convivir pero que se tuvieron en cuenta dentro de los controles, políticas de seguridad y recomendaciones.

Tabla 16. Valores Estimación de Impacto.

		Degradación				
Impacto		1%	10%	50%	80%	100%
	MA	M	A	A	MA	MA
	A	B	M	M	A	A
	M	MB	B	B	M	M

	B	MB	MB	MB	B	B
	MB	MB	MB	MB	MB	MB

Fuente: Magerit V.3- Libro II ï Catalogo de Elementos

A continuación analizará el Impacto Acumulado y el Impacto Residual para cada uno de los activos de la Entidad en las cinco dimensiones de seguridad (D: Disponibilidad, I: Integridad, C: Confiabilidad, A: Autenticidad, T: Trazabilidad), ver Tabla 17.

Tabla 17. Valoración del impacto en activos de la entidad.

ACTIVO/ AMENAZA	**Impacto Acumulado**					**Impacto residual**				
[D] Datos / Información	**D**	**I**	**C**	**A**	**T**	**D**	**I**	**C**	**A**	**T**
Base de Datos del Sistemas de Información Misional										
[E.4] Errores de configuración										
[A.11] Acceso no autorizado										
[A.14] Interceptación de información (escucha)										
Código fuente, código ejecutable del Sistemas de Información Misional										
[E.21] Errores de mantenimiento/ actualización de programas (software)										
[HW] Equipos Informáticos										
Servidores										
[E.4] Errores de configuración										
[E.14] Escapes de información										
A.4] Manipulación de la configuración										
Equipos de computo										
[E.23] Errores de mantenimiento/ actualización de equipos (hardware)										
[SW] Software/Aplicativos										
Sistemas de Información Misional										
[E.1] Errores de los usuarios										
[E.24] Caída del sistema por agotamiento de recursos										
[A.15] Modificación deliberada de la información										
Sistema de Encuestas										
[A.14] Interceptación de información(escucha)										
[A.11] Acceso no autorizado										

[Media] Soportes de información-Backups									
Discos, medios magnéticos									
[E.18] Destrucción de información									
[P] Personal									
Personal de soporte al usuario									
Personal de mantenimiento y soporte de los sistemas de información									
[A.30] Ingeniería social (picaresca)									

Fuente: Autor

10.6 ESTIMACIÓN DEL RIESGO

Para la estimación del riesgo se toman los valores de la frecuencia de ocurrencia de cada amenaza frente a los activos e impacto acumulado ya que estos son los activos que necesitan una acción urgente, teniendo en cuenta la tabla de valoraciones (Tabla 18), los resultados de la estimación del riesgo se pueden visualizar en la Tabla 19.

Tabla 18. Criterios de valoración para estimación de riesgo.

Riesgo		**Frecuencia**			
		PF	FN	F	MF
Impacto	MA	M	A	MA	MA
	A	B	A	MA	MA
	M	B	M	A	A
	B	MB	B	M	A
	MB	MB	MB	B	B

Fuente Magerit V.3- Libro II ï Catalogo de Elementos

.

Tabla 19. Valoración del Riesgo en Activos de Información de la Entidad.

Activo	**Amenaza**	**Impacto**					**F**	**Riesgo**
		D	**I**	**C**	**A**	**T**		
[D] Datos / Información								
Base de Datos del Sistemas de Información Misional								
	[E.4] Errores de configuración							
	[A.11] Acceso no autorizado							
	[A.14] Interceptación de información (escucha)						F	MA

Código fuente, código ejecutable del Sistemas de Información Misional				
[E.21] Errores de mantenimiento/ actualización de programas (software)				
[HW] Equipos Informáticos				
Servidores				
[E.4] Errores de configuración				
[E.14] Escapes de información			F	MA
A.4] Manipulación de la configuración				
Equipos de computo				
[E.23] Errores de mantenimiento/ actualización de equipos (hardware)				
[SW] Software/Aplicativos				
Sistemas de Información Misional				
[E.1] Errores de los usuarios			F	A
[E.24] Caída del sistema por agotamiento de recursos			PF	B
[A.15] Modificación deliberada de la información			F	A
Sistema de Encuestas				
[A.14] Interceptación de información(escucha)			F	MA
[A.11] Acceso no autorizado			F	MA
[Media] Soportes de información-Backups				
Discos, medios magnéticos				
[E.18] Destrucción de información			F	MA
[P] Personal				
Personal de soporte al usuario				
Personal de mantenimiento y soporte de los sistemas de información				
[A.30] Ingeniería social (picaresca)			F	MA

Fuente: Autor.

10.7 INTERPRETACIÓN DE LOS RESULTADOS

Efectuando el análisis de los resultados expuestos en la Tabla 19, se puede concluir las siguientes observaciones:

- La entidad posee protocolos de comunicación que permite la interceptación de datos sensibles y los accesos no autorizados.

- El procedimiento de copias de seguridad no existen los procedimiento documentados tanto para hacer copias de seguridad como para restaurarlas y no hay seguridad de que los procedimientos que actualmente se trabajan sea los más eficientes. Como tampoco se ha mirado la posibilidad de cifrar las copias de seguridad para el caso de que haya un robo de la información.

- No existe capacitaciones en la entidad para crear concientización en la seguridad de la información con sus funcionarios.

- El usuario comete a menudo errores en el ingreso de los datos en el Sistema de Información de la entidad y no existe un módulo de Auditoria donde quede registro de la las operaciones importantes que efectúa el usuario en el sistema y que permita a la entidad llevar una trazabilidad de dichas operaciones.

- En el Sistema de Información Misional de la entidad puede existir manipulación deliberada de la información debido a que existe usuarios ñAdministradores del Sistemaò que tiene un acceso total, tiene los privilegios de funciones administrativas y además puede crear, actualizar y eliminar información en los diferentes módulos. Además algunos de estos usuarios están encargados de corregir datos en el sistema por solicitud de los mismos funcionarios que manejan los módulos cuando ingresan mal la información.

10.8 ESTABLECIMIENTO DE CONTROLES

Teniendo encuenta la investigación realizada, se recomienda los siguientes controles para los Servidores de Aplicaciones de la Entidad:

- Utilizar protocolos de comunicación que cifre los datos para su transporte como HTTPS, la información sensible debe ser transportada bajo un canal seguro.

- El encargado de la configuración debe propender siempre por ocultar información sensible de las aplicaciones para que un atacante no se valga de esta para preparar un ataque más elaborado.

- El encargado de la configuración debe eliminar los metadatos de archivos deben antes de ser compartidos con un tercero o hacerlos públicos.

- En Encargado de la configuración debe deshabilitar las funciones inseguras de un servicio y la opción de visualizar los directorios alojados en el servidor.

- El encargado de la configuración restringir el acceso a objetos del sistema que tengan contenido sensible. Sólo permitirá su acceso a usuarios autorizados.

- Se deben Implementar certificados digitales generados por una entidad certificadora externa válida para aplicaciones, con un tiempo de vigencia no mayor a un año y llaves públicas de 2048 bits.

- La Entidad no debe utilizar certificados digitales con una vigencia superior a un año

- Se debe deshabilitar el soporte para todas las versiones de SSL, solo utilizar el protocolo TLS para HTTPS

- Los componentes provistos por terceros en la entidad deben corresponder a versiones estables, probadas y actualizadas.

Se recomiendan los siguientes controles en el proceso de realizar Copias de Seguridad o Backups:

- Se deben crear estrategias de Backup y recuperación para los activos más importantes y sensibles para la entidad basándose en la evaluación del riesgo.
- Se deben establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo para realizar copias de seguridad y realizar pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.[10]

- Se debe decidir y establecer el tipo de almacenamiento, soporte a utilizar, aplicación de Backup, frecuencia de copia y prueba de soportes.

- Aplicar técnicas de cifrado a copias de seguridad y archivos que contengan datos sensibles o valiosos (está ampliamente relacionado con el objetivo de hacer una copia de seguridad).

Se recomiendan los siguientes controles para Sistema de Información Misional:

- Separación de funciones en los controles de acceso de los usuarios en el Sistema de Información Misional. Debe existir un Administrador con privilegios de funciones administrativas, los usuarios que crean y actualizan información en los diferentes módulos, como también usuario con los privilegios de poder realizar correcciones a la información ingresada por otros usuarios (se debe evitar que exista un Administrador con la capacidad de editar y eliminar información registrada por otros usuarios)

- Implantar un módulo de Auditoria en el Sistema de Información Misional que permita que cumpla con las siguientes características:

    - Auditable en todas las actividades que afectan el estado de un usuario que sean formalmente rastreables. Debe quedar registrado en que módulo se cambió de estado, en qué fecha, que persona realizo las actualización.

[10] 12. Seguridad en la Operativa (Copias de Seguridad). En línea: http://www.iso27000.es/iso27002_12.html

- Trazable para que sea posible determinar dónde ocurre cada actividad en cada uno de sus módulos y poder visualizar reportes.

- Alta integridad en los Log de auditoria, estos registros no pueden ser sobrescritos o modificados por ningún usuario.

Se recomienda realizar Plan de Contingencia para la Entidad que permita:

- Contar con una estrategia planificada compuesta por un conjunto de procedimientos que garanticen la disponibilidad de una solución alterna que permita restituir rápidamente los sistemas de información de la Entidad ante el eventual daño o siniestro que paralice parcial o totalmente los sistemas.

- Garantizar la continuidad en los procesos de elementos críticos necesarios para el funcionamiento de las aplicaciones de misión Entidad.

- Identificar las acciones que se deben llevar a cabo y los procedimientos a seguir en el caso de la presencia de un daño o siniestro que restrinja el acceso a los sistemas de información.

- Establecer las secuencias que se han de seguir para organizar y ejecutar las acciones de control de emergencias.

- Minimizar las pérdidas asociadas a la presencia de un daño relacionado con la gestión de los datos. Proveer una herramienta de prevención, mitigación, control y respuesta a posibles contingencias generadas en la ejecución del proyecto.

11. CONCLUSIONES

Como resultado de este proyecto se obtiene la evaluación del riesgo de los activos analizados en la Entidad, la evaluación de las salvaguardas actuales como controles para mitigar ese riesgo y la propuesta de nuevos controles en los activos para los cuales las salvaguardas existentes no son las más indicadas.

Aplicar la metodología Magerit para el análisis de riesgo es el primer paso para garantizar la seguridad de los activos de información y el normal funcionamiento interno de la entidad.

Los controles resultados de este análisis de riesgos pueden ser tomados como soporte para la implementación del SGSI; encaminado a incrementar la confiabilidad, integridad y disponibilidad de la información.

En los procedimientos para analizar el riesgo fue de gran importancia el estudio de Ethical Hacking que se pudo realizar a la infraestructura tecnológica y a los Sistemas de Información de la Entidad; le siguen en orden de importancia las entrevistas a los administradores de la seguridad y de los servicios y la encuesta para evaluar las buenas prácticas en tecnología de todos los empleados de la entidad.

