Mejoramiento Al Sistema De Gestión De Seguridad De La Información En Enka De Colombia S.A.

Jairo Andrés Acosta Aristizabal

René Mauricio Barrera Tamayo

Yudi Vanessa Sandoval Arango

Universidad Nacional Abierta y a Distancia – UNAD

Especialización en Gestión de Proyectos

2019

Mejoramiento Al Sistema De Gestión De Seguridad De La Información En Enka De Colombia S.A.

Jairo Andrés Acosta Aristizabal

René Mauricio Barrera Tamayo

Yudi Vanessa Sandoval Arango

Asesor

Doctora Oliva Mendoza

Trabajo de investigación como requisito para optar al título de: Especialista en Gestión de Proyectos

Universidad Nacional Abierta y a Distancia – UNAD

Especialización en Gestión de Proyectos

2019

Nota de aceptación

_____

_____

_____

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

Bogotá, 2019

Dedicatoria

La vida y la experiencia misma nos han enseñado que por nuestras vidas pasan muchas personas y momentos y que lo único constante es la familia.

Agradecemos a nuestros padres, esposa(o) e hijas(os) por el apoyo incondicional, por la paciencia, simplemente por todo el amor y la felicidad que generan en nuestras vidas.

Especial mención a nuestros, sin su sacrificio, decisiones, amor y todo lo que se han esforzado nosotros ni siquiera existiríamos.

Agradecimientos

A nuestras familias por todo

A la universidad, tutores y directores por sus enseñanzas.

En Enka de Colombia S.A. por abrirnos las puertas de la compañía tan exitosa.

Abstract

Today, companies have defined information as their most important asset. For this reason, it is necessary to have a clear definition of the computer security to be implemented to offer protection of this and the computer systems that support and preserve it.

Protecting information offers organizations the possibility of obtaining international certifications that support internal processes by having high standards to preserve information as a competitive advantage and in many cases as a business secret.

To achieve certifications, it is necessary to review and evaluate controls and processes in all areas of the organization. At the same time, it is important and critical to involve all the company's personnel regardless of the area to which they belong, since they are the ones who will help implement management systems on a daily basis and avoid that they only remain in written documents.

Tabla de Contenido

Índice de tablas

Índice de figuras

Introducción

Hoy en día, las empresas han definido a la información como su activo más importante. Por tal motivo, se hace necesario contar con una definición clara de las seguridades informáticas a implementar para ofrecer protección de esta y de los sistemas informáticos que la respaldan y la conservan.

Proteger la información ofrece a las organizaciones la posibilidad de obtener certificaciones internacionales que respaldan los procesos internos al contar con altos estándares para conservar la información como una ventaja competitiva y en muchos casos como un secreto empresarial.

Para lograr las certificaciones, es necesario revisar y evaluar en todas las áreas de la organización los controles y procesos. A su vez, es importante y crítico involucrar a todo el personal de la compañía sin importar el área a la que pertenezcan, pues son ellos los que ayudaran a implementar en la cotidianidad los sistemas de gestión y evitar que sólo se queden en documentos escritos.

1. TÍTULO

Mejoramiento al sistema de gestión de seguridad información Y De La Información En Enka De Colombia S.A

2. CAPÍTULO 1

2.1. Formulación del problema o pregunta de investigación

Teniendo en cuenta que día a día todas las empresas tienen más necesidad de utilizar modelos sistematizados para difundir y guardar la información necesaria para su desarrollo y funcionamiento, dichas empresas.

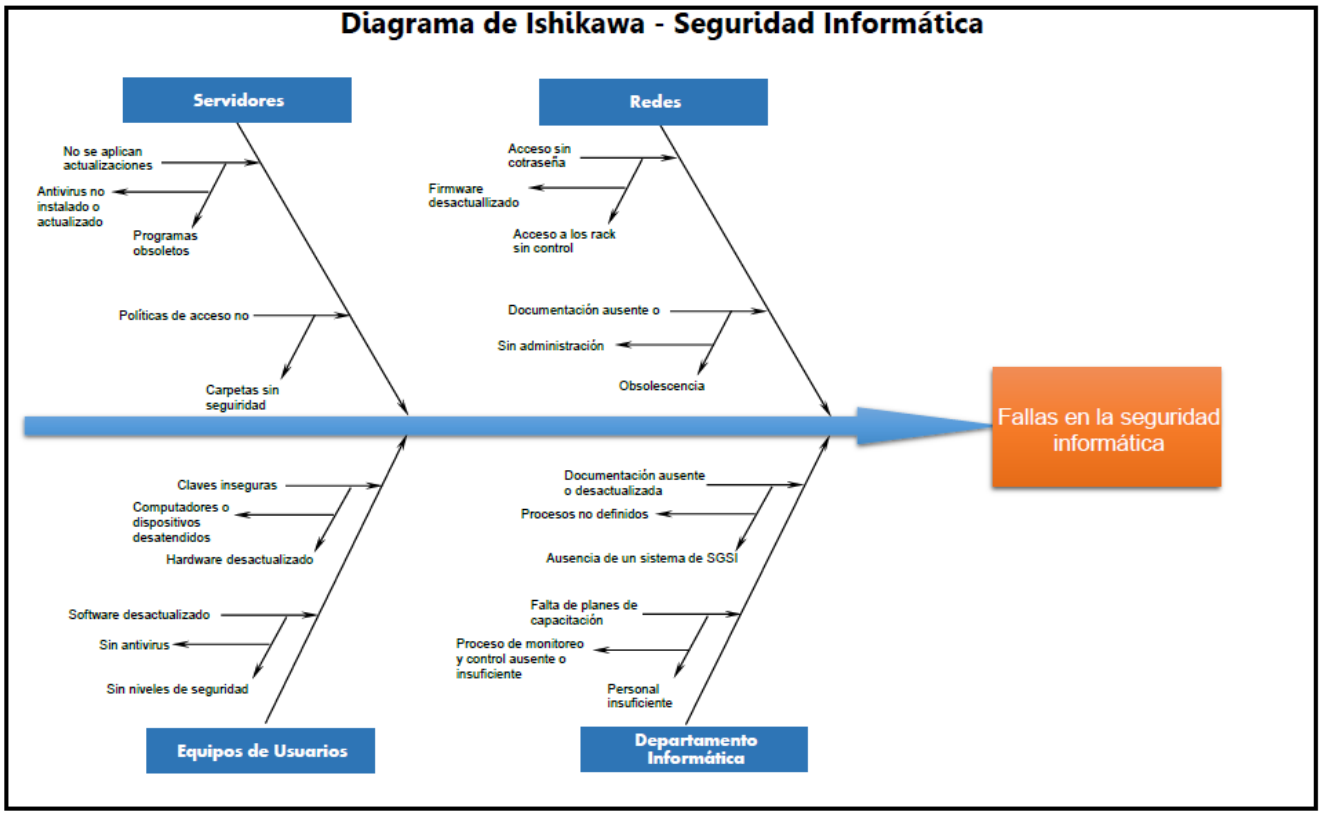
En 2014, Enka de Colombia planteó la implementación de un sistema de gestión de seguridad de la información. Para ese entonces, la estructura organizacional, operativa y de tecnología contaba con un diseño acordé a las necesidades vigentes del negocio. Los usuarios hacían uso a tecnologías que les permitieron cumplir sus funciones y permiten la evolución organizacional.

Hoy en día, los usuarios requieren contar con tecnologías que les permiten lograr niveles de colaboración, accesibilidad a la información sin comprometer la integridad y confiabilidad de la información. Temas relacionados con la seguridad eran aspectos secundarios y de poco peso en la organización. Proteger la información es una prioridad para las organizaciones y para Enka de Colombia ya que es uno de sus activos más valiosos para ser competitivos y permanecer en una economía global.

Enka de Colombia S.A., ¿cuenta con modelos de seguridad eficaces, que los haga menos vulnerables ante ataques cibernéticos que puedan apoderarse de información confidencial que pueda poner en peligro la razón de ser de la compañía?

2.2.Diagrama de Ishikawa

Figura 1. Diagrama de Ishikawa



2.3.Justificación y alcance del proyecto

2.3.1. Justificación

Enka de Colombia S.A. cuenta con procesos implementados para cumplir con la norma ISO 9001. Dichos procesos vienen siendo actualizados de tal forma que permitan alcanzar excelencia operativa y el mejoramiento continuo.

Nuestro proyecto se enfocará en el mejoramiento y actualización del SGSI para el área de tecnología (TI) teniendo presente los diferentes procesos que se tiene ya enmarcados e identificando que proyectos nuevos deben ser creados para cumplir con la norma.

Nuestro enfoque además de incluir la seguridad en la información es analizar y proponer un modelo para la seguridad sobre la infraestructura, la cual incluye servidores, redes, telecomunicaciones, firewall, seguridad perimetral seguridad en equipos de los usuarios, internet, es decir, aspectos relacionados con el hardware.

2.3.2. Alcance

Este proyecto busca cubrir a nivel de fases los puntos más sensibles de la información teniendo como meta el control y administración de esta sin perder con las nuevas tecnologías el aseguramiento del bien más importante y el activo más esencial la información.

Tabla 1: Fases del proyecto

Fases	Actividades generales
Fase 0. Revisión de documentación	Recopilar la información de la compañía en cuanto a las políticas de seguridad Revisar los controles y la documentación asociada Identificar la necesidad

Fase 1. Seguridad Servidores	Evaluación de la infraestructura. Verificación del directorio activo Verificación de las políticas de contraseñas. Verificación seguridad en el servicio de correo. Verificación de los Firewall
Fase 2. Seguridad Entorno usuario final	Estado de roles de usuarios y perfiles. Seguridad de la información en portátiles y uso Administración y manejo de dispositivos móviles. Uso de dispositivos usb Estudio entorno antivirus
Fase 3. Seguridad bases de datos	Análisis de vulnerabilidades de bases de datos Manejo de seguridades Backup y contingencias

2.4.Objetivos

2.4.1. Objetivo General

Evaluar el Sistema de Gestión de Seguridad de la Información (SGSI) enfocado a los procesos del área de Tecnología e Infraestructura (TI)

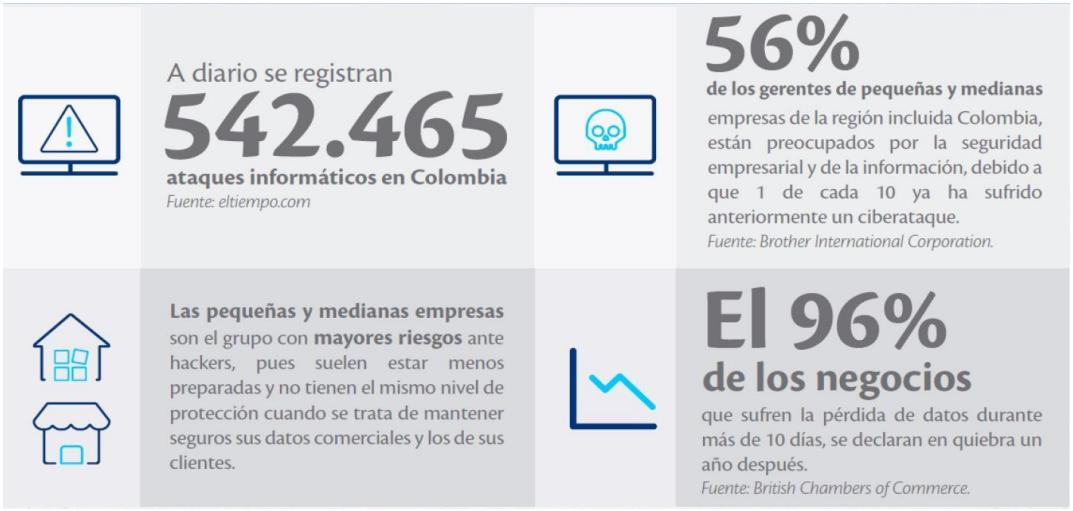
2.4.2. Objetivos Específicos

- Identificar el estado actual de los procesos existentes en el área de TI
- Identificar los riesgos actuales para el alcance en el SGSI
- Establecer la brecha de seguridad entre los procesos y el SGSI bajo la norma ISO27001:2013
- Establecer los parámetros para el diseño y planeación de un SGS

2.5.Marco Teórico

2.5.1. Marco conceptual

Siendo la información, el activo más preciado en las organizaciones, es entonces relevante tomar en serio la seguridad de la información y la infraestructura informática que la soporta. A continuación, algunos datos compartidos en el Tigo Une Business Meeting de 2018, donde se evidencia el crecimiento que se viene presentado año tras año sobre los ataques informáticos que se registran en Colombia:



Por ello nuestra investigación se enfoca en un tema que tiene alta relevancia en las organizaciones para evitar la pérdida de información y funcionalidad del negocio para así mantener la integridad, disponibilidad y confiabilidad de la información

2.5.1.1.Marco Histórico, antecedentes o estado del arte

a. Antecedentes Generales

Es necesario considerar que para toda empresa a nivel nacional e internacional la información es considerado un recurso indispensable para el desarrollo de su actividad diaria, ante esto se debe evitar a toda costa la pérdida, distorsión o uso inadecuado de la misma.

Por lo anterior, toda empresa debe tener una política de seguridad de la información clara que propenda por evitar el acceso desautorizado que pueda ocasionar problemas tanto a nivel interno como externo de la misma.

Cada vez es más sencilla la forma de interconexión a través de las diferentes redes informáticas lo que hace más vulnerable toda la organización relacionada con el manejo y control de la información, por esto se debe tener la disciplina necesaria que dicte los métodos y procedimientos para un correcto procesamiento y almacenamiento temporal y final de los datos. La finalidad de este trabajo es desarrollar el proceso necesario para lograr que las diferentes empresas que tengan a su haber el manejo de gran cantidad de información se interesen por adoptar un sistema que sea replicable sin importar el sector al que se esté dedicando su actividad social y/o comercial.

b. Antecedentes del proyecto

Tal y como lo expresa Computer Security Institute (CSI) de San Francisco las amenazas de incidentes en la red son básicamente producidos por elementos dentro de las mismas empresas investigadas. Además de esto cada vez son más diversos los posibles ataques cibernéticos que pueden presentarse, hace solo unos lustros eran ataques básicos como troyanos o spyware pero

ahora debido a la sofisticación de los sistemas y al avance que se viene presentando en cuanto al manejo de la información existen infinidad de amenazas las cuales deben ser reconocidas y atacadas para lograr un procedimiento que permita la seguridad informática hacia dentro y fuera de las empresas.

Para esto debemos tener claro aspectos como:

- ¿Qué información se debe proteger?
- ¿Quién la debe proteger?
- ¿Cuál es la información importante y cual la banal que no resulta indispensable para la seguridad de la empresa?

Estas preguntas son el inicio de todo el proceso del diseño de las políticas de seguridad, para lograr de esta manera tener los recursos adecuados y a su vez conocer los costos reales de su implementación.

Como principios claves para el desarrollo de cualquier política de seguridad puede considerarse:

1. La CONFIDENCIALIDAD; referente a la privacidad que debe tener toda la información almacenada.
2. La INTEGRIDAD; referente a la validez, confiabilidad y asegurabilidad de no duplicidad de la misma.
3. La DISPONIBILIDAD; la información siempre debe estar segura, pero es necesario que siempre pueda ser consultada y verificada por el personal encargado de la política.

Es importante, por último, tener presente que:

> La implementación de políticas de seguridad informática en una organización es una solución que no solo busca proteger, preservar y administrar de una manera eficiente todo tipo de recursos con los que cuenta una organización, sino que también busca dar una solución, prevenir, evitar, controlar y minimizar los daños de incidentes que afectan a la organización. (Agudelo, 2014, pág. 20)

c. Hipótesis

Teniendo en cuenta que día a día todas las empresas tienen más necesidad de utilizar modelos sistematizados para difundir y guardar la información necesaria para su desarrollo y funcionamiento, dichas empresas, ¿cuentan con modelos de seguridad eficaces, que los haga menos vulnerables ante ataques cibernéticos que puedan apoderarse de información confidencial que pueda poner en peligro la razón de ser de la compañía?

3. CAPÍTULO 2

3.1.Metodología / Estrategias

Figura No 2. Esquema de proceso metodológico

Para ello se ha definido el siguiente proceso para la elaboración del proyecto:

Análisis

- Estudio y verificación del actual sistema de gestión de seguridad de la información.
- Identificación del alcance y objetivos
- Recolección de hallazgos y activos críticos.
- Clasificación de los resultados y análisis de riesgos a partir de una identificación de amenazas, fuentes, vulnerabilidades, cuantificación de impacto y probabilidad y cálculo del riesgo.

Planeación

- Elaboración estructura de trabajo
- Recolección de requerimientos
- Definición de entregables y recursos
- Cronograma

3.2. Grupo De Estudio

Tabla 2. Equipo de trabajo

RECURSO	**DESCRIPCIÓN**	**INSTITUCIÓN**
Ingeniero civil Jairo Andrés Acosta Aristizabal	Miembro del proyecto	UNAD
Ingeniero de sistemas René Mauricio Barrera Tamayo	Miembro del proyecto	UNAD
Administradora de empresas Yudy Vanessa Sandoval Arnago	Miembro del proyecto Analista Infraestructura y Seguridad informática	UNAD – Enka de Colombia
Miryam Zapata Castrillón	Coordinadora Infraestructura	Enka de Colombia
Luis Fernando Vallejo	Gerente	Enka de Colombia

3.3 Unidad de análisis

Para este proyecto, la unidad de análisis se enfocó en la revisión de los estudios realizados en el 2014 sobre los procesos. Relacionados con la seguridad de la información en Enka de Colombia.

Los procesos para tener en cuenta son:

Política de seguridad

Monitoreo del Sistema de Gestión de la Seguridad de la Información

Gestión de activos (Hardware y Software)

Control de acceso y seguridad física

Continuidad del Negocio

Análisis de riesgos

Matriz y mapa de riesgos.

3.3.Cronograma

Tabla 3. Cronograma

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	MES 7	MES 8	MES 9	MES 10	MES 11	MES 12
Conocimiento de la normatividad								x	X			
Revisión de los procesos, documentación y políticas existentes									X			
Definir los alcances a aplicar y evaluar									X	x		
Evaluar el modelo para el análisis de riesgos y clasificación de proyectos según su criticidad. Verificación de los esquemas de seguridad en infraestructura										x	x	
Entrega modelo sugerido											x	

3.5 Presupuesto

Tabla 4. Presupuesto

RECURSO	DESCRIPCION	PRESUPUESTO ($)
Equipo Humano	Grupo de investigación	50.000.000
Equipos y Software	Computadores para los investigadores	10.000.000
Viajes y Salidas de Campo	No aplica	0
Materiales y suministros	No aplica	0
Bibliografía	Documentación de procesos y procedimientos	0
TOTAL		**60.000.000**

4. CAPÍTULO 3

4.1. Análisis de Resultados

En las visitas realizadas a la compañía, se revisa la documentación existente y las configuraciones aplicadas sobre su infraestructura. Con ello se evidencia los siguientes hallazgos:

Revisión de las políticas para la seguridad de la información

"Se definirá un conjunto de políticas de seguridad de la información, aprobado por la administración, publicado y comunicado a los empleados y colaboradores externos." (ISO/IEC 2. , 2013, pág. 2)

Procesos identificados

PW-15-007 Política de seguridad informática

Hallazgo positivo

Cuenta con políticas de seguridad documentadas, publicadas y aplicadas a los procesos de informática. El documento se encuentra en la Intranet de la compañía y actualizado a las necesidades de seguridad que exige el entorno. Adicionalmente se tienen controles implementados para garantizar el cumplimiento (ver figura 7).

El área de informática cuenta con un portal documental con toda la documentación requerida y relacionada con los procesos administrativos, técnicos y operativos para garantizar la continuidad de los servicios.

Hallazgo negativo

No se evidencia una oportunidad de mejora.

Organización de la Seguridad de la Información

Con la Organización de la Seguridad de la Información se puede establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización. A su vez permite mantener la seguridad de que los recursos de tratamiento de la información de los activos de información de la organización sean accesibles por terceros. (ISO/IEC 2. , 2013, pág. 4).

Procesos identificados

PQ01182 – Procedimiento de Selección

Hallazgo positivo

Los roles, responsabilidades y cargos de la compañía se encuentras correctamente definidos y documentados.

Hallazgo negativo

Aún sigue pendiente la creación y asignación del cargo responsable del SGSI

La segregación de funciones

"Conflicto de funciones y áreas de responsabilidad deben estar separados para reducir las oportunidades de modificación o mal uso de los activos de la organización no autorizado o involuntario." *(ISO/IEC 2. , 2013, pág. 4)*

***Procesos identificados*.**

No se evidencia la existencia de un documento físico donde se pueda verificar el proceso.

***Hallazgo Positivo*.**

Se evidencia la existencia de roles y cargos definidos conformes a la estructura organizacional de la compañía.

***Hallazgo Negativo*.**

No se evidencia.

Política de dispositivo móvil

"La política y el apoyo a las medidas de seguridad serán adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles." (ISO/IEC 2. , 2013, pág. 4)

Procesos identificados.

PW-15-007 Política de seguridad informática.

Hallazgo Positivo.

La compañía no permite la conexión de dispositivos móviles a las conexiones corporativas existentes. Para ello cuenta con un servicio de internet adicional para la conexión de dichos dispositivos. Dicha conexión no se enlaza con la red de producción.

Hallazgo Negativo.

Importante revisar y ajustar la política para la conexión de dispositivos móviles. Al usuario conocer la contraseña del acceso al Internet libre, puede llegar a conectar un equipo corporativo en dicha red y puede presentar una vulnerabilidad de seguridad.

Seguridad de los Recursos Humanos

> Con la Seguridad de los Recursos Humanos se puede definir las responsabilidades de la seguridad antes de la contratación laboral mediante la descripción adecuada del trabajo, los términos y condiciones del empleo. Para asegurar que los empleados, contratistas y terceras partes son conscientes de las amenazas de seguridad, de sus responsabilidades y obligaciones y que están provistos para cumplir con la política de seguridad de la organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos. (ISO/IEC 2. , 2013, pág. 9)

Procesos identificados.

FQ-01-001 SELECCIÓN INDUCCIÓN, COMPETENCIAS

Hallazgo Positivo.

Se evidencia la existencia de un proceso que define los lineamientos sobre la solicitud de nuevo personal. Se evidencia que existe un documento donde se especifica el tipo de evaluación por realizar en cada proceso de selección según el rol o cargo a desempeñar.

Hallazgo Negativo.

Sin evidencias

Responsabilidades de gestión

“Gestión pedirán a todos los empleados y contratistas a aplicar la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.” (ISO/IEC 2. , 2013, pág. 9)

Procesos identificados.

FQ-01-001 SELECCIÓN INDUCCIÓN, COMPETENCIAS.

Hallazgo Positivo.

Se evidencia que existen contratos a proveedores y contratistas donde se incluyen cláusula de confidencialidad de la información.

Se evidencia que se hacen entrenamientos sobre las políticas.

Se evidencia la existencia de controles para monitorizar el cumplimiento de las políticas de seguridad, los cuales son reportados en una aplicación.

Hallazgo Negativo.

Sin evidencias. Proceso bien implementado.

Concienciación sobre la seguridad de la información, la educación y la formación

"Todos los empleados de la organización y, en su caso, los contratistas deberán recibir una educación adecuada sensibilización y formación y actualizaciones periódicas en las políticas y procedimientos de la organización, que sea relevante para su función de trabajo." (ISO/IEC 2. , 2013, pág. 9)

Procesos identificados.

FQ-01-001 Entrenamiento PQ-01-181 Procedimiento de entrenamiento.

Hallazgo Positivo.

Se evidencia la realización de entrenamientos sobre el manejo de la información a todas las personas administrativas cuando ingresan.

Se evidencia el envío de correos denominados tips de seguridad donde se educa a los usuarios en buenas prácticas de seguridad.

Hallazgo Negativo.

No existe evidencia de entrenamientos en políticas de seguridad para contratistas, proveedores, empleados.