Los controles de seguridad de la información buscan disminuir el riesgo actual a su nivel mínimo. La entidad actualmente presenta un nivel de riesgo informático considerable, que con el apoyo de las directivas y de todo el personal es posible contrarrestar.

Se recomoienda a la Entidad utilizar protocolos de comunicación que cifre los datos para su transporte como HTTPS, la información sensible debe ser transportada bajo un canal seguro.

Se recomienda a la Entidad la separación de funciones en los controles de acceso de los usuarios en el Sistema de Información Misional como también que se implemente un módulo de Auditorías que permita determinar en dónde ocurre cada actividad en cada uno de sus módulos y poder visualizar reportes de trazabilidad

Se recomienda a la Entidad realizar Plan de Contingencia que permita identificar las acciones que se deben llevar a cabo y los procedimientos a seguir en el caso de la presencia de un daño o siniestro que restrinja el acceso a los sistemas de información

BIBLIOGRAFIA

FABIÁN DÍAZ, Andrés y COLLAZOS, Gloria Isabel. Implementación de un SGSI en la comunidad de Nuestra Señora de Gracia, alineado tecnológicamente con la norma ISO 27001. En línea: http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf. 2012.

AMAYA TARAZONA, Carlos Alberto y SUAREZ SIERRA, Lorena Patricia. Curso de Sistema de Gestión de la Seguridad de Información SGSI. Bogotá. UNAD, 2013.

El Portal de ISO 27001 en Español. En línea: http://www.iso27000.es/

GONZÁLEZ BARROSO, Jesús. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid. Ministerio de Hacienda y Administraciones Públicas. Libro I de la metodología Magerit ofrece los lineamientos necesarios en el Proceso de Gestión de Riesgos dentro de un marco de trabajo para administrar los riesgos derivados del uso de tecnologías de la información. 2012.

--------. Guía de Técnicas. Madrid. Ministerio de Hacienda y Administraciones Públicas. Libro III de la metodología Magerit describe las técnicas usadas para hacer el Análisis de riesgos. 2012.

--------. Catálogo de Elementos. Madrid. Ministerio de *Hacienda y* Administraciones Públicas. (v.3.0): Metodología de análisis y Gestión de riesgos los sistemas de información. Libro número II de la metodología MAGERIT, estandariza los elementos objeto de proyecto de análisis necesarios para generar un inventario de activos, para luego hacer la administración de estos. 2012.

ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información. En línea: http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

INTECO (Instituto Nacional de Tecnologías De La Comunicación). Fases para la Implantación de un SGSI. En línea: http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Fases_SGSI/

JOAN, Ayerbe. Porque un plan director de seguridad. En línea: http://blog.s21sec.com/2007/12/por-qu-un-plan-director-de-seguridad.html. 2007

MINTIC (Ministerio de Tecnologías de la Información y de las Telecomunicaciones). Ley 1273 de 2009. En línea: http://www.mintic.gov.co/portal/604/w3-article-3705.html

PORTAL ADMINISTRACIÓN ELECTRÓNICA. Magerit v3: Metodología de Análisis y Gestión de Riesgos de los sistemas de información. En línea: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VCmVZhZRVJQ

FERRER, Rodrigo. Metodología de análisis del riesgo. En línea: http://www.sisteseg.com/files/Microsoft_Word_-_METODOLOGIA_DE_ANALISIS_DE_RIESGO.pdf

UNIVERSIDAD CARLOS III DE MADRID. Análisis del riesgo dentro de una auditoria informática: pasos y posibles metodologías. En línea: http://e-archivo.uc3m.es/bitstream/handle/10016/16802/PFC_Carmen_Crespo_Rin.pdf?sequence=1

Anexo A. Encuesta De Análisis De La Seguridad De La Información En La Entidad

Pregunta	Respuesta
Navegación Web	
¿A través de que contralan la navegación en internet (un servidor proxy, un Router o un Firewall)?	FIREWALL
¿Cuáles son los responsables que tienen acceso a determinar quiénes pueden acceder a navegar por internet?	El administrador de la seguridad
¿A que sitios web pueden tener acceso los usuarios y cuáles son las caracterizaciones de los sitios web?	Existen las siguientes categorías: • Responsabilidad potencial: Abuso Infantil, discriminación, violencia, grupos extremos • Contenido para adultos: Aborto, Alcohol, drogadicción, educación sexual, pornografía etc. • Alto consumo de ancho de banda: Almacenamiento masivo, descarga de software, *Streaming.* • Riesgos de seguridad: Sitios web maliciosos, *Phishing*, *Spam* • Interés General personal: Publicidad arte, entretenimiento, Investigación, Educación, redes sociales • Interés General de Negocios: Paginas financieras, paginas gobierno, entidad • Paginas no clasificadas.
¿Documentar el método para reportar que está navegando en la web, a quien se entregan los reportes y con qué frecuencia	La herramienta firewall genera un reporte y seguimiento de usuarios.
¿Todos los empleados están conscientes de las políticas de navegación web?	Se tiene planeado hacer campañas de sensibilización

¿Es una política de empresa no bajar los controles ActiveX sin firmar a menos que sean aprobadas por el área de Seguridad de Información?	Están restringidas las descargas. Esto se controla directamente en la misma maquina en el sistema operativo Windows a través del directorio activo
¿Cuáles son las reglas para definir una contraseña de usuario?	• 8 Caracteres • Deben estar conformadas por letras, números y caracteres. • Mayúsculas y minúsculas • No repetir las ultimas 10 contraseñas
Backup	
Documentar qué información necesita ser respaldada, la frecuencia con la que debe ser respaldada, y el plazo en que debe mantenerse.	No existe documentación
¿Se realizan backup semanalmente a la información del Sistemas de Información Misional?	Se realizan Copia de seguridad Full semanales y diferenciales diariamente
¿Existe documentación de los pasos para restaurar una copia de seguridad?	No
Se ha considera la posibilidad de encriptar las cintas de copias de seguridad a fin de que los datos no puedan recuperarse si se pierden o se los roban.	No
Que procedimiento se utilizan a nivel de seguridad de la información en las bases de datos:	• Definición de permisos exactos a nivel de dominio • Cada servicio de cada instancia tiene un usuario definido • Se definen grupos de dominio y se asigna permios a nivel de grupos de dominio.
Plan de Contingencia	
Existe algún plan de contingencia debidamente documentada	No
Físicos	
¿Hay UPS y generadores en el lugar?, ¿Estos son los suficientes buenos, en caso de irse la energía cuanto tiempo podrían	1 Hora con plena carga. No hay planta.

estos mantener los equipos informáticos funcionando?	
¿Qué clase de protección contra incendios que el centro de datos y sala de servidores?	Existen extintores para fuego.
Pc y portátiles	
¿Desarrollan políticas para el uso de los dispositivos USB extraíble?	No existen restricciones para utilización de USB
¿Ejecutar antivirus y anti-spyware en todos los equipos pc o portátilesô	Se ejecuta agente antivirus constantemente. Se actualiza los clientes de antivirus constantemente contra una consola central
¿Desarrollan un procedimiento para garantizar que los pc y portátiles han instalado los últimos parches?	Se actualizan a través de un servicio centralizado de Microsoft
¿Mantienen registros detallados de la actividad del usuario, en concreto, la hora de conexión, la duración y el lugar desde donde ha entrado en él?	Existen registros de actividades por plataforma o sistema de información.
Acceso Remoto	
¿Se controla el acceso dial-up (RAS) y VPN de acceso remoto. Sólo establecer permisos para los que verdaderamente lo necesitan?	Si
¿Qué controles de seguridad se utilizan en las conexiones VPN (MR)?	• Autenticación centralizada a través de directorio activo • Acceso a través de Firewall perimetral • Para algunos usuarios críticos se tiene autenticación adicional por certificados digitales (ejemplo proveedores)
¿Se documentan las políticas de la empresa sobre acceso remoto?	No existen políticas para el acceso remoto
¿Se aplica algún método para garantizar que los clientes a través de la conexión de acceso remoto tengan un buen antivirus y parches instalados para evitar que se infecten los sistemas de la empresa?	Se realiza a través de un agente VPN que se instala en el equipo remoto (se instala la primera vez)

¿Considere la posibilidad de utilizar tokens como un método de autenticación secundario para el acceso remoto. De esta forma, si un nombre de usuario y contraseña son robados, que todavía no se puede utilizar para tener acceso a la red sin el token?	Si
Servidores, router, and switches	
¿Cada cuánto se ejecuta software antivirus sobre los servidores?	Se realiza un escaneo completo cada 8 días. Y el antivirus siempre está corriendo por si ocurre alguna amenaza.
¿Asegurar que los servidores, routers y switches tienen los últimos parches instalados?	Se actualizan los parches cada mes
¿Cómo se efectúa el Registrar los log de estos dispositivos a un servidor central de registro?	Los log se trabajan con la herramienta SIEM, que maneja el Log de operaciones del sistema operativo Windows. Con la herramienta LEM de Solar Wind (correlacionador de eventos), registra todos los logs, si hay una alerta critica la notifica al correo. Las alertas críticas están relacionadas con caída de un servicio, llenado de un disco duro, problemas de memoria, alta ocupación del procesador.
¿Ejecutan el software de supervisión de la ejecución de manera que puede recibir avisos si algo anormal sucede en los servidores o la red. Muchas veces, esto puede ser una indicación de una violación a la seguridad o de otro problema crítico?	Con la herramienta LEM se envía alertas de intrusiones de usuarios no autorizados
¿Quién es el administrador de acceso de estos dispositivos y con qué frecuencia se cambia la contraseña?	El administrador de servidores. Las contraseñas se cambian cada mes.
¿Cuáles son los privilegios y qué método de acceso se dará a los proveedores de acceso que necesitan para apoyar y / o	Se les limita el acceso a cada proveedor, permitiéndole ingresar solo a los servidores que necesita acceder. Por ejemplo el proveedor de Sharepoint accede solo al servidor de Sharepoint, el proveedor de

cambiar los servidores y dispositivos de red?	correo solo al servidor de correo, el de Solar Wind solo al servidor de Solar Wind.
Software, Red de Internet y externa	
¿Se han realizado pruebas de penetración en la conexión a Internet periódicamente?	Se realizan pruebas de penetración 1 vez al año. Realizadas por un tercero.
¿Cómo se proteger la red interna y la zona desmilitarizada de la red ?	Se protege con el Firewall y un IPS (Controlador de tráfico) entre las diferentes zonas del firewall o estructura de la red.
¿Existe documentación de las reglas del firewall con explicaciones, y cuáles son las configuraciones de servidor de seguridad coherente a través de los diferentes segmentos?	Si existe
¿Utilizan un sistema de prevención de intrusos para poner fin a ataques maliciosos?	Se utiliza IPS Fortinet.
¿Se tiene un número bajo de conexiones a Internet como sea posible (incluyendo conexiones de acceso telefónico). Cada conexión a Internet es una vía para un atacante malicioso para entrar en su red?	Depende las necesidades de cada usuario el número de sesiones no está restringidas.
¿Mantienen suficientes registros (logs) de la actividad de red aprobada?	Se hace suficiente registro de Log con SIEM
¿Se cifran los datos confidenciales que se transfieren a través de la red?	No se cifran, solo los que viajan por VPN-IPSEC
¿Suelen buscar intentos repetidos de conexión no autorizados para conectarse a su sistema a través de una red? ¿Mantiene registros suficientes de toda la actividad de red relacionada con su sistema?	Si con la herramienta IPS- SIEM (correlacionador de eventos)