Gestión de Activos

> "Con la Gestión de Activos se puede alcanzar y mantener una protección adecuada de los activos de la Organización ya que todos los activos estarían justificados y tendrían asignado un propietario quien sería el responsable de un mantenimiento adecuado de los controles no obstante, el propietario permanece como responsable de la adecuada protección de los activos para así clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento." (ISO/IEC 2. , 2013, pág. 13)

Inventario de activos

"Los activos asociados a las instalaciones de procesamiento de información y la información deben ser identificados y un inventario de estos bienes serán elaborados y mantenidos." (ISO/IEC 2. , 2013, pág. 13)

Procesos identificados.

No se evidencia la existencia de un documento físico donde se pueda verificar el proceso.

Hallazgo Positivo.

Se evidencia que el área de plataforma maneja varios inventarios de activos de información en archivos de Excel (hardware y software).

Hallazgo Negativo.

No existe un proceso documentado para el inventario de activos.

No se tiene indicadores de gestión de los inventarios

No se tiene una aplicación que facilite la gestión de activos. Proceso manual.

Uso aceptable de los activos

"Las reglas para el uso aceptable de la información y de los activos asociados a las instalaciones de procesamiento de información y la información deben ser identificados, documentados e implementados." *(ISO/IEC 2. , 2013, pág. 14)*

Procesos identificados.

PW-15-007 Política de seguridad informática.

Hallazgo Positivo.

Se evidencia que en el proceso de inducción de nuevos empleados se hace mención del trato y manejo de equipos que se les asigna. En las políticas de seguridad de la compañía en el ítem 2.9 se hace alusión al uso del puesto de trabajo.

Hallazgo Negativo.

No existe un documento de responsabilidad frente a los recursos que se les entregan a los empleados

Retorno de los activos

"Todos los empleados y usuarios de la fiesta externa deberán devolver todos los activos de la organización en su poder a la terminación de su empleo, contrato o acuerdo." (ISO/IEC 2. , 2013, pág. 15)

Procesos identificados.

Procedimiento Actualización Usuarios.

Hallazgo Positivo.

Se evidencia la existencia de un procedimiento que especifica las actividades de retiro de usuario de los sistemas de información.

Hallazgo Negativo.

Sin evidencias

Manejo de activos

"Los procedimientos para el manejo de los activos deberán desarrollarse y aplicarse de conformidad con el esquema de clasificación de la información aprobada por la organización." (ISO/IEC 2. , 2013, pág. 16)

Procesos identificados.

No se evidencia la existencia de un documento físico donde se pueda verificar este proceso.

Hallazgo Positivo.

Se tiene definido un archivo de inventario donde se describe información del hardware como serial, service tag, modelo. De igual forma se describe el área a la que corresponde, responsable, fecha de asignación, entre otros. Esto mismo se aplica para los archivos de registros de inventarios de los dispositivos como impresoras, Acces Point y Switches.

Hallazgo Negativo.

No existe un procedimiento de manejo de inventarios

No se evidencia dentro de los inventarios los monitores

No se evidencia inventarios para contratistas, proveedores internos y externos.

Gestión de soportes extraíbles

"Los procedimientos se aplicarán para la gestión de medios extraíbles de acuerdo con el esquema de clasificación adoptado por la organización." (ISO/IEC 2. , 2013, pág. 17)

Procesos identificados.

PW-15-007 Política de seguridad informática.

Hallazgo Positivo.

Existe una estrategia que involucra el manejo y manipulación de medios extraíbles para este caso manejo de discos externos.

Existen políticas de antivirus para el bloqueo de medios extraíbles aplicados al área operativa de planta, además cuenta con políticas de directorio activo que maneja restricciones de accesos en la mayoría de los equipos operativos.

Existen logs donde está el registro de la conexión de uso de medios extraíbles.

Hallazgo Negativo.

No se evidencia el monitoreo periódico de la conexión de medios extraíbles.

La eliminación de los medios de comunicación

"Medios deberán ser desechados de forma segura cuando ya no es necesario, utilizando procedimientos formales." (ISO/IEC 2. , 2013, pág. 18)

Proceso identificados.

PW-15-007 Política de seguridad informática.

Hallazgo Positivo.

Se evidencia que se hace una disposición adecuada de los activos para dar de baja en donde se elimina todo tipo de información corporativa antes de esto.

Se evidencia que la entrega de chatarra tecnológica.

Hallazgo Negativo.

No se evidencia la existencia de un proceso donde se definan los pasos a seguir en caso de la eliminación segura de equipos, eliminación de información y datos.

Control de Acceso

> "Con el Control de Acceso se puede controlar los accesos a la información, los recursos y los procesos de negocio en base a las necesidades de seguridad de la Organización, se puede establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad para Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información. Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición, a su vez se puede considerar los riesgos de trabajar en entornos desprotegidos y aplicar la protección conveniente cuando se trate de informática móvil." (ISO/IEC 2. , 2013, pág. 19)

Política de control de acceso

"Se establecerá una política de control de acceso, documentado y revisado en base a los requisitos de seguridad de negocios y de información." (ISO/IEC 2. , 2013, pág. 19)

Procesos identificados.

PW-15-007 Política de seguridad informática

FQ-01-001-Seguridad física

Hallazgo Positivo.

Se evidencia que se tiene una política sobre el control de acceso a la información y se sigue un proceso para solicitarlo.

Existe un aplicativo que soporta este proceso de control de acceso.

Se evidencia una adecuada implementación de un sistema de control de acceso a los centros de cómputo y a la empresa.

Se cuenta con la clasificación de la información y de la clasificación de los perfiles de acceso

Hallazgo Negativo.

No se evidencia

El acceso a las redes y los servicios de red

"Los usuarios sólo deberán disponer de acceso a los servicios de red y de la red que han sido específicamente autorizados para su uso." *(ISO/IEC 2. , 2013, pág. 20)*

Procesos identificados.

PW-15-007 Política de seguridad informática; Procedimiento Solicitud de terceros; Actualización de usuarios - Ingreso o Retiro.

Hallazgo Positivo.

Se evidencia que se tiene un proceso de solicitud de ingreso de usuario donde se especifica los servicios a asignarle y recursos.

Se evidencia que existe un proceso para servicio de terceros.

Se evidencia la existencia de un archivo de permisos de carpetas en servidores.

Se evidencia un check list para revisiones de seguridad en usuarios y servidor de nómina categorizado como servidor crítico.

Se evidencia la existencia de un proceso y un formato para la solicitud de conexión VPN.

Hallazgo Negativo.

Existe parcialmente información donde se evidencia el control sobre la seguridad en la red. Hay ausencia de un proceso documentado y definido.

Gestión de derechos de acceso privilegiado

"La asignación y utilización de los derechos de acceso preferente se deberá restringirse y controlarse." (ISO/IEC 2. , 2013, pág. 22)

Procesos identificados.

Actualización de usuarios - Ingreso o Retiro.

Hallazgo Positivo.

Se tiene dentro del proceso de ingreso a la compañía para el área de plataforma asignar unos servicios a determinados grupos de directorio activo según la función.

Hallazgo Negativo.

Sin evidencia

Gestión de la información de autenticación de secreto de los usuarios

"La asignación de la información secreta de autenticación se controla a través de un proceso de gestión formal." (ISO/IEC 2. , 2013, pág. 22)

Procesos identificados.

PW-15-007 Política de seguridad informática.

Hallazgo Positivo.

Se evidencia que en las políticas de seguridad se describe el manejo de contraseñas igualmente se tienen tips de seguridad enviados a todo el personal educando la importancia, uso, creación de contraseñas seguras;

Se evidencia la existencia de políticas de grupo de dominio en cuanto a seguridad de contraseñas longitud mínima de 8 caracteres, bloqueo de contraseña 3 intentos fallidos, cambio de contraseña cada 30 días.

Hallazgo Negativo.

Sin evidencia

Revisión de los derechos de acceso de usuario

"Los propietarios de activos revisarán los derechos de acceso de los usuarios a intervalos regulares". (ISO/IEC 2. , 2013, pág. 23)

Procesos identificados.

Procedimiento de Revisión Seguridad.

Hallazgo Positivo.

Se evidencia que se tiene incorporado por el jefe de infraestructura realizar unas revisiones semanales en cuanto a Directorio Activo, Accesos a internet (Proxy), conexiones VPN.

Igualmente se evidencian reportes de usuarios activos, inactivos, y una serie de reportes a nivel de dominio de manera que se logren identificar inconsistencias.

Se evidencia la realización de reportes de vulnerabilidades de servidores cada 3 meses.

Hallazgo Negativo.

Todas las actividades SGSI no están documentadas en el proceso de "Procedimiento de Revisión Seguridad".

Restricción de acceso Información

“El acceso a las funciones de información y sistema de aplicación se limitará de acuerdo con la política de control de acceso.” (ISO/IEC 2. , 2013, pág. 25)

Procesos identificados.

Metodología de Desarrollo ENKA; Actualización de usuarios - Ingreso o Retiro.

Hallazgo Positivo.

Existe un proceso denominado “Metodología de desarrollo ENKA”.

La Administradora de base de datos evidencia la existencia de un formato de manejo de seguridades.

Se evidencia en el área de plataforma un proceso de ingreso y retiro donde se especifica el rol del usuario, aplicaciones a instalar, permisos.

Hallazgo Negativo.

Se debe reforzar el control relacionado con la propiedad, la asignación de permisos y el acceso a las carpetas en los servidores file server.

Sistema de gestión de contraseñas

"Sistemas de gestión de contraseña deben ser interactivas y se asegurarán de contraseñas de calidad." (ISO/IEC 2. , 2013, pág. 26)

Procesos identificados.

PW-15-007 Política de seguridad informática.

Hallazgo Positivo

Se evidencia que en las políticas de seguridad se describe el manejo de contraseñas, creación de contraseñas seguras.

Se evidencia la existencia de políticas de grupo de dominio en cuanto a seguridad de contraseñas longitud mínima de 8 caracteres, bloqueo de contraseña 3 intentos fallidos, cambio de contraseña cada 30 días.

Se evidencia uso de aplicación de encripción de equipos (doble autenticación) para los equipos críticos asignados a los usuarios.

Hallazgo Negativo.

El uso del sistema de encripción es limitado a un número reducido de usuarios. Se ha

aumentado el número de usuarios móviles lo que hace necesario ampliar la cobertura.

Control de acceso al código fuente del programa

"Se debe limitar el acceso al código fuente del programa" *(ISO/IEC 2. , 2013, pág. 28)*

Procesos identificados.

Metodología de Desarrollo ENKA.

Hallazgo Positivo.

Se evidencia la existencia de una metodología de desarrollo en las etapas de desarrollo e implementación el manejo del código fuente.

Se evidencia la existencia de repositorios de los códigos fuente en un servidor con las seguridades adecuadas.

Hallazgo Negativo.

No se evidencia.

Criptografía

Con la criptografía se busca proteger la integridad, confidencialidad y autenticidad de la información. En este caso, a través de dos controles, lo que propone es desarrollar una adecuada política de empleo de estos controles criptográficos y administrar las claves que se emplean de forma consciente." (ISO/IEC 2. , 2013, pág. 28)

Política sobre el uso de controles criptográficos

"Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollado e implementado." (ISO/IEC 2. , 2013, pág. 28)

Procesos identificados.

PW-15-007 Política de seguridad informática.

Hallazgo Positivo.

Se evidencia que existe un programa de cifrado adquirido por la empresa cuyo uso está destinado al cifrado de discos en usuarios con información sensible, Presidencia, Vicepresidencias, Jefes de división, Costos, Ventas.

Hallazgo Negativo.

No se evidencia un modelo de encripción para bases de datos SQL, para datos de aplicaciones administrativas, para discos externos que salen con información sensible de la empresa.

Gestión de claves

"Una política sobre el uso, la protección y la duración de las claves criptográficas se desarrolló e implementó a través de todo su ciclo de vida." (ISO/IEC 2. , 2013, pág. 29)

Procesos identificados.

PW-15-007 Política de seguridad informática.

Hallazgo Positivo.

Se evidencia que el software PGP universal server ofrece un manejo de llaves óptimo esto aplicado a los usuarios que lo tienen instalado.

Hallazgo Negativo.

No se evidencia una política de controles criptográficos y en qué caso son necesarios.

No se evidencia un modelo de encripción para bases de datos SQL, para datos de aplicaciones administrativas, para discos externos que salen con información sensible de la empresa

La protección contra amenazas externas y ambientales

"La protección física frente a los desastres naturales, ataques maliciosos o accidentes debe ser diseñado y aplicado." (ISO/IEC 2. , 2013, pág. 29)

Procesos identificados

PH 93 409 – Plan General Evacuación

PH-93-413-panorama riesgos.

Hallazgo Positivo.

Existen procesos y están alineados con la ISO18001.

Hallazgo Negativo.

No se evidencian

Trabajar en zonas seguras

"Los procedimientos para trabajar en las áreas de seguridad deben ser diseñadas y aplicadas." (ISO/IEC 2. , 2013, pág. 33)

Procesos identificados.

FQ-01-001 SEGURIDAD FÍSICA.

Hallazgo Positivo.

Se evidencian la existencia de procesos y están alineados con la ISO18001.

Los procesos están documentados y existen registros que lo evidencian.

Se evidencia el uso del carnet y tarjetas de acceso para el ingreso a áreas segura.

Se evidencia que en algunas zonas se usan estrategias de control de acceso por medio de llaves físicas son certificados por la BASC (Business Alliance for Secure Commerce).

Se evidencia letreros que evidencien la existencia de cámaras de seguridad en la empresa.

Hallazgo Negativo.

Sin evidencia.

Zonas de entrega y carga

"Los puntos de acceso, tales como las zonas de entrega y de carga y otros puntos, donde personas no autorizadas puedan entrar en los locales se deberán controlar y, si es posible, aislada de las instalaciones de procesamiento de información para evitar el acceso no autorizado." (ISO/IEC 2. , 2013, pág. 33)

Procesos identificados.

PR-14-002 Entrada y salida de personal.

Hallazgo Positivo.

Se evidencia la existencia de controles a nivel de hardware como a nivel de personas

Los procesos están documentados y existen registros que lo evidencian

Se evidencia el uso del carnet y targets de acceso para el ingreso a áreas segura.

Se evidencia que en algunas zonas se usan estrategias de control de acceso por medio de llaves físicas son certificados por la BASC (Business Alliance for Secure Commerce).

Se evidencia un proceso o procedimiento para el manejo de planilla/formato ingreso herramientas contratistas.

Hallazgo Negativo.

No se evidencia un proceso para el manejo de planilla de control ingreso de portátiles

Emplazamiento y Protección del equipo

"El equipo debe estar ubicado y protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado." (ISO/IEC 2. , 2013, pág. 34)

Procesos identificados.

PH-93-413-panorama riesgos.

Hallazgo Positivo.

Se evidencia la existencia de procesos y están alineados con la ISO18001

Se evidencia la existencia de análisis de riesgos ambientales documentados.

Hallazgo Negativo.

No se evidencian.

Seguridad del cableado

"Energía, cableado estructurado y telecomunicaciones que transporta datos o el apoyo a los servicios de información debe ser protegido contra la intercepción, interferencia o daños." (ISO/IEC 2. , 2013, pág. 35)

Procesos identificados.

FQ-01-001 Mantenimiento De La Plataforma Informática

Hallazgo Positivo.

Se evidencia una adecuada ejecución de los proyectos relacionados con el cableado.

Se evidencia una estandarización del cableado de redes.

Se evidencian planos actualizados

Hallazgo Negativo.

No hay cableado certificado en un 80% de la empresa

No se cumple el estándar en la terminación de cableado

Se evidencia una red paralela a la administrada por TI y que es administrada por instrumentación que no cumple con los mismos estándares.

El mantenimiento del equipo

"El equipo debe mantenerse correctamente para asegurar su continua disponibilidad e integridad." *(ISO/IEC 2. , 2013, pág. 35)*

Procesos identificados.

FQ-01-001 Mantenimiento De La Plataforma Informática.

Hallazgo Positivo.

Se evidencia la existencia de un programa de mantenimientos de equipos tanto lógico como físico

Existe un indicador de mantenimiento en el que se evidencia cada mes en los grupos primario de informática.

Hallazgo Negativo.

Sin evidencias

Seguridad de los equipos y de los activos fuera del establecimiento

"Seguridad se aplicará a los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de los locales de la organización." (ISO/IEC 2. , 2013, pág. 36)

Procesos identificados.

FQ-01-001 Seguridad Física.

Hallazgo Positivo

Se evidencia la existencia de un proceso de control de salida de equipos de la empresa.

Hallazgo Negativo.

No existe un sistema de guayas en los equipos portátiles

Las personas de seguridad no tienen claridad cuales portátiles son de la compañía y cuales son personales.

La seguridad para los portátiles de la compañía que se extraen de la organización está parcialmente aplicada. Se deben aplicar controles que refuercen la seguridad a conexiones externas.

Equipos de usuario Desatendido

"Los usuarios deberán asegurarse de que el equipo desatendido tiene la protección adecuada." *(ISO/IEC 2. , 2013, pág. 37)*

Procesos identificados.

PW-15-007 Política de seguridad informática.

Hallazgo Positivo.

Se evidencia la existencia de un proceso para los servidores y uso de servicios terminal services

Se evidencia la existencia de tips de seguridad educando al usuario con tema equipos desatendidos.

Hallazgo Negativo.

Todos los usuarios no bloquean sus equipos al ausentarse de sus puestos de trabajo.

Se debe ajustar el control para el tiempo de inactividad del equipo de cómputo. En algunos equipos no funciona.

Política de escritorio y pantalla Despejado

"Se adoptarán una política de escritorio limpio de papeles y soportes de almacenamiento extraíbles y una política de la pantalla clara para las instalaciones de procesamiento de información." (ISO/IEC 2. , 2013, pág. 38)

Procesos identificados.

PW-15-007 Política de seguridad informática

Hallazgo Positivo.

Se evidencia a través de tips de seguridad documentos educando al usuario con el uso de escritorio despejado.

Hallazgo Negativo.

No se evidencia una política de escritorio y pantalla despejada

No se evidencia registros de monitoreo periódico para las aplicaciones de la política de escritorio y pantalla despejada.

Operaciones de Seguridad

"Con las Operaciones de Seguridad se puede asegurar la operación correcta y segura de los recursos de tratamiento de información donde se establecen responsabilidades y procedimientos para la gestión y operación de todos los recursos para el tratamiento de la

información, esto incluye el desarrollo de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias con los cuales se pueden monitorear su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se prestan cumplen con todos los requerimientos acordados con los terceros, también se requiere tener ciertas precauciones para prevenir y detectar la introducción de código malicioso y códigos móviles no autorizados por lo cual los usuarios deberían conocer los peligros que puede ocasionar el software malicioso o no autorizado y los administradores deberían introducir controles y medidas especiales para detectar o evitar su introducción."

Copia de seguridad de la información

"Las copias de seguridad de la información, el software y las imágenes del sistema se adoptarán y se prueban regularmente de acuerdo con un ic pol copia de seguridad acordado" *(ISO/IEC 2. , 2013, pág. 42)*

Procesos identificados.

Procedimiento de backup de la información Corporativa, Servidores, Función y Respaldo.

Hallazgo Positivo.

Se evidencia la existencia de un proceso de backup y recuperación para servidores, bases de datos, información corporativa

Una vez al año se tiene incorporadas buenas prácticas para realizar simulacros de recuperación de servidores críticos.

Hallazgo Negativo.

Sin evidencia

El registro de eventos

"Los registros de eventos de grabación de las actividades del usuario, excepciones, fallas e información se producirán los eventos de seguridad, cuidados y revisiones regulares." (ISO/IEC 2. , 2013, pág. 43)

Procesos identificados.

Procedimiento de Revisión Seguridad.

Hallazgo Positivo.

Se evidencia la existencia de un proceso de revisiones diarias, semanales y mensuales de seguridad y estado de salud de la plataforma

Se evidencia la existencia de una biblioteca en el portal "informática" donde se guardan las evidencias y controles por año, por mes, por día.

Hallazgo Negativo.

Sin evidencia

Protección de la información de registro

"Instalaciones de registro y la información de registro se protegerán contra la manipulación y acceso no autorizado." (ISO/IEC 2. , 2013, pág. 44)

Procesos identificados.

Procedimiento de Revisión Seguridad, Manual Seguridad.

Hallazgo Positivo.

Se evidencia que en los controles establecidos las personas no se tienen acceso a modificar los log de los sistemas.

Hallazgo Negativo.

No se evidencia en el procedimiento de revisiones de seguridad los responsables del acceso a los logs, ni la protección a los mismos.

Sincronización de reloj

"Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o dominio de seguridad se sincronizan con una sola fuente de tiempo de referencia." (ISO/IEC 2. , 2013, pág. 45)

Procesos identificados.

Hora y Sincronización equipos, Situación de hora ENKA de Colombia

Hallazgo Positivo.

Se evidencia la existencia de un proceso incorporado para la sincronización de la hora de todos los equipos de ENKA desde el servidor NTP en este caso el controlador de dominio.

Hallazgo Negativo.

Se debe estructurar un documento con el procedimiento "hora y sincronización de equipos".

La instalación del software en los sistemas operativos

"Los procedimientos se llevarán a cabo para controlar la instalación de software en los sistemas operativos." (ISO/IEC 2. , 2013, pág. 45)

Procesos identificados.

PW-15-007 Política de seguridad informática, Manual del administrador de seguridad informática.

Hallazgo Positivo.

Se tiene incorporado controles de instalación de aplicaciones en equipos de usuarios

Se tiene incorporado un sistema de actualización de aplicaciones Microsoft mediante WSUS y en esquema de pruebas para servidores y usuarios.

Se evidencia el control de instalación de aplicaciones para el área administrativa desde medios extraíbles

Hallazgo Negativo.

No se evidencia implementación de un sistema de actualización de parches para programas distintos de Microsoft

Gestión de vulnerabilidades técnicas

"Información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan se obtendrá en el momento oportuno, la exposición de la organización a tales vulnerabilidades evaluado y tomado las medidas adecuadas para hacer frente a los riesgos asociados." (ISO/IEC 2. , 2013, pág. 46)

Procesos identificados.

Manual del administrador de seguridad informática.

Hallazgo Positivo.

Se tiene incorporado un proceso de chequeo de vulnerabilidades y test de penetración para el servidor y los usuarios de nomina

Se tiene incorporado en los mantenimientos de servidores chequeo de vulnerabilidades con el software de Microsoft Baseline Security analyzer.

Hallazgo Negativo.

No se evidencia que el proceso de chequeo de vulnerabilidades en los servidores este documentado en el manual del administrador de seguridad, ni la periodicidad con que se realiza, ni los planes de acción

No se evidencia la existencia de un chequeo de vulnerabilidades y test de penetración para los equipos de red y comunicaciones

No se evidencia la existencia de un chequeo de vulnerabilidades para los equipos de usuario críticos de la compañía diferentes a nomina como presidente, vicepresidentes, ventas, costos.

Seguridad en las Comunicaciones

"Con la Seguridad en las Comunicaciones se asegura la protección de la información en las redes y la protección de su infraestructura de apoyo, las cuales pueden cruzar las fronteras de la organización, exige la atención a los flujos de datos, implicaciones legales, monitoreo y la protección donde los medios son controlados y físicamente protegidos

además se establecen los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.” (ISO/IEC 2. , 2013, pág. 49)

Controles de red

“Las redes deberán ser gestionados y controlados para proteger la información en los sistemas y aplicaciones.” (ISO/IEC 2. , 2013, pág. 49)

Procesos identificados.

Manual del administrador de seguridad informática.

Hallazgo Positivo.

Se tiene un proceso incorporado para las revisiones de todos los servicios de plataforma

Se realizan monitoreos, diarios, semanales, mensuales.

Hallazgo Negativo.

Sin evidencia

Seguridad de los servicios de red

“Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red deben ser identificados e incluidos en los acuerdos de servicios de red, si estos servicios son prestados en la empresa o subcontratados.” (ISO/IEC 2. , 2013, pág. 49)

Procesos identificados.

Administrador de directorio Activo

Hallazgo Positivo

Se tiene para los dispositivos de red configurados los rol de accesos a los dispositivos administrador, operador

Hallazgo Negativo.