¿Monitorizan la actividad de red en busca de tráfico excesivo o inusual que llega a su sistema?	Si se trabaja con Solar Winds.
¿Hay protección en las comunicaciones en redes públicas?	Se manejan certificados digitales para el acceso a páginas públicas, tales como conexión de correo la empresa por internet o él envió de información a bancos
Wireless	
¿Periódicamente se convoca a una compañía externa para realizar una prueba de penetración de las redes de acceso inalámbrico?	Se realiza 1 vez al año.
¿Qué forma de encriptación WEP se utiliza?	WPA - WPA2
¿Consideran la posibilidad de utilizar la autenticación 802.1X como un método secundario método de autenticación para usuarios Wireless (además de clave WEP)?	Si se puede considerar
¿Consideran el establecimiento de la red inalámbrica en la zona desmilitarizada?	Existe un proyecto actualmente para colocar la red Wireless en una zona independiente del Firewall.
¿Se ha definido la política de seguridad inalámbrica y educar a los usuarios sobre la misma?	En la actualidad no existe documentación de las políticas inalámbricas.
¿Permiten el tráfico desde la red de usuarios Wireless hacia los servicios corporativos?	No se permite
Información	
¿Existen controles para el uso medios removibles (MR)?	No existen
¿Existen procedimientos formales para alta y baja de usuarios (MR) (Acceso no autorizado)?	No
Personal	
¿Existe concienciación y formación en seguridad para los funcionarios de la entidad (MR)?	En la actualidad no existe.

¿Existe supervisión a terceros dentro de la entidad?	Hay una persona que figura como interventora, pero no existe un seguimiento especifico

Anexo B. Encuesta De Evaluación Del Uso De La Tecnología Y Los Sistemas De Seguridad De La Información

1. ¿Si le envían un mensaje a su correo personal de su banco de confianza para que ingrese a un Link especifico que le solicita información confidencial. Usted que hace?

    a. Utiliza el Link sugerido por el banco e ingresa sus datos personales
    b. Llama a servicio al cliente del banco para confirmar el correo recibido.
    c. Elimina el correo
    d. Solicita ayuda de un amigo.
    e. Llama a soporte de la oficina de Tecnología.

2. ¿A su correo institucional han llegado correos masivos de remitentes externos a la entidad?
    a. Si
    b. No

3. ¿Si al navegar en Internet aparece una ventana y le pide dar aceptar o descargar?

    a. usted le da clic sin preocuparse de que se trata.
    b. Lee con detenimiento el mensaje que aparece
    c. Pide ayuda de alguien cercano que sepa de sistemas o llama a la oficina de tecnología
    d. Le da cancelar o cerrar a la ventana

4. ¿Usted cierra la sesión de su sistema cada vez que se levanta de su equipo?
    a. Si
    b. No

5. ¿Cómo define sus contraseñas?

    a. Utiliza los nombres de sus padres o de sus hijos para que sea más fácil de recordar
    b. Utiliza como mínimo 8 caracteres, que contenga letras, números y símbolos
    c. Utiliza una palabra corta acompañada de un número
    d. Utiliza una frase corta fácil de recordar.

6. ¿En su memoria USB, en su celular u otro dispositivo portable acostumbra a llevar copias de la información de la Oficina?

a. Nunca
b. Algunas veces
c. Con frecuencia
d. Siempre

7. ¿Si a Usted le solicitan conservar la información a través de medios que garanticen su preservación, en otras palabras hacer copias de seguridad de la información gestionada en la entidad, prefiere?

a. No darle importancia
b. Conservarla en su computador.
c. Conservarla en los discos de red o carpetas compartidas alojadas en otro computador a fin de preservarla.
d. Guardarla en otros medios (Celular, CD, USB, Discos externos).

8. ¿Si crea copias de seguridad de la información de la entidad en medios físicos como DVD, CD, USB. Donde las ubica?

a. En el cajón de su oficina
b. en un archivo especial destinado para ello
c. en su casa

9. ¿Si a Usted le asignan una contraseña, para evitar olvidarla acostumbra?

a. Registrarla en un archivo.
b. Copiarla en una hoja que deja encima del escritorio.
c. Copiarla en un Post-it y lo pega en la pantalla del computador.
d. Memorizarla.
e. Revelarla a un tercero.

10. ¿Usted hace parte del equipo de la entidad que está evaluando una cifra que va a ser publicada próximamente. Al subir al ascensor para salir a almorzar se encuentra un amigo de otra dependencia en el ascensor al cual le comenta el valor de la cifra. Usted no se fija que en el ascensor iba un periodista carnetizado del diario El Tiempo. Días después aparece la noticia antes que la publique la entidad, usted que hace:

a. Llama al diario El Tiempo a quejarse.
b. Admite el error cometido y lo comenta con sus superiores.
c. Pregunta al señor vigilante del edificio si conoce al tipo.
d. Ninguna de las anteriores.

11. ¿Usted cree que la información personal de los empleados de la entidad tales como: Dirección casa, teléfonos, la conocen?

a. Todos los empleados de la entidad
b. Los administradores del sistema de Recursos Humanos
c. Usted solamente
d. Ninguna de las anteriores

12. ¿Si Usted está buscando información en un directorio o carpeta privada, e involuntariamente se da cuenta que puede ingresar a la(s) carpeta(s) de otra(s) dependencia(s), que acción toma?

    a. Navega por las subcarpetas y revisa la información existente
    b. No le da importancia y continúa con su búsqueda
    c. Comenta con otro(a) compañero (a) la situación
    d. Notifica a sistemas este hallazgo

13. ¿Cuál de las siguientes opciones considera adecuada para él envió de impresiones a la impresora de su dependencia?

    a. Se puede imprimir cualquier tipo de documento
    b. Solo se deben imprimir documentos institucionales
    c. Se puede imprimir cualquier cosa pero sin que se den cuenta
    d. No se puede imprimir nada porque desde la Oficina de Informática nos vigilan
    e. La oficina de tecnología no vigila las impresiones y por esta razón se puede imprimir cualquier cosa

14. ¿Si al ingresar en alguna página de Internet, y esta se ve correctamente, y le sale el siguiente aviso ñpara poder ver la página correctamente debe instalar un controlador Xò ¿usted realiza alguna de las siguientes acciones?

    a. Permite la Instalación
    b. Investiga para qué sirve el controlador que se requiere instalar
    c. Llama a Soporte para que le indique que acción realizar
    d. Acepta que no puede instalarlo, porque por seguridad están restringidas las descargas

15. ¿Si una entidad externa solicitan a una Dependencia de la organización información perteneciente a la organización, usted como funcionario que haría?

    a. Le dice que le envía la información por correo electrónico.
    b. Le dice que venga a la oficina y le entrega una copia.
    c. Consulta el directorio de fuentes de información para saber quién es el responsable.
    d. Consulta con jefe inmediato si está permitido compartir esta información.

16. ¿Usted mantiene la información de naturaleza confidencial de la entidad en:

a. La carpetas Mis documentos de su área
b. La carpeta Escritorio de su Área
c. Una carpeta ubicada en la raíz disco C
d. En una carpeta ubicada en la raíz de otra unidad (si esta se encuentra disponible)

17. ¿Siempre que coloca su unidad USB en su computador UD?

a. Le pasa el antivirus, antes de acceder a ella
b. No le pasa en antivirus, y realiza intercambios de información.

18. ¿Si alguno de sus conocidos le informa que le están llegando mensajes raros desde su cuenta de correo institucional usted:

a. Llamar a la mesa de ayuda e informar de la situación
b. No reporta y cambia la clave de su sesión, pensando que con esto solucionará el problema
c. No le da importancia al comentario

19. ¿Usted acostumbra a usar correos diferentes a los institucionales para envió de información que tiene que ver con la entidad?

a. Si
b. No

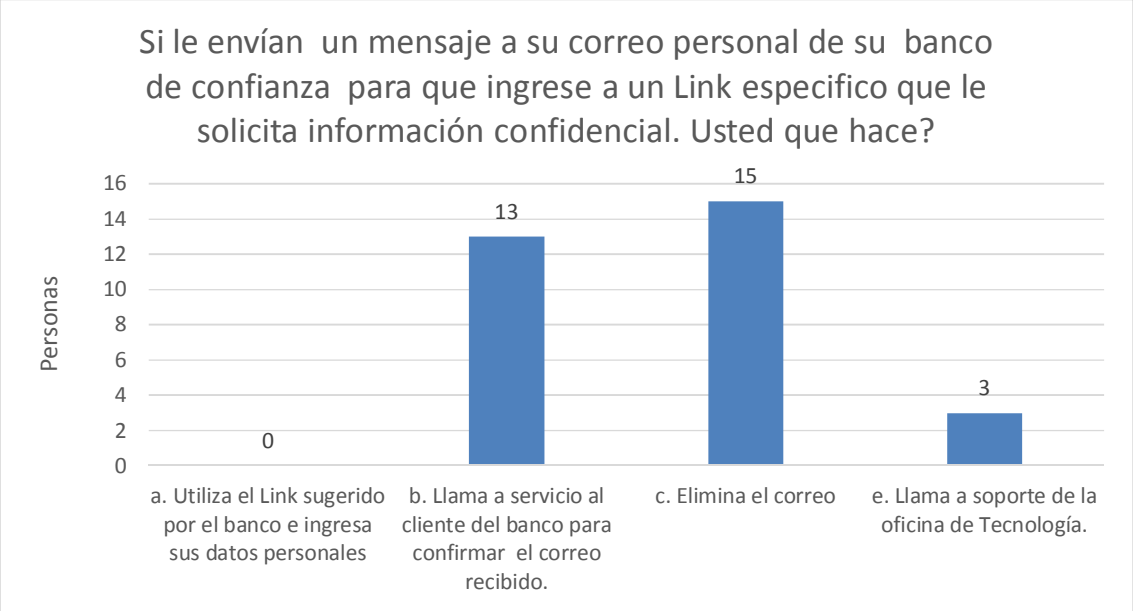
20. ¿Acostumbra a ir a cafés Internet a consultar su cuenta de correo institucional o de la entidad donde trabaja?