No existe documentación de cómo se configuran las seguridades de switches y Acces Point.

No se evidencia dentro del grupo de soporte técnico la limitación de acceso al directorio Activo (cualquiera puede agregar, modificar o eliminar)

Todo el grupo de soporte técnico tiene conocimiento de las contraseñas de administrador de dominio

Se tienen varios administradores de dominio

Las políticas y los procedimientos de transferencia de información

"Políticas de transferencia formales, procedimientos y controles deberán estar en su lugar para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación." (ISO/IEC 2. , 2013, pág. 51)

Procesos identificados.

PW-15-007 Política de seguridad informática.

Hallazgo Positivo.

Se tiene incorporado en los procesos de inducción y entrenamiento del personal nuevo explicar las buenas prácticas para el uso del correo electrónico, la transferencia de archivos, el uso de la red inalámbrica de visitantes y producción.

Hallazgo Negativo.

No existe una política para el manejo y transferencia de la información a clientes, proveedores, contratistas y empleados

La mensajería electrónica

"Información involucrada en la mensajería electrónica será debidamente preservada." (ISO/IEC 2. , 2013, pág. 52)

Procesos identificados.

No se evidencia la existencia de un documento físico donde se pueda verificar el proceso.

Hallazgo Positivo.

Se tiene incorporada la metodología IPSEC (abreviatura de Internet Protocol security) para las conexiones VPN (virtual private network).

Hallazgo Negativo.

No se tiene para el servicio de correo electrónico metodologías o canales de encriptados

Los acuerdos de confidencialidad o de no divulgación

"Requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, revisado y documentado regularmente." (ISO/IEC 2. , 2013, pág. 53)

Procesos identificados.

FQ-01-001 SELECCIÓN INDUCCIÓN, COMPETENCIAS

Hallazgo Positivo.

Se tiene una cláusula de confidencialidad de la información en el contrato laboral (sección 7.3).

Hallazgo Negativo.

Sin evidencias

Revisión técnica de las aplicaciones después de operar cambios de plataforma

"Cuando se cambian las plataformas de operación, aplicaciones críticas de negocio deben ser revisados y probados para asegurar que no hay impacto negativo en las operaciones de la organización o de la seguridad." (ISO/IEC 2. , 2013, pág. 58)

Procesos identificados.

FQ-01-001 MANTENIMIENTO DE LA PLATAFORMA INFORMÁTICA

Hallazgo Positivo.

Se tiene incorporado dentro de un proceso de actualización de plataforma realizar reuniones de planeación donde se establecen las actividades, responsables y pruebas

Para el caso de cambios en aplicaciones críticas se tiene documentados los casos de pruebas, funcionales y de seguridad, en algunos casos se hacen pruebas de vulnerabilidad externas.

Hallazgo Negativo

Sin evidencia

Restricciones en los cambios a los paquetes de software

"Las modificaciones a los paquetes de software se pondrán trabas, otros, las modificaciones necesarias y todos los cambios deben ser estrictamente controlados." (ISO/IEC 2. , 2013, pág. 59)

Procesos identificados.

FQ-01-001 DESARROLLO Y MANTENIMIENTO DE SOFTWARE APLICATIVO

FQ-01-001 MANTENIMIENTO DE LA PLATAFORMA INFORMÁTICA

Hallazgo Positivo.

En las aplicaciones que aplica se establecen logs de pruebas, esto se define en los requerimientos del software

Se establecen bloqueos para aplicaciones como el software de antivirus en los equipos de los usuarios, se bloquean funcionalidades del sistema operativo

Hallazgo Negativo.

Sin evidencias

Pruebas de aceptación del sistema

"Los programas de pruebas de aceptación y los criterios conexos se establecerán para los nuevos sistemas de información, actualizaciones y nuevas versiones." (ISO/IEC 2. , 2013, pág. 61)

Procesos identificados.

FQ-01-001 DESARROLLO Y MANTENIMIENTO DE SOFTWARE APLICATIVO

Hallazgo Positivo.

En el plan de pruebas se establecen los criterios de aceptación del software según el sistema de calidad y el monitoreo de defectos reportados.

Hallazgo Negativo.

Sin evidencias

Gestión de Seguridad de la Información de Incidentes

Con la Gestión de Incidentes se pueden establecer controles enfocados al tratamiento de los incidentes de seguridad y no sólo al reporte de los mismos, para garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas. (ISO/IEC 2. , 2013, pág. 67)

Responsabilidades y procedimientos

“Las responsabilidades y los procedimientos de gestión se establecerán para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.” (ISO/IEC 2. , 2013, pág. 67)

Procesos identificados.

PW-15-002-SOLICITUDES DE SERVICIO A LA DIVISIÓN DE INFORMÁTICA.

Hallazgo Positivo.

Se tiene un sistema donde se ingresan todos los incidentes que afectan la disponibilidad, integridad y confidencialidad, los cuales pueden ser reportados por todas personas de la compañía.

Dentro de los roles se tiene especificado la función de quienes ingresan y clasifican los incidentes de seguridad.

Hallazgo Negativo.

No existe una clasificación explicita que defina las solicitudes de servicios como incidentes de seguridad.

Informar sobre los eventos de seguridad de información

“Los eventos de seguridad de información se comunicarán a través de canales de gestión adecuadas tan pronto como sea posible.” (ISO/IEC 2. , 2013, pág. 68)

Procesos identificados.

PW-15-002-SOLICITUDES DE SERVICIO A LA DIVISIÓN DE INFORMÁTICA

Hallazgo Positivo.

En el entrenamiento inicial de los empleados se les informa el procedimiento a seguir para el reporte de incidentes.

Hallazgo Negativo.

No existe una clasificación explicita que defina las solicitudes de servicios como incidentes de seguridad

Presentación de informes de información debilidades de seguridad

"Se requiere que los empleados y contratistas que utilizan los sistemas y servicios de información de la organización para observar y reportar cualquier debilidad de seguridad de información observadas o sospechadas en los sistemas o servicios." (ISO/IEC 2. , 2013, pág. 69)

Procesos identificados.

PW-15-002-SOLICITUDES DE SERVICIO A LA DIVISIÓN DE INFORMÁTICA

Hallazgo Positivo.

Se tiene un proceso de ingreso y tratamiento de incidentes tanto para empleados como contratistas internos

Hallazgo Negativo.

Los contratistas y proveedores externos cumplen parcialmente el proceso de ingreso y tratamiento de incidentes

Valoración de eventos de seguridad de la información y toma de decisiones

"Se evaluarán los eventos de seguridad de información y se decidirá si han de ser clasificados como incidentes de seguridad de la información." (ISO/IEC 2. , 2013, pág. 69)

Procesos identificados.

FQ-01-001 MANTENIMIENTO DE LA PLATAFORMA INFORMÁTICA

Hallazgo Positivo.

Se tiene incorporado en los grupos primarios de informática mensuales el análisis de resultados de las solicitudes atendidas y los re procesos a través de indicadores, allí se establecen acciones correctivas o preventivas con sus respectivos planes de acción

Hallazgo Negativo.

No se evidencia la clasificación de incidentes de seguridad, ni la criticidad, ni tiempos de entrega.

Respuesta a incidentes de seguridad de la información

"Los incidentes de seguridad de información deberán recibir una respuesta de conformidad con los procedimientos documentados." (ISO/IEC 2. , 2013, pág. 69)

Procesos identificados.

FQ-01-001 MANTENIMIENTO DE LA PLATAFORMA INFORMÁTICA

Hallazgo Positivo.

Se evidencia la existencia de informes de gestión sobre incidentes los cuales son reportados a la dirección mensualmente.

Se tiene evidencia de la existencia de actas con los resultados del tratamiento a los incidentes y esta es aprobada por la dirección.

Hallazgo Negativo.

No está documentado el proceso donde se definen los tiempos de revisión y línea de mando.

Aprendiendo de los incidentes de seguridad de la información

"Los conocimientos adquiridos a partir del análisis y la resolución de incidentes de seguridad de información se utilizan para reducir la probabilidad o el impacto de los incidentes en el futuro." (ISO/IEC 2. , 2013, pág. 70)

Procesos identificados.

FQ-01-001 MANTENIMIENTO DE LA PLATAFORMA INFORMÁTICA

Hallazgo Positivo.

Se evidencia para los incidentes registros de la solución y tratamiento, en caso de requerirse se hacen acciones correctivas, preventivas y de mejoramiento

Hallazgo Negativo.

No está documentado el proceso para el tratamiento de incidentes de seguridad.

Aspectos de seguridad de información de la gestión de continuidad del negocio

> "Con los Aspectos de seguridad de información de la gestión de continuidad del negocio se pueden establecer controles para asegurar la redundancia de las instalaciones de tratamiento de información y así reducir, a niveles aceptables, la interrupción causada por los desastres y fallos de seguridad (que, por ejemplo, puedan resultar de desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación."

Información de planificación de continuidad de seguridad

"La organización debe determinar sus necesidades de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre." *(ISO/IEC 2. , 2013, pág. 71)*

Procesos identificados.

PLAN DE CONTINGENCIA PARA SISTEMAS DE INFORMACION

Hallazgo Positivo.

Se evidencia la existencia de procesos que aplican al plan de continuidad de negocios contienen la recuperación de los servidores y servicios críticos de plataforma garantizando la continuidad de la plataforma en un tiempo asumido por la empresa

Proceso de continuidad y contingencia es uno de los procesos más sólidos dentro de la organización

Hallazgo Negativo.

Sin evidencia

Verificar, revisar y evaluar la información de seguridad de continuidad

"La organización debe verificar los controles de seguridad de la información de continuidad establecido y aplicado a intervalos regulares con el fin de asegurarse de que son válidos y eficaces en situaciones adversas." (ISO/IEC 2. , 2013, pág. 73)

Procesos identificados.

PLAN DE CONTINGENCIA PARA SISTEMAS DE INFORMACION

Hallazgo Positivo.

El departamento realiza una vez al año como mínimo un simulacro para verificar que los procesos si sean efectivos la información queda registrada en actas de grupo de trabajo de soluciones planta, soluciones administrativas, infraestructura. Con los resultados de los simulacros se crean Acciones correctivas, preventivas y de mejoramiento.

Hallazgo Negativo.

Sin evidencia

Cumplimiento

"Con el Cumplimiento se pude evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad" (ISO/IEC 2. , 2013, pág. 74)

Disponibilidad de instalaciones para el procesamiento de la información

"Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir con los requisitos de disponibilidad." (ISO/IEC 2. , 2013, pág. 73)

Procesos identificados.

No se puede evidenciar la existencia de un documento físico donde se pueda verificar el proceso.

Hallazgo Positivo.

Existe evidencia dentro del proceso parte del proceso de continuidad de negocio con actividades relacionadas orientadas hacia la recuperación de los servidores de bases de datos y aplicaciones críticas

Hallazgo Negativo.

No se evidencia la existencia de un proceso consolidado con todas las actividades relacionadas al plan de continuidad de negocio de acuerdo a la norma ISO27001:2013

Cumplimiento

"Con el Cumplimiento se pude evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad" (ISO/IEC 2. , 2013, pág. 74)

Identificación de la legislación aplicable y los requisitos contractuales (Control 18.1.1.).

"Todos los requisitos pertinentes, legislativas estatutarias, reglamentarias y contractuales enfoque de la organización para cumplir con estos requisitos deberán ser identificados de manera

explícita, documentan y mantienen actualizados para cada sistema de información y la organización.” (ISO/IEC 2. , 2013, pág. 74)

Procesos identificados.

No se puede evidenciar la existencia de un documento físico donde se pueda verificar el proceso.

Hallazgo Positivo.

Existe dentro de los contratos cláusulas de confidencialidad, especificando términos legales entre las partes en el caso de contratistas y proveedores.

Se tiene clausulas en los contratos para el cuidado de la propiedad intelectual para contratistas y proveedores.

Hallazgo Negativo.

No se evidencia un documento donde se definan y estipulen las leyes aplicables en tema de seguridad informática en la compañía (Marco legal) y los controles efectuados para garantizar el cumplimiento de las mismas.

No se tienen en los contratos de empleados cláusulas de confidencialidad y de propiedad intelectual

Derechos de propiedad intelectual

“Los procedimientos apropiados se aplicarán para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y uso de productos de software propietario.” (ISO/IEC 2. , 2013, pág. 74)

Procesos identificados.

No se evidencia la existencia de un documento físico donde se pueda verificar el proceso.

Hallazgo Positivo.

Se tiene en los contratos una cláusula hacia la propiedad intelectual, cláusula de confidencialidad y manejo de la información

Dentro de las políticas existen secciones para la instalación de software.

Se monitorea periódicamente el software instalado en los equipos de la compañía

Hallazgo Negativo.

No se evidencia un documento donde se defina la periodicidad del monitoreo de software.

No se evidencian documentos de informes de los monitoreo hechos al software

No se evidencia incidentes asociados a la instalación de software no autorizado

Privacidad y protección de datos personales

"Privacidad y protección de la información de identificación personal que se garantizará a lo dispuesto en la legislación y la reglamentación en su caso pertinente." (ISO/IEC 2. , 2013, pág. 76)

Procesos identificados.

No se puede evidenciar la existencia de un documento físico donde se pueda verificar el proceso.

Hallazgo Positivo.

Se tiene controles de acceso a la información que garantizan la confidencialidad, integridad y disponibilidad.

Los documentos físicos están bajo llave en zonas seguras y solo pueden ser accedidos por personal autorizado

Se evidencia la existencia de procesos que muestran que hay seguridades a nivel de servidores, evidencias de capacitación a usuario en manejo de permisos en recursos compartidos, un control de llaves para manejo de archivos físicos

Se tiene incorporado dentro de las revisiones del departamento técnico realizar revisiones de seguridades en cada micro a su cargo.

Hallazgo Negativo.

La información no tiene ninguna clasificación.

No se evidencia la documentación de los procesos de clasificación y tipos de protección y cuidados que se tiene para cada tipo de información

No esta difundido el tratamiento de datos personales que hace la compañía y su finalidad de las personas.

No todas las zonas y espacios que son monitoreados y gravados son informados a las personas sobre su tratamiento y finalidad.

No existen procesos establecidos y documentados para el tratamiento de información de grabaciones de video y llamada.

El cumplimiento de las políticas y normas de seguridad

"Los gerentes deberán comprobar periódicamente el cumplimiento del tratamiento y los procedimientos de información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad." (ISO/IEC 2. , 2013, pág. 77)

Procesos identificados.

PW-15-007 Política de seguridad informática

Hallazgo Positivo.

Se evidencia dentro del portal de informática los seguimientos, actas de gestión, en el sistema track it se tienen las actividades y soluciones, en el sistema de acciones correctivas se tiene acciones establecidas para el manejo de incidentes de seguridad con su trazabilidad.

Se evidencia dentro de los contratos las obligaciones legales de las partes tanto para empleados como contratistas

Se evidencia en el reglamento de la empresa la orientación al cumplimiento de la norma Se evidencia en las evaluaciones de desempeño la evaluación del compromiso y el acatamiento de las normas

Hallazgo Negativo.

No se tiene una política donde se defina el tratamiento de la información segura y buenas prácticas

No se tienen establecidos controles para monitorizar y reportar todo uso indebido de los sistemas de información

No se tiene una política que describa la finalidad de los monitoreo a los servicios críticos de plataforma y áreas seguras (monitoreos de red, servicios, llamadas, videos)

No se tiene una estrategia de comunicación para todas las personas internas y externas sobre los monitoreos y su finalidad

No existe un proceso de revisión periódica del cumplimiento de los requerimientos legales.

No se evidencia las actas de revisión de los requerimientos legales

4.2.Análisis de Riesgos

A partir de los hallazgos, se identifican los aspectos críticos en los cuales la compañía debe definir un plan de acción y remediación para controlar y disminuir las brechas de seguridad y así contar con un SGSI más adecuado a la normatividad.

Hemos clasificado los resultados creando el análisis de riesgos por lo que se siguieron los siguientes lineamientos para la obtención final de la matriz:

- Identificación de las amenazas
- Identificación de las fuentes
- Identificación de las vulnerabilidades
- Cuantificación de impacto y probabilidad
- Cálculo de riesgo
- Cuantificación de la prioridad

Figura 3: Análisis Matriz de riesgos Seguridad

MATRIZ DE ANÁLISIS DE RIESGOS PARA LA SEGURIDAD						
PROCESO	RIESGOS	EVALUACIÓN		VALORACIÓN		
		PROBABILIDAD	SEVERIDAD	CALIFICACIÓN POR RIESGO	RIESGO INHERENTE DEL PROCESO	NIVEL DEL RIESGO INHERENTE
INFORMÁTICA	Ciberataque - ataque de virus informático	3	3	9	8	MEDIO
	Ciberataque - intrusión a los sistemas de información (secuestro de información)	2	4	8		
	Actos inconscientes o mal intencionados del recurso humano	3	4	12		
	Uso inapropiado de recursos informáticos (internet, correo electrónico)	3	2	6		
	No disponibilidad de los sistemas de información	2	4	8		
	Daños en los equipos de computo	3	1	3		
	Corte de energía	1	4	4		
	Fallas en las comunicaciones	3	4	12		
GESTIÓN HUMANA	Contratación personal no confiable (Personal que haya tenido algún proceso o antecedente Judicial activo)	4	3	12	13	ALTO
	Contratación de personal con antecedentes de consumo de sustancias psicoactivas	4	4	16		
	Contratación de personal con documentos falsos	4	4	16		
	Empleados con conductas delictivas o en contra de la empresa	3	4	12		
	Mal uso del nombre de Enka por uniformes con logo	3	3	9		
SEGURIDAD FISICA	Abaleo dentro de las instalaciones	4	3	12	13	ALTO
	Acceso no autorizado áreas de almacenamiento de contenedores llenos y vacíos	4	3	12		
	Accidente de tránsito dentro de la planta	2	4	8		
	Acto terrorista y/o atentado	2	5	10		
	Agresión de terceros a personal de seguridad	5	1	5		
	Consumo y/o comercialización de sustancias prohibidas	4	4	16		
	Disparo accidental dentro de la planta	4	4	16		
	Hurto al interior de las instalaciones	4	4	16		
	Ingreso de paquetes, objetos y/o correspondencia no autorizada o sospechosa	4	4	16		
	Ingreso de personas en estado de alicoramiento y/o consumo de drogas	5	3	15		
	Ingreso no autorizado a las instalaciones	4	4	16		
	Intrusión no autorizada a las instalaciones	4	4	16		
	Retraso en las rutas	5	2	10		
	Sabotaje	4	5	20		

ANALISIS DE RIESGOS

Proceso identificado	Amenaza	Fuente	Vulnerabilidad	Impacto	Probabilidad	Valor Riesgo	Criticidad	Promedio	Prioridad	Nivel PROB
Politicas	Desactualización	Personas	Falta de seguimiento a los procesos	2	100%	2	Tolerable	5.0	Critico	5
Politicas	Uso incorrecto	Personas, contratistas, proveedores	Deficiente entrenamiento y capacitación	3	50%	1.5	Tolerable	5.0		5
Politicas	incumplimiento	personas, contratistas, proveedores	Controles deficientes	5	100%	5	Critico	5.0		15
Politicas	Fuga de informacion	personas, contratistas, proveedores	Controles deficientes	5	50%	2.5	Tolerable	5.0		7.5

ANALISIS DE RIESGOS

Proceso identificado	Amenaza	Fuente	Vulnerabilidad	Impacto	Probabilidad	Valor Riesgo	Criticidad	Promedio	Prioridad	Nivel PROB
Monitoreo del SGSI	Desactualización	personas	Falta de seguimiento a los procesos	2	100%	2	Tolerable	2.5	Media	5
Monitoreo del SGSI	Fuga de informacion	personas, contratistas, proveedores	Falta de efectividad en los controles y monitoreo a los procesos criticos	3	50%	1.5	Tolerable	2.5		5
Monitoreo del SGSI	Incumplimiento	empleados	deficiente entrenamiento y capacitación sobre los proecesos como tambien monitoreo a los servicios criticos	5	50%	2.5	Tolerable	2.5		7.5
Monitoreo del SGSI	Intrusión	Personas maliciosas	Deficiente control de acceso y falta de monitoreo a los servicios criticos	3	20%	0.6	Aceptable	2.5		2
Monitoreo del SGSI	Pérdida de capacidad	Planeación de recursos	Falta de planeación	5	20%	1	Aceptable	2.5		3
Monitoreo del SGSI	Errores de código	Ingenieria de software Proveedor de software	Falta de verificación y validación Inadecuada selección de proveedor	3	20%	0.6	Aceptable	2.5		2

ANALISIS DE RIESGOS

Proceso identificado	Amenaza	Fuente	Vulnerabilidad	Impacto	Probabilidad	Valor Riesgo	Criticidad	Promedio	Prioridad	Nivel PROB
Contratacion y legalidad	incumplimiento	personas, contratistas, proveedores	Falta de clarida en los contratos en terminos de proteccion de la informacion	5	100%	5	Critico	5.0	Muy Alta	15
Contratacion y legalidad	fuga de informacion	personas, contratistas, proveedores	Falta de clarida en los contratos en terminos de proteccion de la informacion	5	60%	3	No tolerable	5.0		9
Contratacion y legalidad	Afectaciones legales	personas, contratistas, proveedores	Falta de clarida en los contratos en terminos de proteccion y uso de la informacion	5	40%	2	Tolerable	5.0		6

ANALISIS DE RIESGOS

Proceso identificado	Amenaza	Fuente	Vulnerabilidad	Impacto	Probabilidad	Valor Riesgo	Criticidad	Promedio	Prioridad	Nivel PROB
Analisis de riesgos	Errores de código	Ingeniería de software Proveedor de software	Falta de prosesos documentados	5	100%	5	Critico	4.5	Muy Alta	15
Analisis de riesgos	Fallas de funcionamiento	Configuración Personas	Falta de control de amenazas de factoers de riesgos	5	30%	1.5	Tolerable	4.5		4.5
Analisis de riesgos	Piratería	Personas maliciosas	Falta de controles eficientes para el control de acceos el desearrollo de software	5	40%	2	Tolerable	4.5		6
Analisis de riesgos	Códigos maliciosos	Personas maliciosas Empleados	Falta de controles para las uso de dispositivos moviles	5	80%	4	No tolerable	4.5		12
Analisis de riesgos	Pérdida de capacidad	Planeación de recursos	Falta de monitorea a los riesgos de seguridad	5	40%	2	Tolerable	4.5		6
Analisis de riesgos	Uso incorrecto	Personas	Falta de controles eficaces	5	90%	4.5	Critico	4.5		13.5
Analisis de riesgos	Daño de equipos por fallo eléctrico	Instalación eléctrica Sobrecarga Estática	Falta de controles eficases para la gestion del riesgo	5	20%	1	Aceptable	4.5		3
Analisis de riesgos	Daño equipo por desgaste	instalaciones, clima	Falta de controles eficaces	5	20%	1	Aceptable	4.5		3

ANALISIS DE RIESGOS

Proceso identificado	Amenaza	Fuente	Vulnerabilidad	Impacto	Probabilidad	Valor Riesgo	Criticidad	Promedio	Prioridad	Nivel PROB
Clasificacion y gestion de activos	Perdida de la informacion	Personas maliciosas Empleados	los activos no estan identificados	5	90%	4.5	Critico	4.5	Muy Alta	13.5
Clasificacion y gestion de activos	Fuga de informacion	Personas maliciosas Empleados	Falta de clasificacion de activos	5	90%	4.5	Critico	4.5		13.5
Clasificacion y gestion de activos	Uso incorrecto	Personas desinformadas	desconocimiento de los cuidados de cada activo de la informacion	5	100%	5	Critico	4.5		15
Clasificacion y gestion de activos	Pérdida de capacidad	Mantenimiento	falta de documentacion y revision de los activos y su estados	5	90%	4.5	Critico	4.5		13.5