a. Si
b. No

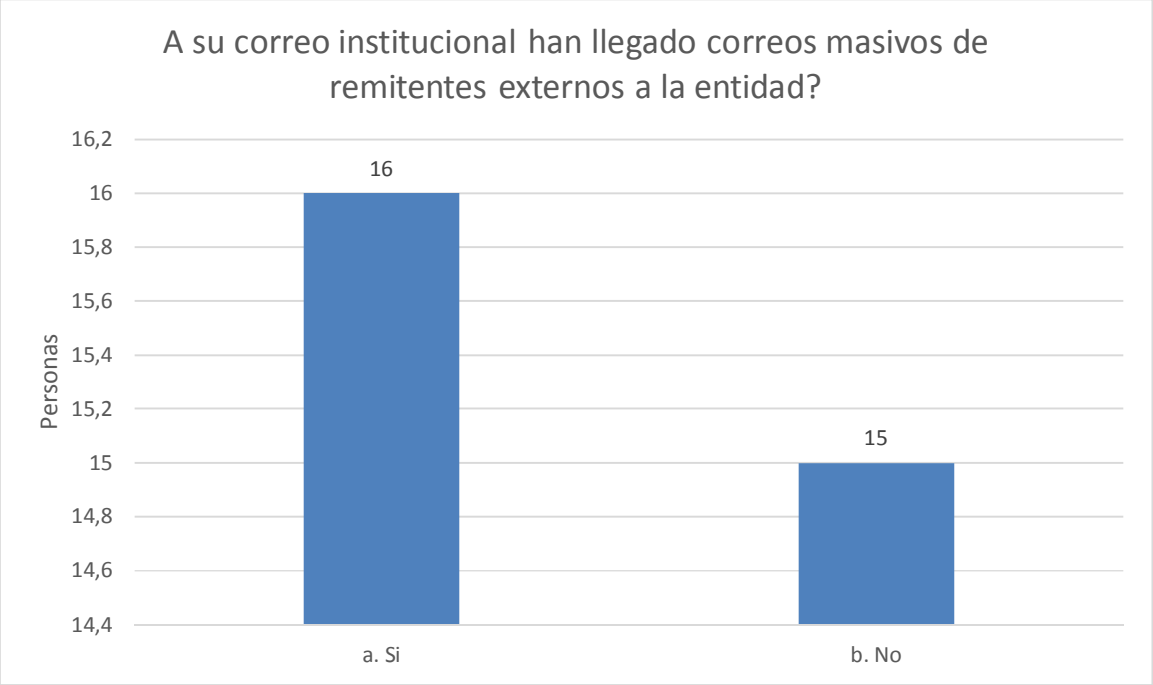
21. ¿Considera que la información de propiedad de la entidad debe ser privada e intransferible, por tal razón se debe:

a. Mejorar los controles de acceso.
b. Impedir el uso de dispositivos externos que permitan la difusión de la información.
c. Capacitar a los usuarios en el buen manejo de la información de propiedad de la entidad
d. Otra

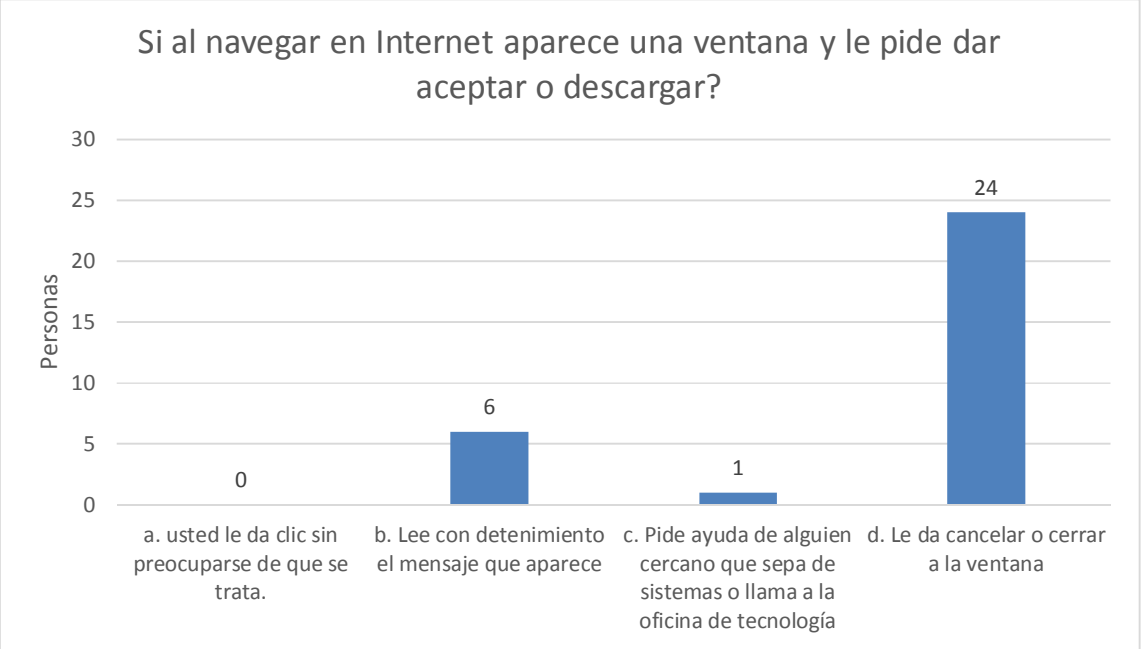
Anexo C. Gráfico Pregunta 1 De La Encuesta E Evaluación Del Uso De La Tecnología



Anexo D. Gráfico Pregunta 2, De La Encuesta De Evaluación Del Uso De La Tecnología

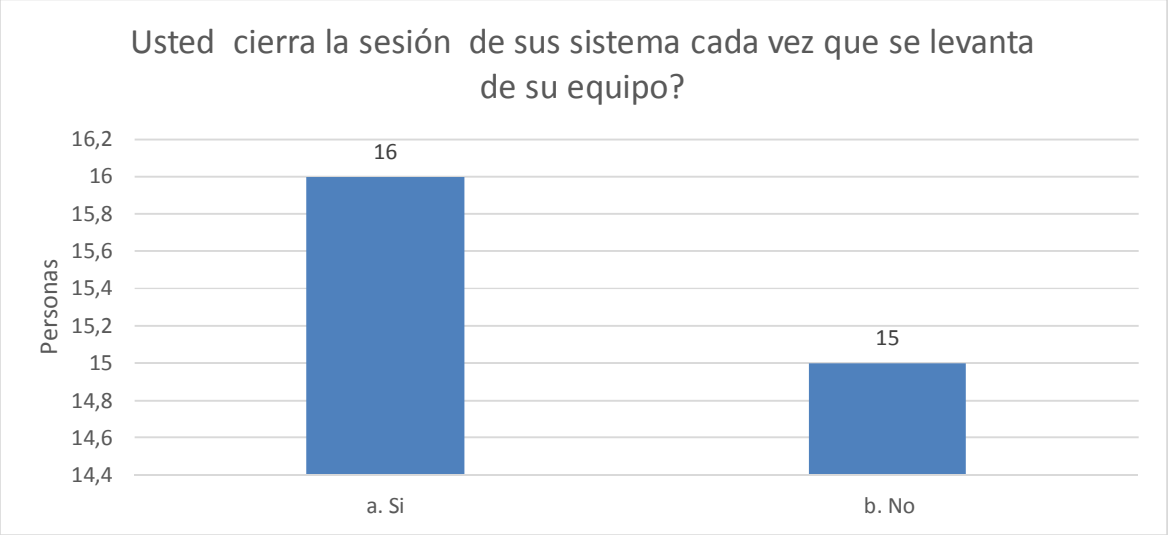


Anexo E. Gráfico Pregunta 3, De La Encuesta De Evaluación Del Uso De La Tecnología



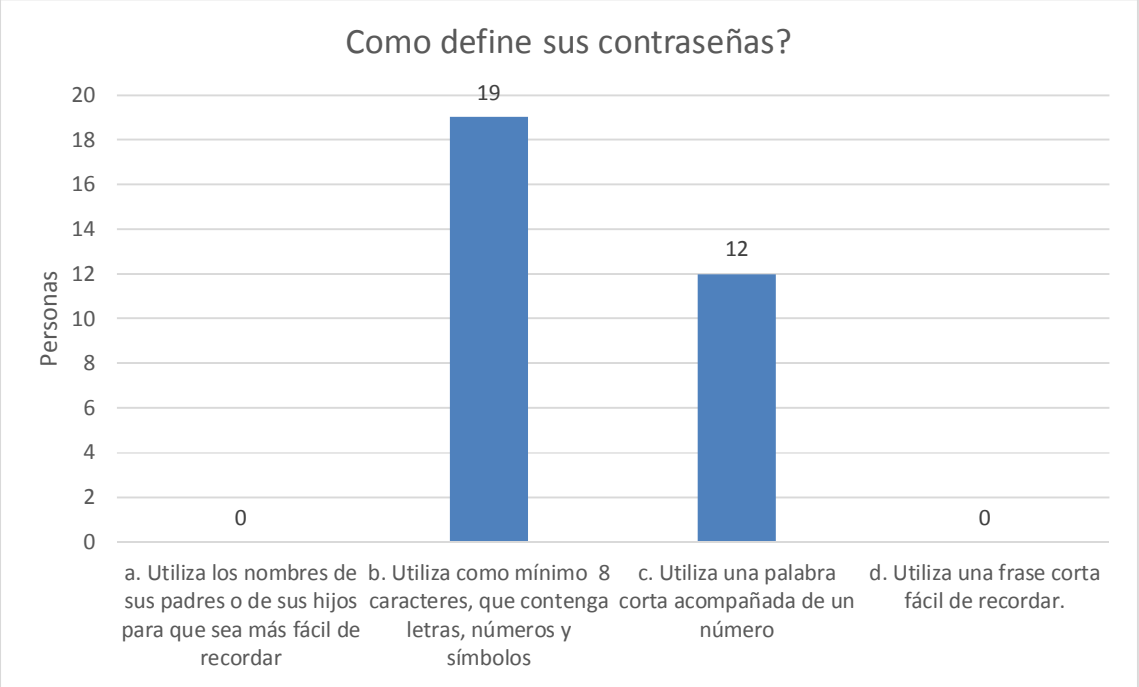
Fuente Autor.