ANALISIS DE RIESGOS

Proceso identificado	Amenaza	Fuente	Vulnerabilidad	Impacto	Probabilidad	Valor Riesgo	Criticidad	Promedio	Prioridad	Nivel PROB
Controles de accesos y seguridad fisica	Consulta no autorizada	Personas	Falta de documentacion y controles de acceso a los sistemas de informacion y areas seguras	5	20%	1	Aceptable	1.0	Baja	3
Controles de accesos y seguridad fisica	Robo de información	Personas	Falta de controles de acceso a los sistemas de informacion y areas seguras	5	20%	1	Aceptable	1.0		3
Controles de accesos y seguridad fisica	Alteración	Personas	Falta de controles de acceso a los sistemas de informacion y areas seguras	5	20%	1	Aceptable	1.0		3

ANALISIS DE RIESGOS

Proceso identificado	Amenaza	Fuente	Vulnerabilidad	Impacto	Probabilidad	Valor Riesgo	Criticidad	Promedio	Prioridad	Nivel PROB
Servicios de plataforma	Uso incorrecto	Personas desinformadas	Deficiente entrenamiento y capacitación	5	100%	5	Critico	5.0	Muy Alta	15
Servicios de plataforma	Pérdida de capacidad	Planeación de recursos	Falta de documentacion de procesos	5	40%	2	Tolerable	5.0		6
Servicios de plataforma	Desactualización	personas	Falta de seguimiento a los procesos	5	100%	5	Critico	5.0		15

ANALISIS DE RIESGOS

Proceso identificado	Amenaza	Fuente	Vulnerabilidad	Impacto	Probabilidad	Valor Riesgo	Criticidad	Promedio	Prioridad	Nivel PROB
Desarrollo de Aplicaciones	Piratería	Personas maliciosas	Falta de documentacion y controles de acceso a los sistemas de informacion	2	40%	0.8	Aceptable	1.6	Media	2
Desarrollo de Aplicaciones	Uso incorrecto	Personas desinformadas	Deficiente entrenamiento y capacitación	2	80%	1.6	Tolerable	1.6		4
Desarrollo de Aplicaciones	incumplimiento	aplicaciones	falta de analisis de riesgos de seguridad	2	50%	1	Aceptable	1.6		2.5

ANALISIS DE RIESGOS

Proceso identificado	Amenaza	Fuente	Vulnerabilidad	Impacto	Probabilidad	Valor Riesgo	Criticidad	Promedio	Prioridad	Nivel PROB
Plan de continuidad del negocio	Interrupción del negocio	instalaciones electricas, instalaciones, clima	Falta de estrategias de recuperacion	3	80%	2.4	Tolerable	2.5	Media	8
Plan de continuidad del negocio	Pérdida de capacidad	Mantenimiento	Falta de dimencionamiento de recuperacion	5	10%	0.5	Aceptable	2.5		1.5
Plan de continuidad del negocio	Afectaciones legales	personas, contratistas, proveedores	falta de definicion de tiempos admisibles de interrupcion en los contratos	5	50%	2.5	Tolerable	2.5		7.5

ANALISIS DE RIESGOS

Proceso identificado	Amenaza	Fuente	Vulnerabilidad	Impacto	Probabilidad	Valor Riesgo	Criticidad	Promedio	Prioridad	Nivel PROB
Criptografía	Robo de información	Personas maliciosas	falta de controles documentados	5	80%	4	No tolerable	5	Muy Alta	12
Criptografía	Copia no autorizada	Personas	falta de controles documentados	5	60%	3	No tolerable	5		9
Criptografía	Consulta no autorizada	Personas	Deficiente entrenamiento y capacitación	5	60%	3	No tolerable	5		9
Criptografía	Uso incorrecto	Personas	Deficiente entrenamiento y capacitación	5	100%	5	Critico	5		15

Prioridad	Riesgo	Min	Max
Baja	Aceptable	0.1	1.3
medio	Tolerable	1.4	3
Alta	No tolerable	3.1	4
Muy alta	Critico	4.1	5

Nivel	Rangos	TABLA IMPACTO EN IFORMACIÓN (disponibilidad, confiabilidad, integridad)
1	Insignificante	La información no esta disponible por menos de 3 horas.
2	Menor	La información no esta disponible 3 y 8 horas
3	Medio	La información no esta disponible 8 y 14 horas
4	Mayor	La información no esta disponible 15y 24 horas
5	Superior	La información no esta disponible 24 en adelante

Figura 4. Mapa De riesgos

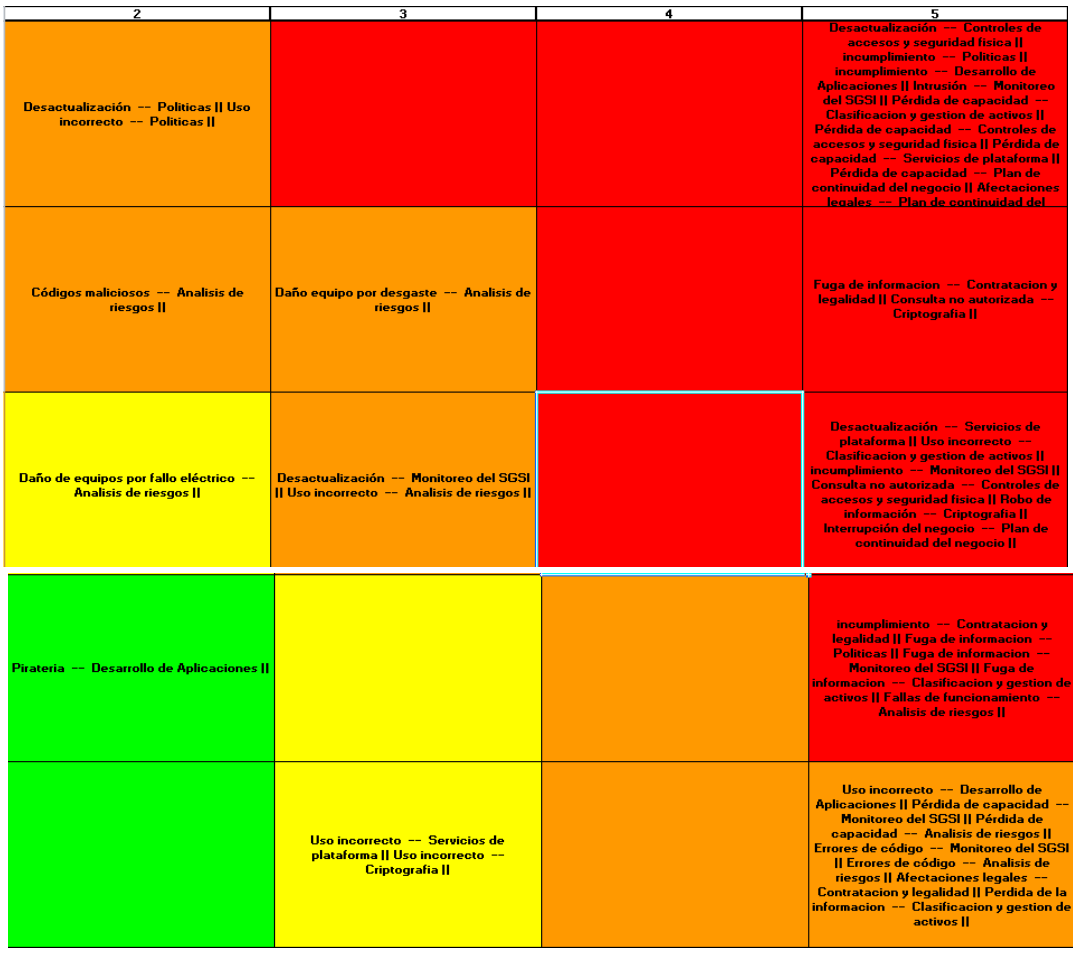


Figura 5. Distribución Porcentual

DISTRIBUCIÒN PORCENTUAL

ZONA	%	Total riesgos
Bajo	**2.43902439**	**1**
Medio	**7.31707317**	**3**
Medio-Alto	**31.7073171**	**13**
Altos	**58.5365854**	**24**

4.3.Definición de proyectos

Los proyectos resultantes obtenidos y la criticidad de los mismos fueron:

Tabla 3. Proyectos y Criticidad.

Proyecto	Criticidad
Proyecto Políticas	Critico
Proyecto Monitoreo del SGSI	Media
Proyecto contratación y legalidad	Alta
Proyecto clasificación y gestión de activos	Muy Alta
Proyecto controles de accesos y seguridad física	Baja
Proyecto servicios de plataforma	Alta
Proyecto desarrollo de Software	Baja
Proyecto plan de continuidad del negocio	Media
Proyecto análisis de riesgos	Media

Figura 6: Red Enka

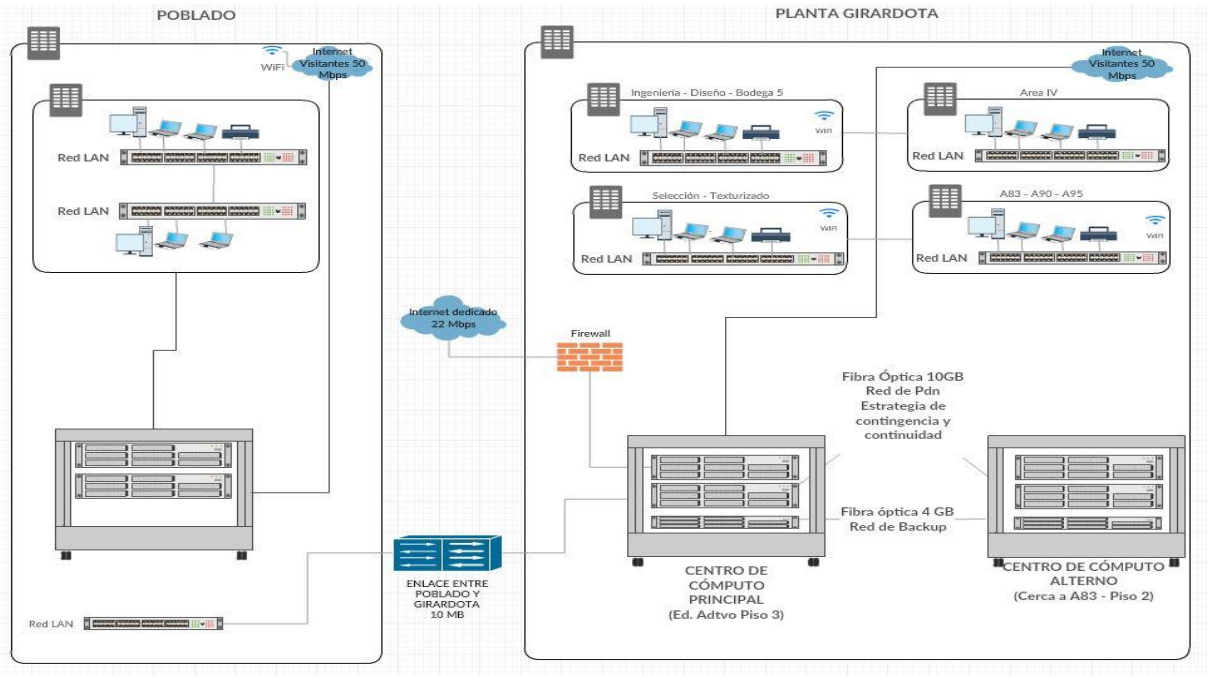


Figura 7: control licenciamiento

OFFICE	97 Pro	2000 Std	2000 Pro	Xp pro	2003 Std	2003 Pro	2007 Small Busines	2007 Std	2007 Pro Spa	2007 Pro	2010 Std	2010 Pro	2013 Std	2013 Pro	2016 Std	2016 Pro	365 Pro Plus	O365 BE	O365 BP	O365 E3
Licencias compradas o libres	0	40	99	4	21	77	3	28	1	4	90	12	16	2	19	1	1	2	31	2
Licencias asignadas	0	8	11	0	25	63	0	30	1	6	107	11	5	2	11	0	0	2	21	2
Diferencia	0	32	88	4	-4	14	3	-2	0	-2	-17	1	11	0	8	1	1	0	10	0
Comentarios																				