Anexo F. Gráfico Pregunta 4, De La Encuesta De Evaluación Del Uso De La Tecnología



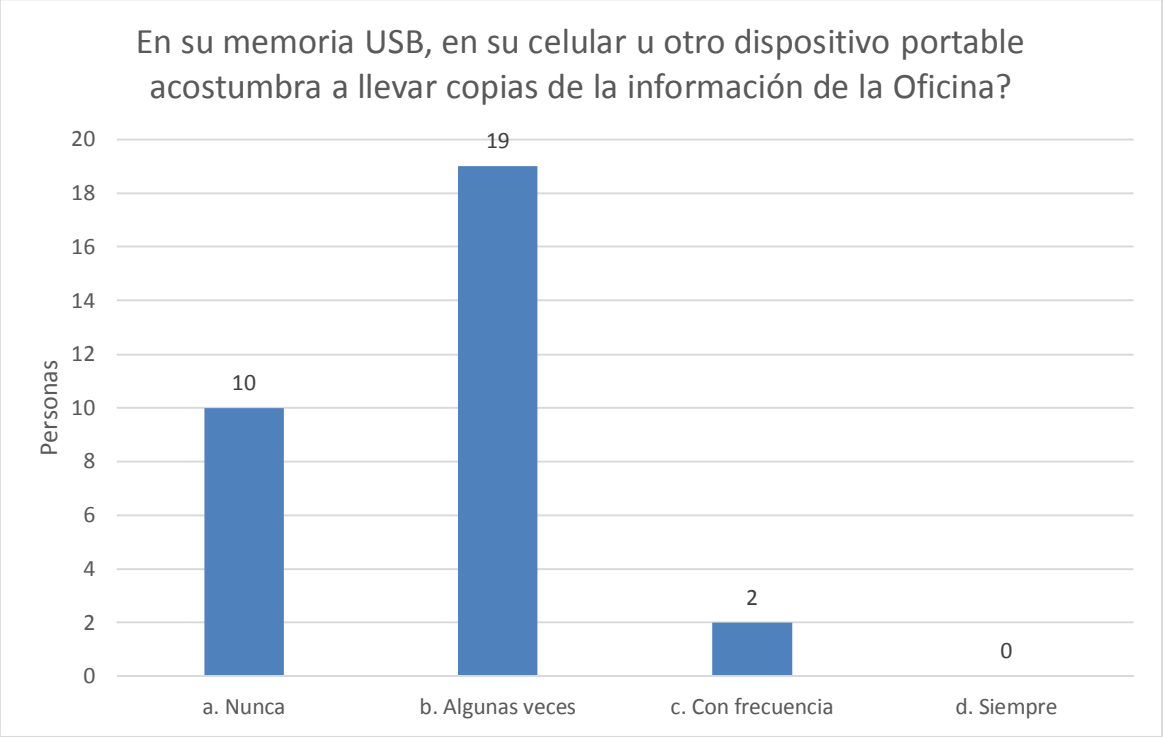
Fuente Autor

Anexo G. Gráfico Pregunta 5, De La Encuesta De Evaluación Del Uso De La Tecnología



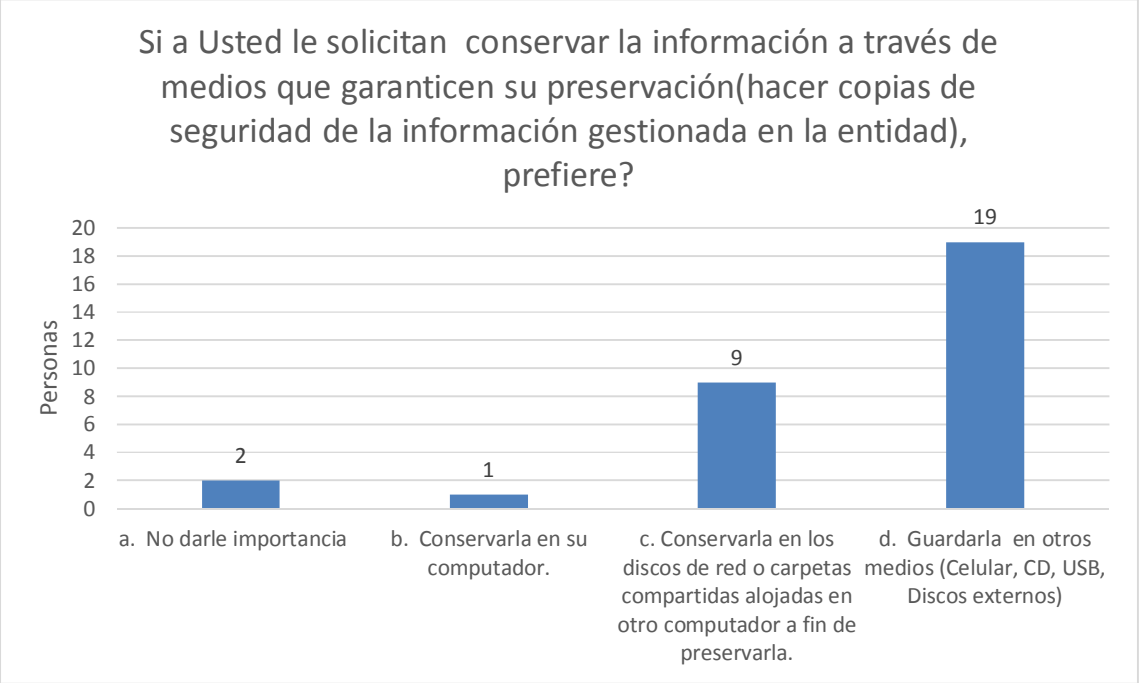
Fuente Autor

Anexo H. Gráfico Pregunta 6, De La Encuesta De Evaluación Del Uso De La Tecnología



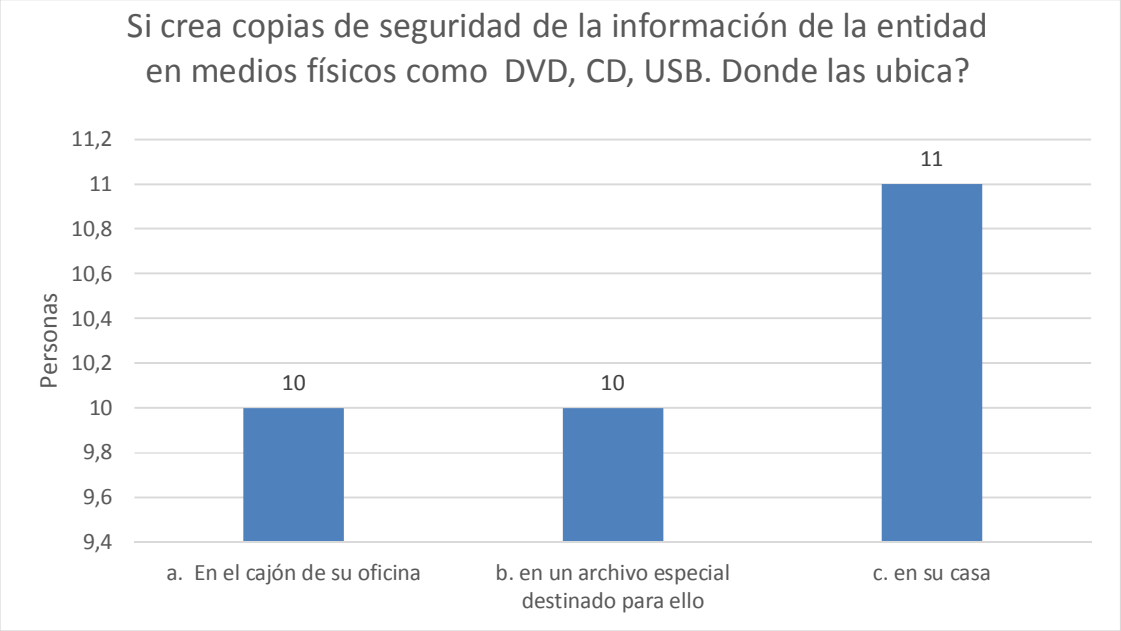
Fuente Autor

Anexo I. Gráfico Pregunta 7, De La Encuesta De Evaluación Del Uso De La Tecnología



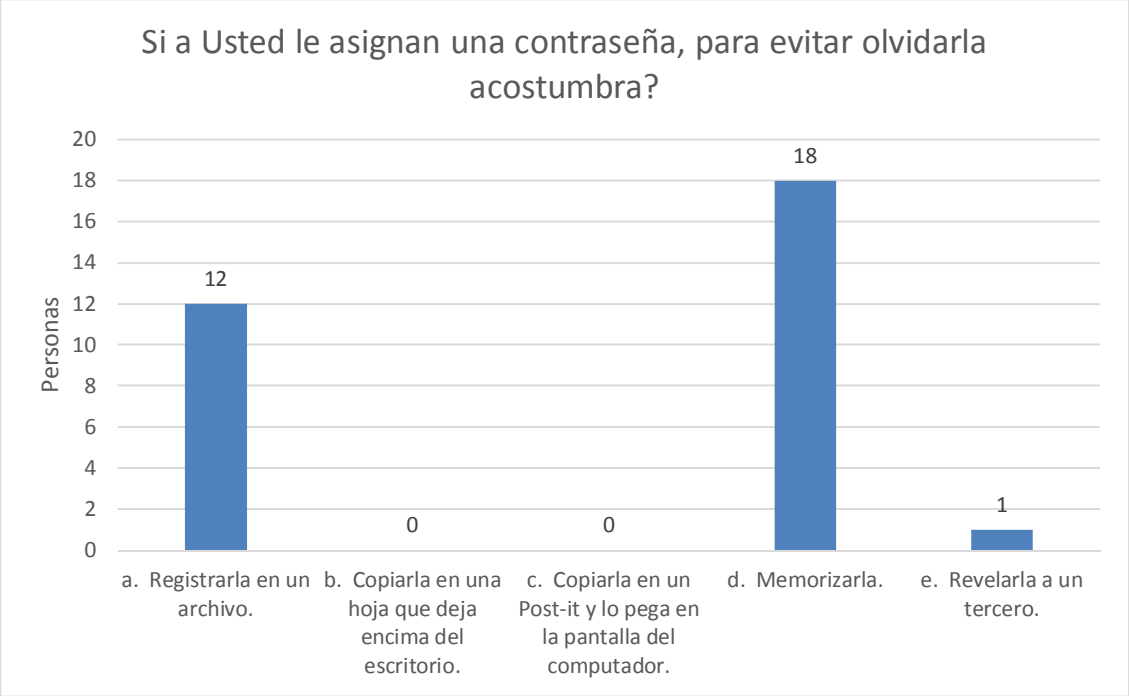
Fuente Autor

Anexo J. Gráfico Pregunta 8, De La Encuesta De Evaluación Del Uso De La Tecnología



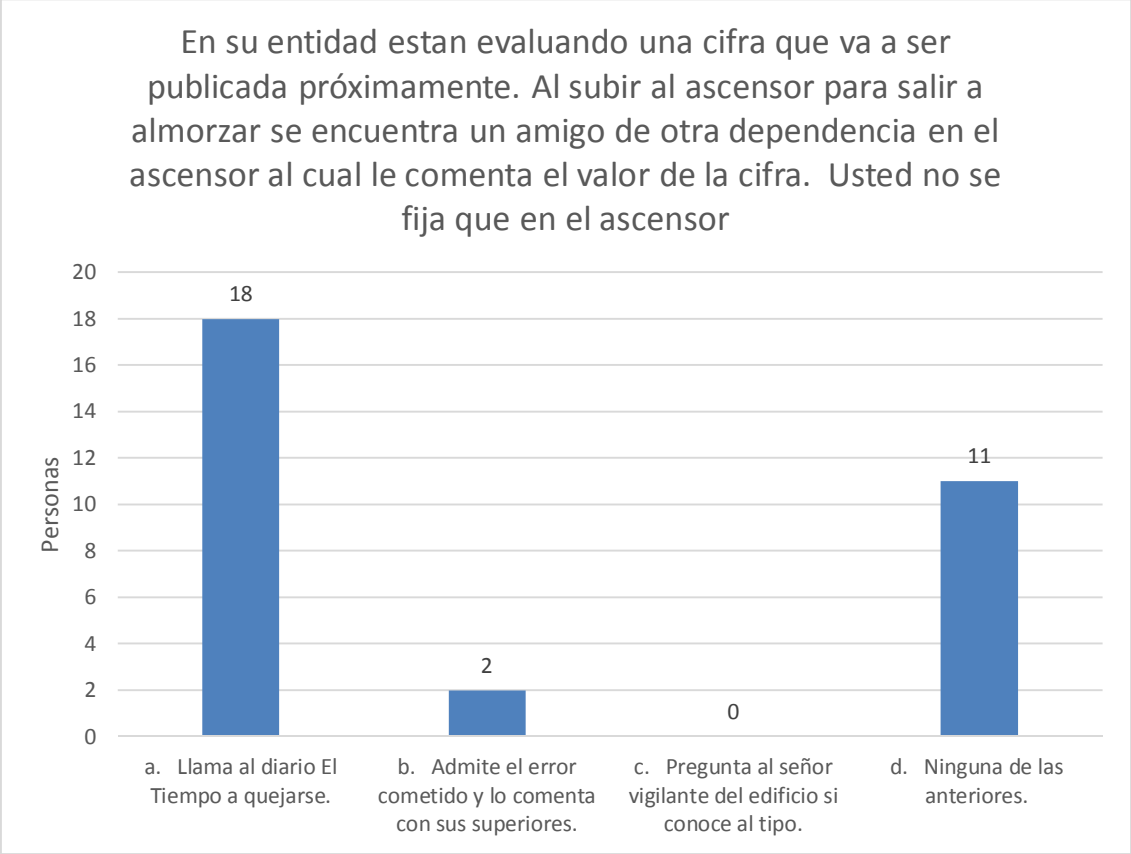
Fuente Autor

Anexo K. Gráfico Pregunta 9, De La Encuesta De Evaluación Del Uso De La Tecnología



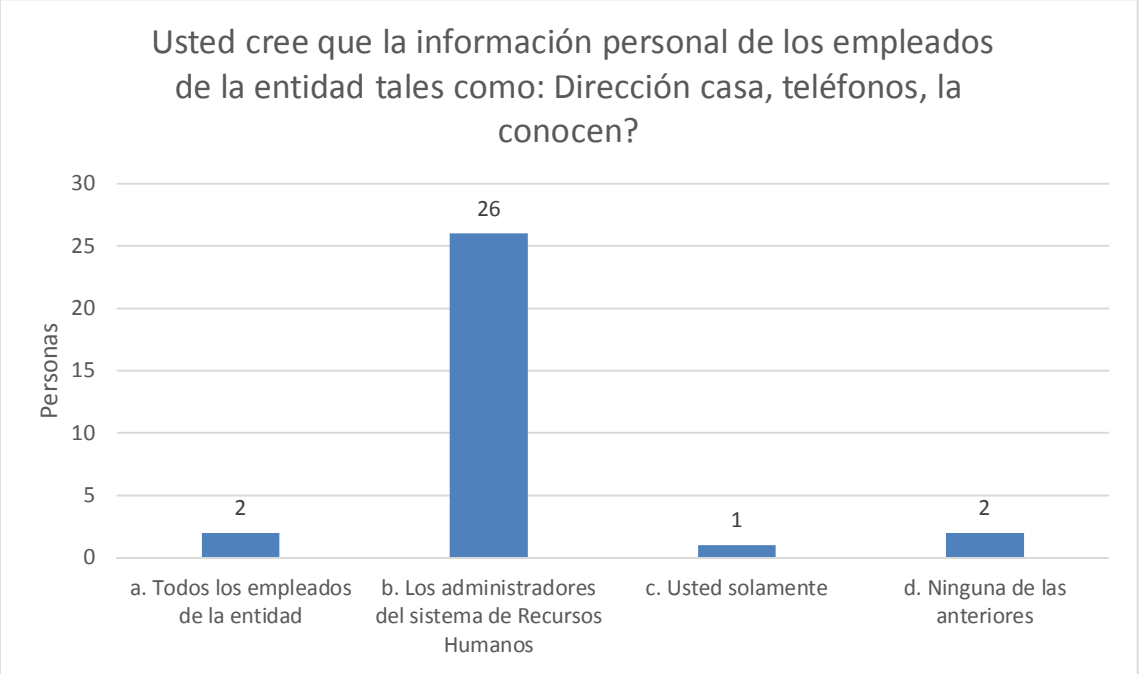
Fuente Autor

Anexo L. Gráfico Pregunta 10, De La Encuesta De Evaluación Del Uso De La Tecnología



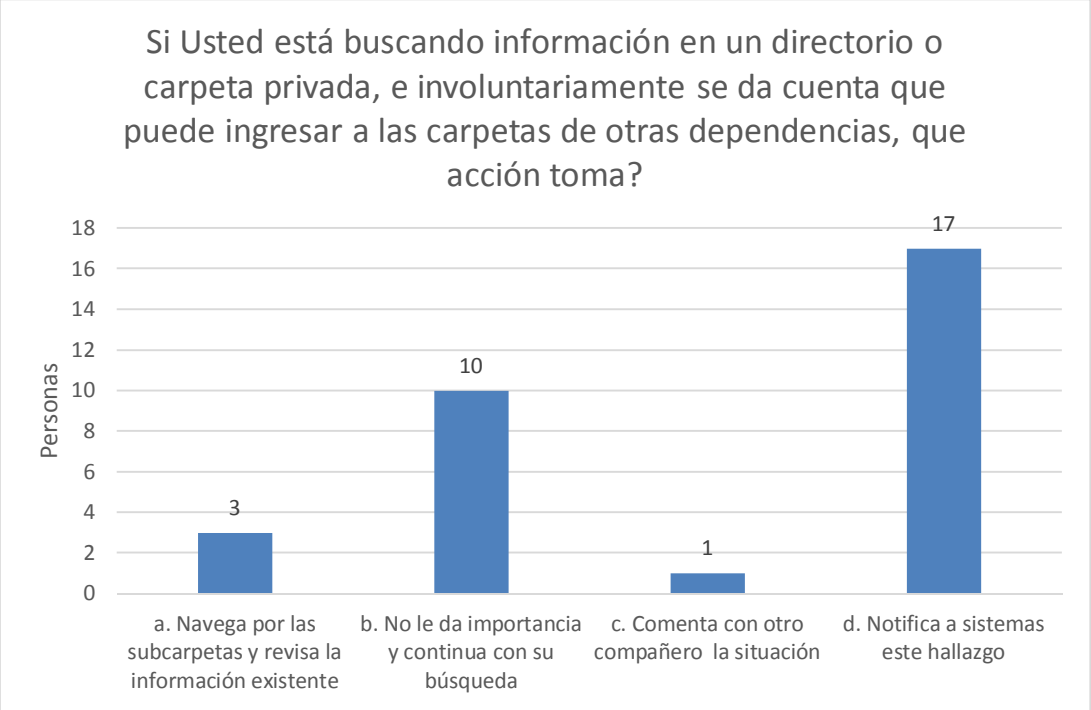
Fuente Autor

Anexo LL. Gráfico Pregunta 11, De La Encuesta De Evaluación Del Uso De La Tecnología



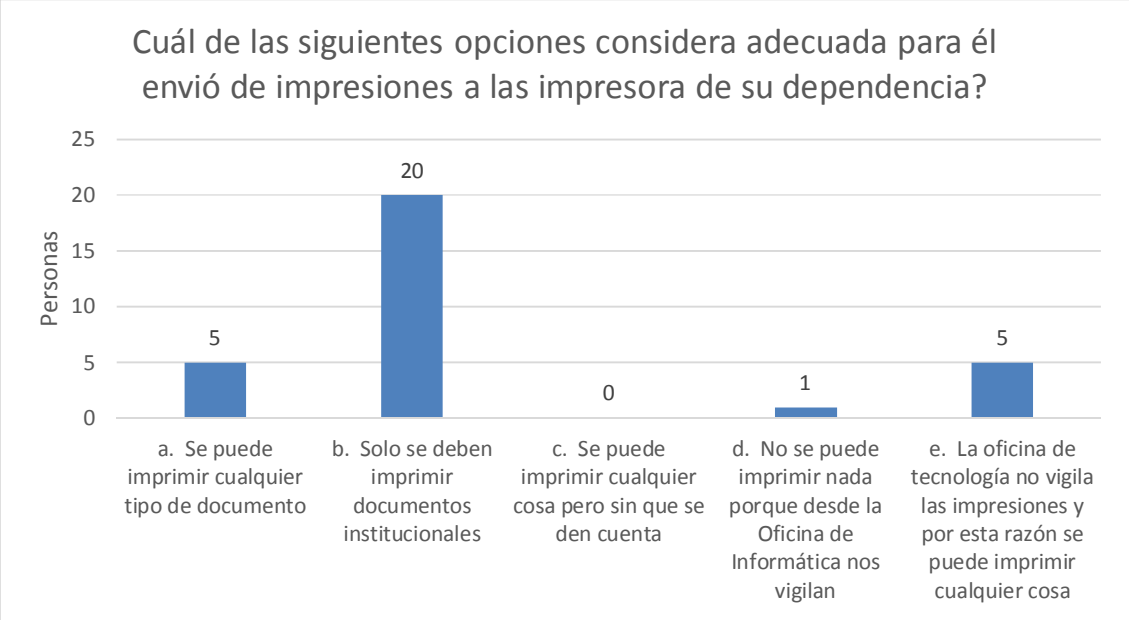
Fuente Autor

Anexo M. Gráfico Pregunta 12, De La Encuesta De Evaluación Del Uso De La Tecnología



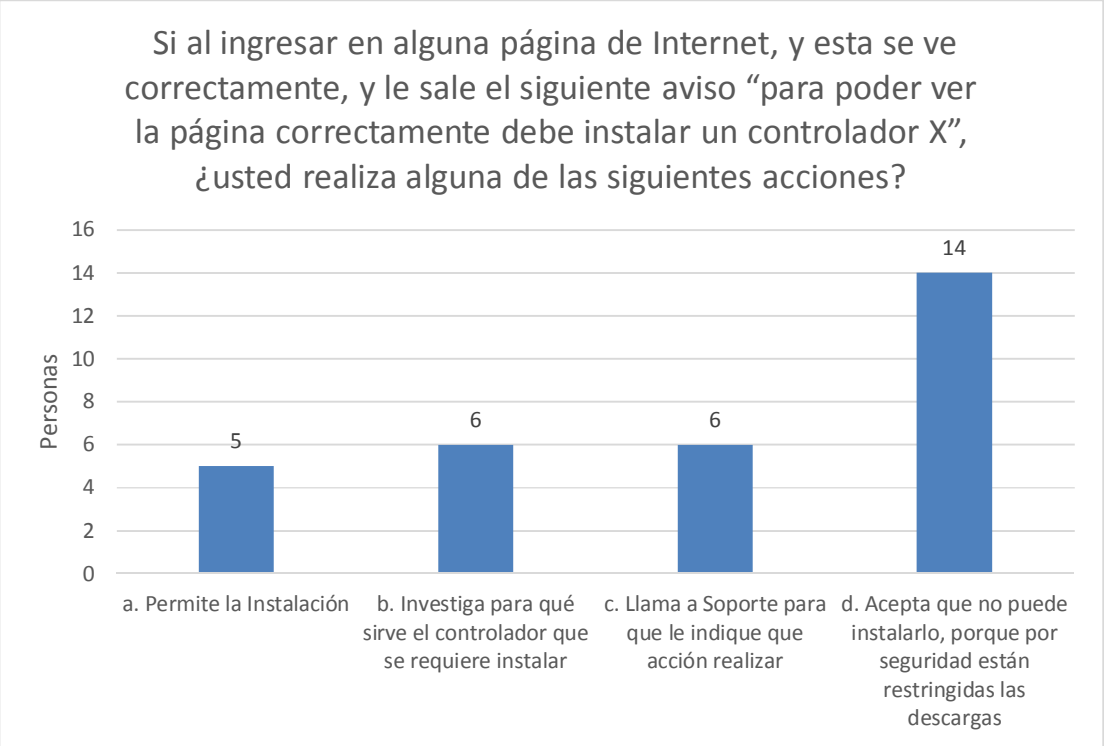
Fuente Autor

Anexo N. Gráfico Pregunta 13, De La Encuesta De Evaluación Del Uso De La Tecnología



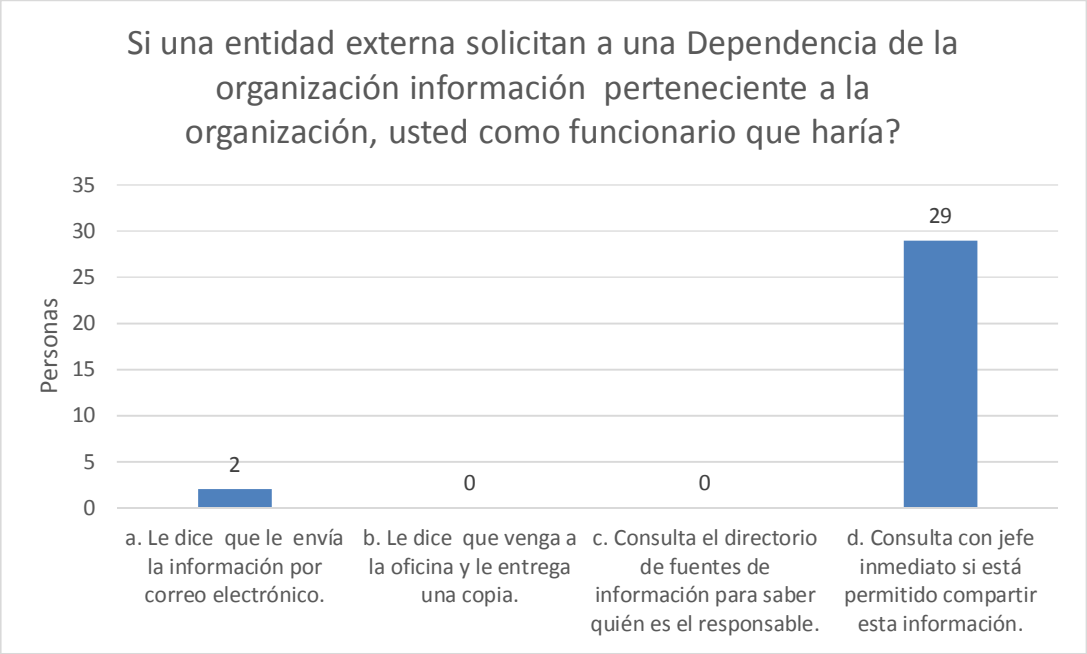
Fuente Autor

Anexo Ñ. Gráfico Pregunta 14, De La Encuesta De Evaluación Del Uso De La Tecnología



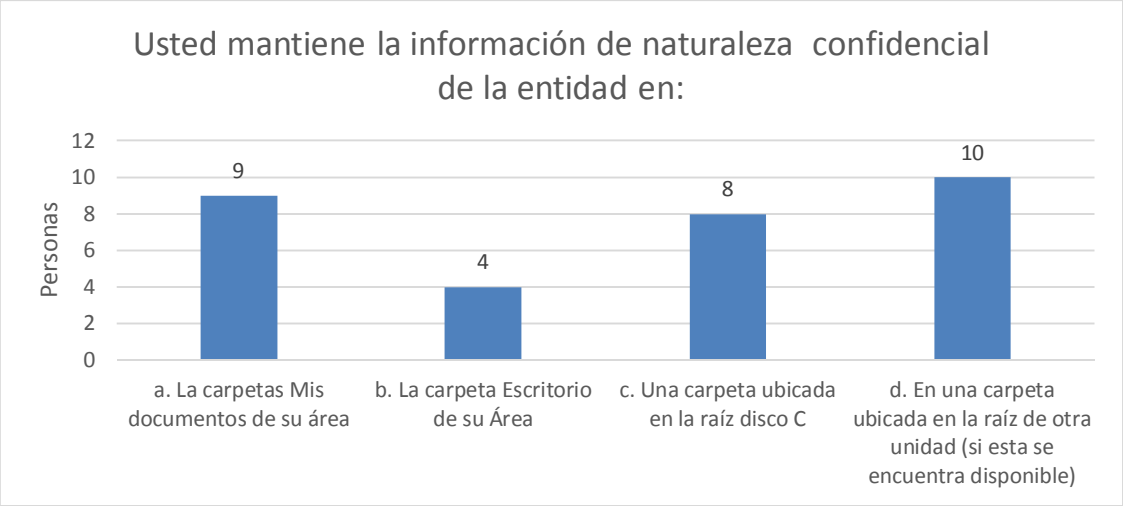
Fuente Autor

Anexo O. Gráfico Pregunta 15, De La Encuesta De Evaluación Del Uso De La Tecnología



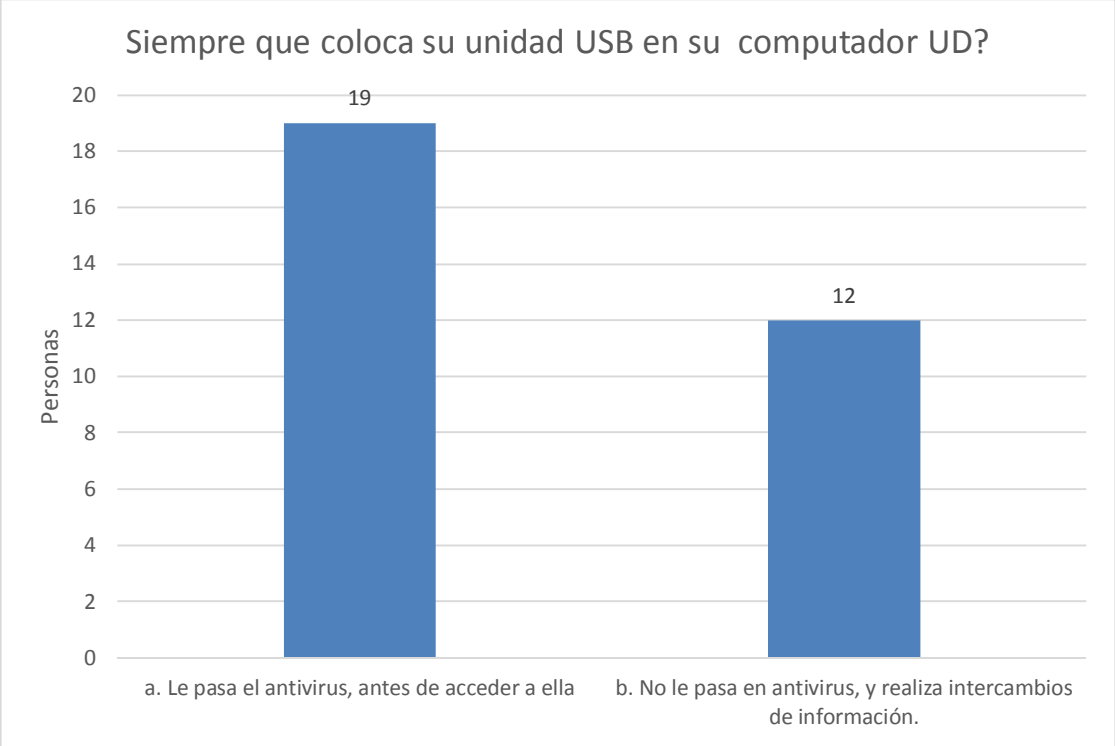
Fuente Autor

Anexo P. Gráfico Pregunta 16, De La Encuesta De Evaluación Del Uso De La Tecnología



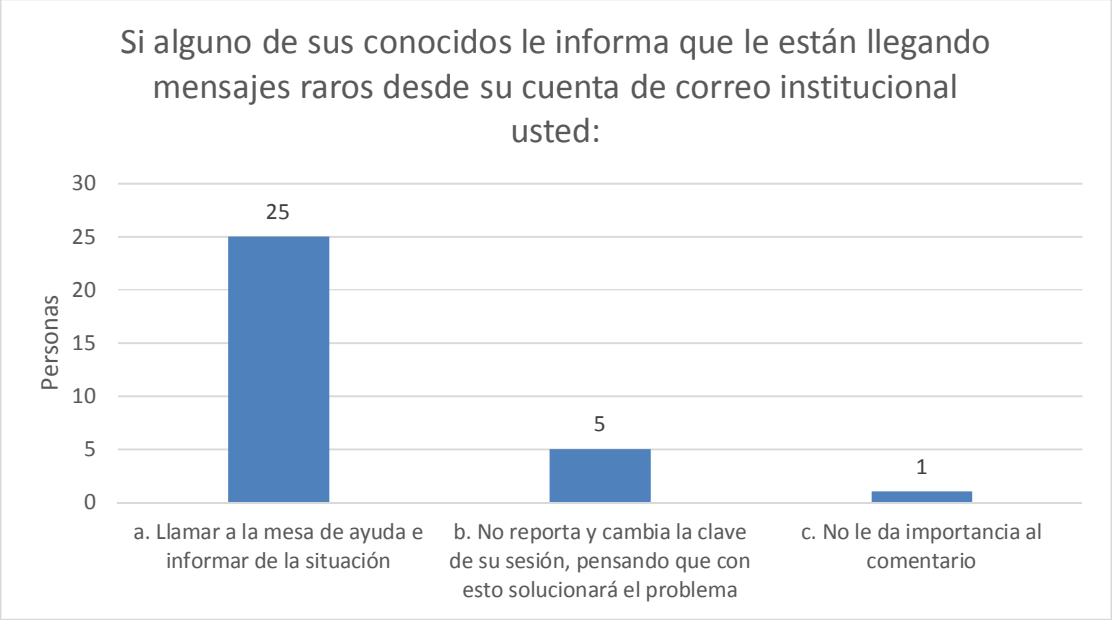
Fuente Autor

Anexo Q. Gráfico Pregunta 17, De La Encuesta De Evaluación Del Uso De La Tecnología



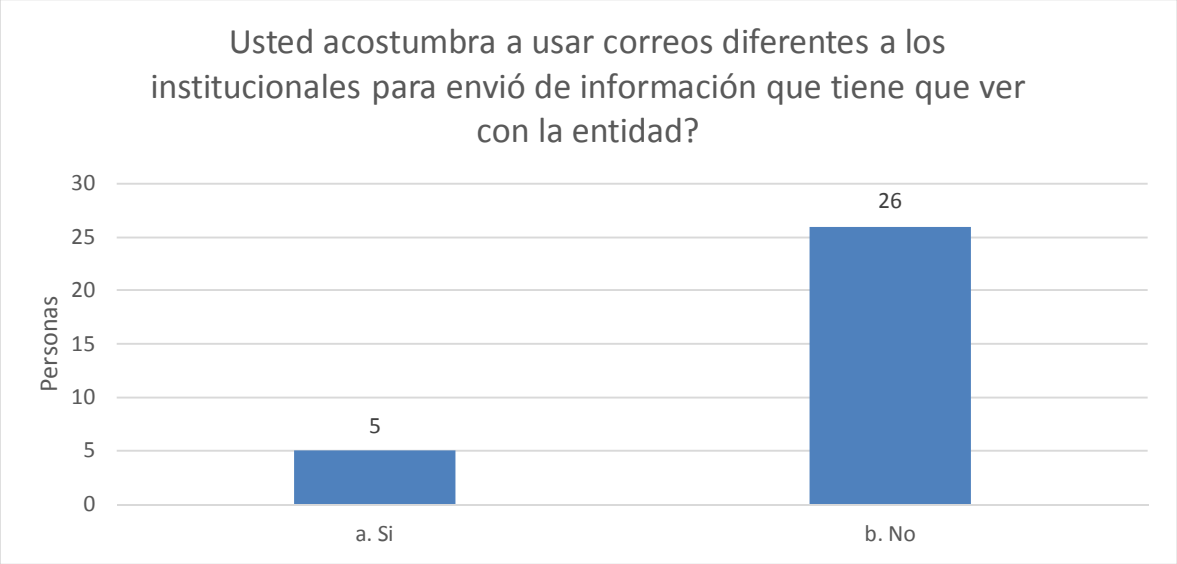
Fuente Autor

Anexo R. Gráfico Pregunta 18, De La Encuesta De Evaluación Del Uso De La Tecnología



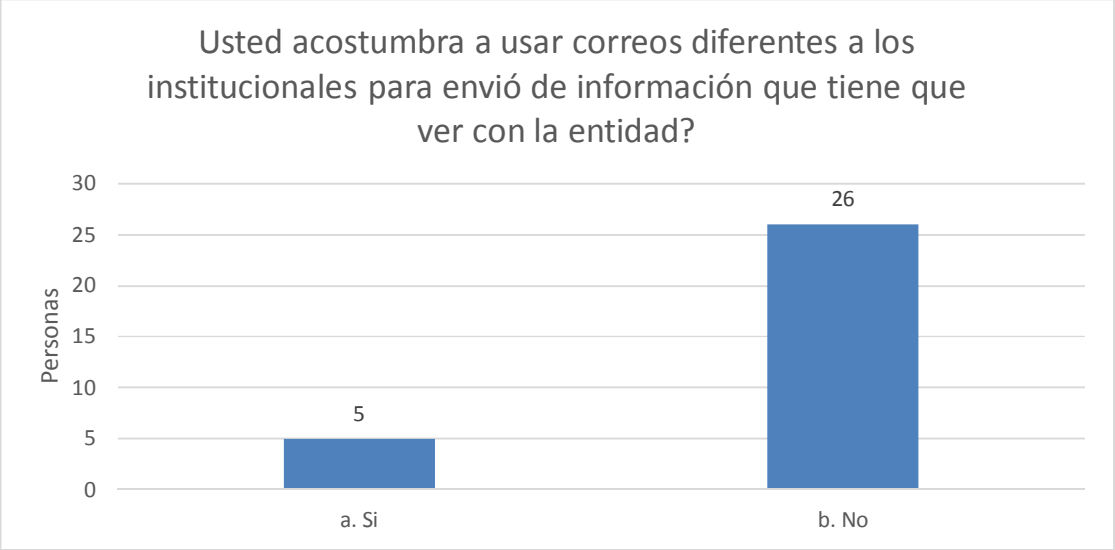
Fuente Autor

Anexo S. Gráfico Pregunta 19, De La Encuesta De Evaluación Del Uso De La Tecnología



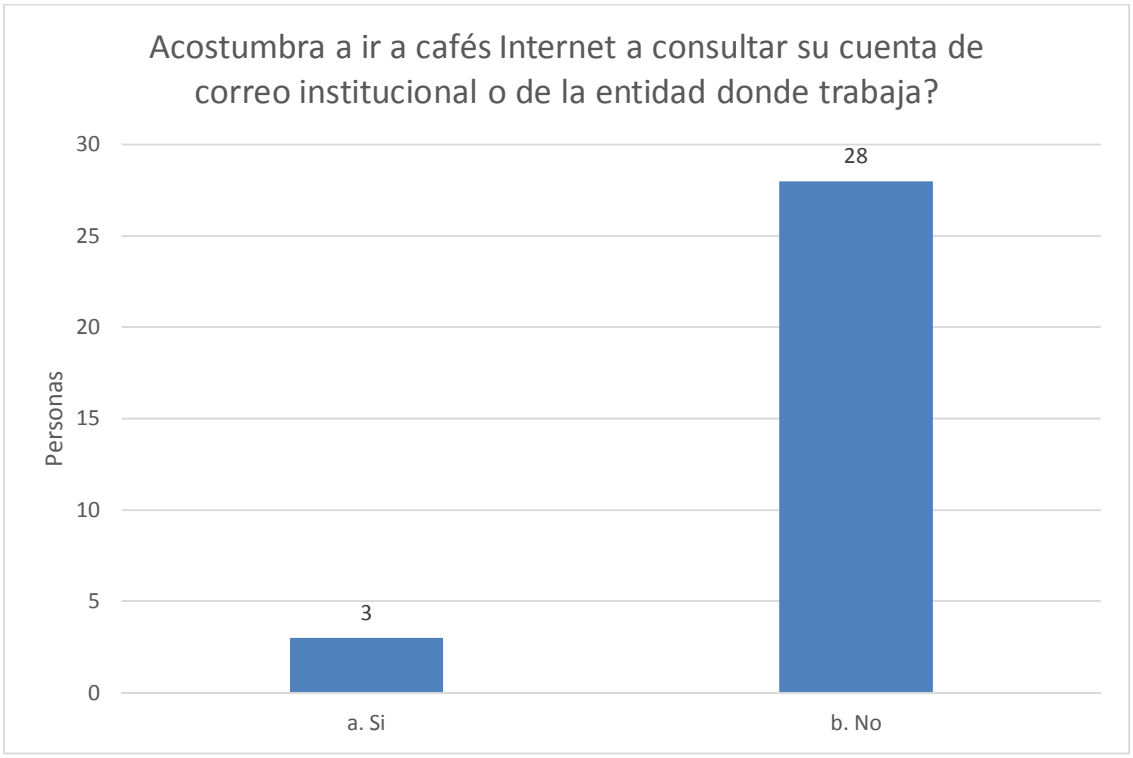
Fuente Autor

Anexo T. Gráfico Pregunta 19, De La Encuesta De Evaluación Del Uso De La Tecnología



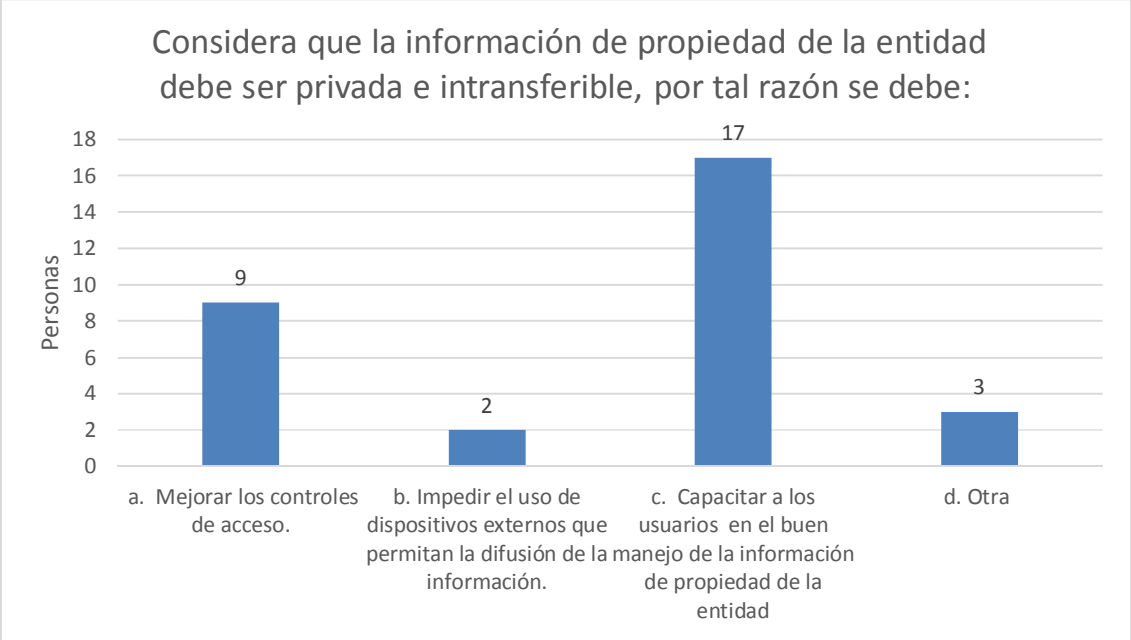
Fuente Autor

Anexo U. Gráfico Pregunta 20, De La Encuesta De Evaluación Del Uso De La Tecnología



Fuente Autor

Anexo V. Gráfico Pregunta 21, De La Encuesta De Evaluación Del Uso De La Tecnología



Fuente Autor