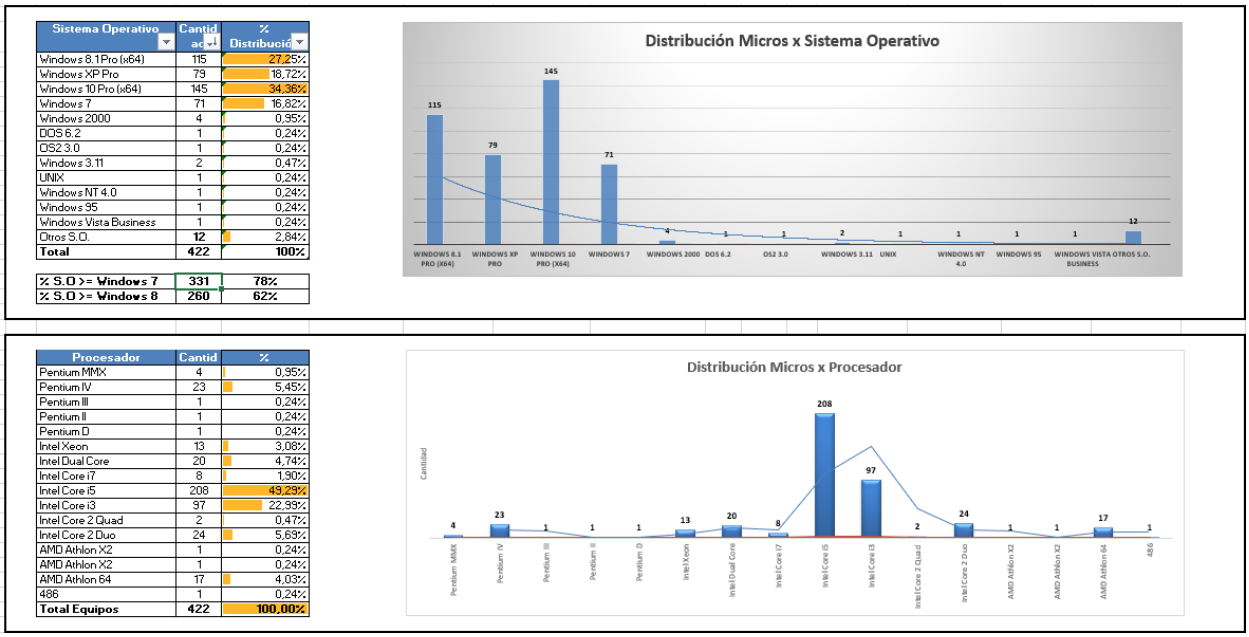
Se cruzan
Se cruzan
Se cruzan

EXCHANGE	2007 Std Svr	2010 Std Svr	Online Plan1	5.5 CAL	2000 CAL	2003 Std CAL	2007 Std CAL x Usr	2007 Std CAL x Dev	2010 Std CAL x Usr	2010 Std CAL x Dvc	2013 Std CAL x Usr	2013 Std CAL x Dev
Licencias compradas o libres	1	1	45	27	334	350	0	100	60	0	50	50
Licencias asignadas	1	1	25	0	0	0	0	139	41	57	0	0
Diferencia	0	0	20	27	334	350	0	-39	19	-57	50	50
Comentarios												

	Visual Studio								Project					Visio			Power BI Pro	Lync Online
VISUAL STUDIO - PROJECT - VISIO	2016 Pro	2015 Pro	2013 Pro	2012 Pro	2010 Pro	2008 Pro	2005 Pro	2003 Pro	2016 Std	2003 Svr	2003 Pro	2003 CAL Svr	2000	2003 Std Svr	2003 Pro	2000 Pro		2013
Licencias compradas o libres	3	4	4	2	5	4	12	6	1	1	6	10	1	5	5	3	4	4
Licencias asignadas	0	7	8	0	1	4	2	0	1	0	6	0	0	0	2	0	4	3
Diferencia	3	-3	-4	2	4	0	10	6	0	1	0	10	1	5	3	3		1
	Comentarios: Faltan 4 licencias								Comentarios					Comentarios				

OTROS	ISA		Office Communicator		Word			Excel					Access						Outlook	
	2006 Svr Std	2004 Std Svr fProc	2007	2007 Std	2000	2003	2007	5	2000	2002	2003	2007	2	97	2000	2002	2003	2007	2010	2000	2003
Licencias compradas o libres	1	1	1	4	7	35	0	0	91	5	0	0	0	20	22	5	0	0	0	0	0
Licencias asignadas	0	0	0	0	2	3	0	1	14	0	2	0	1	0	4	0	8	3	1	4	6
Diferencia	1	1	1	4	5	32	0	-1	77	5	-2	0	-1	20	18	5	-8	-3	-1	-4	-6

Figura 8: controles activos (Hardware)

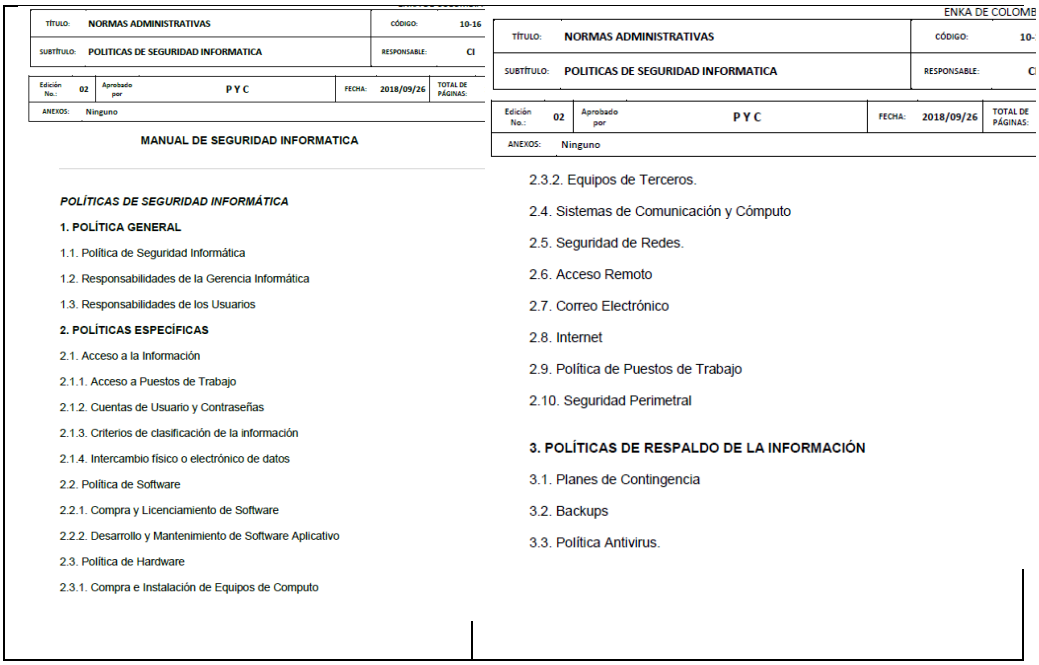


Sistema Operativo	Cantidad	% Distribución
Windows 8.1 Pro (x64)	115	27,25%
Windows XP Pro	79	18,72%
Windows 10 Pro (x64)	145	34,36%
Windows 7	71	16,82%
Windows 2000	4	0,95%
DOS 6.2	1	0,24%
OS2 3.0	1	0,24%
Windows 3.11	2	0,47%
UNIX	1	0,24%
Windows NT 4.0	1	0,24%
Windows 95	1	0,24%
Windows Vista Business	1	0,24%
Otros S.O.	12	2,84%
Total	**422**	**100%**

% S.O >= Windows 7	**331**	**78%**
% S.O >= Windows 8	**260**	**62%**

Procesador	Cantidad	%
Pentium MMX	4	0,95%
Pentium IV	23	5,45%
Pentium III	1	0,24%
Pentium II	1	0,24%
Pentium D	1	0,24%
Intel Xeon	13	3,08%
Intel Dual Core	20	4,74%
Intel Core i7	8	1,90%
Intel Core i5	208	49,29%
Intel Core i3	97	22,99%
Intel Core 2 Quad	2	0,47%
Intel Core 2 Duo	24	5,69%
AMD Athlon X2	1	0,24%
AMD Athlon X2	1	0,24%
AMD Athlon 64	17	4,03%
486	1	0,24%
Total Equipos	**422**	**100,00%**

Figura 9: Manual de seguridad informática



TÍTULO:	NORMAS ADMINISTRATIVAS		CÓDIGO:	10-16
SUBTÍTULO:	POLITICAS DE SEGURIDAD INFORMATICA		RESPONSABLE:	CI
Edición No.:	02	Aprobado por: P Y C	FECHA:	2018/09/26
TOTAL DE PÁGINAS:				
ANEXOS:	Ninguno			

MANUAL DE SEGURIDAD INFORMATICA

POLÍTICAS DE SEGURIDAD INFORMÁTICA

1. POLÍTICA GENERAL

1.1. Política de Seguridad Informática

1.2. Responsabilidades de la Gerencia Informática

1.3. Responsabilidades de los Usuarios

2. POLÍTICAS ESPECÍFICAS

2.1. Acceso a la Información

2.1.1. Acceso a Puestos de Trabajo

2.1.2. Cuentas de Usuario y Contraseñas

2.1.3. Criterios de clasificación de la información

2.1.4. Intercambio físico o electrónico de datos

2.2. Política de Software

2.2.1. Compra y Licenciamiento de Software

2.2.2. Desarrollo y Mantenimiento de Software Aplicativo

2.3. Política de Hardware

2.3.1. Compra e Instalación de Equipos de Computo

ENKA DE COLOMB
TÍTULO: NORMAS ADMINISTRATIVAS CÓDIGO: 10-
SUBTÍTULO: POLITICAS DE SEGURIDAD INFORMATICA RESPONSABLE: C
Edición No.: 02 Aprobado por: P Y C FECHA: 2018/09/26 TOTAL DE PÁGINAS:
ANEXOS: Ninguno

2.3.2. Equipos de Terceros.

2.4. Sistemas de Comunicación y Cómputo

2.5. Seguridad de Redes.

2.6. Acceso Remoto

2.7. Correo Electrónico

2.8. Internet

2.9. Política de Puestos de Trabajo

2.10. Seguridad Perimetral

3. POLÍTICAS DE RESPALDO DE LA INFORMACIÓN

3.1. Planes de Contingencia

3.2. Backups

3.3. Política Antivirus.

Figura 10: Plan de contingencia

ENKA DE COLOMBIA S.A.

TITULO:	INFORMÁTICA	CODIGO:	PW-15-011
SUBTITULO:	PLAN DE CONTINGENCIA Y CONTINUIDAD DE LA INFRAESTRUCTURA INFORMATICA	RESPONSABLE:	CI

Edición No.:	03	Aprobado por	CI	FECHA:	2019/02/26	TOTAL DE PAGINAS:	9
ANEXOS:	10 anexos						

TABLA DE CONTENIDO

Figura 11 Política de contraseñas

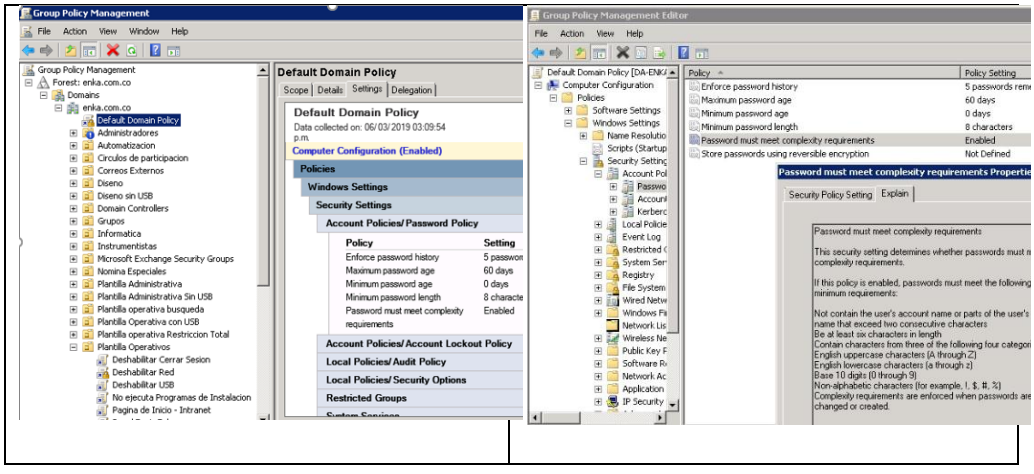
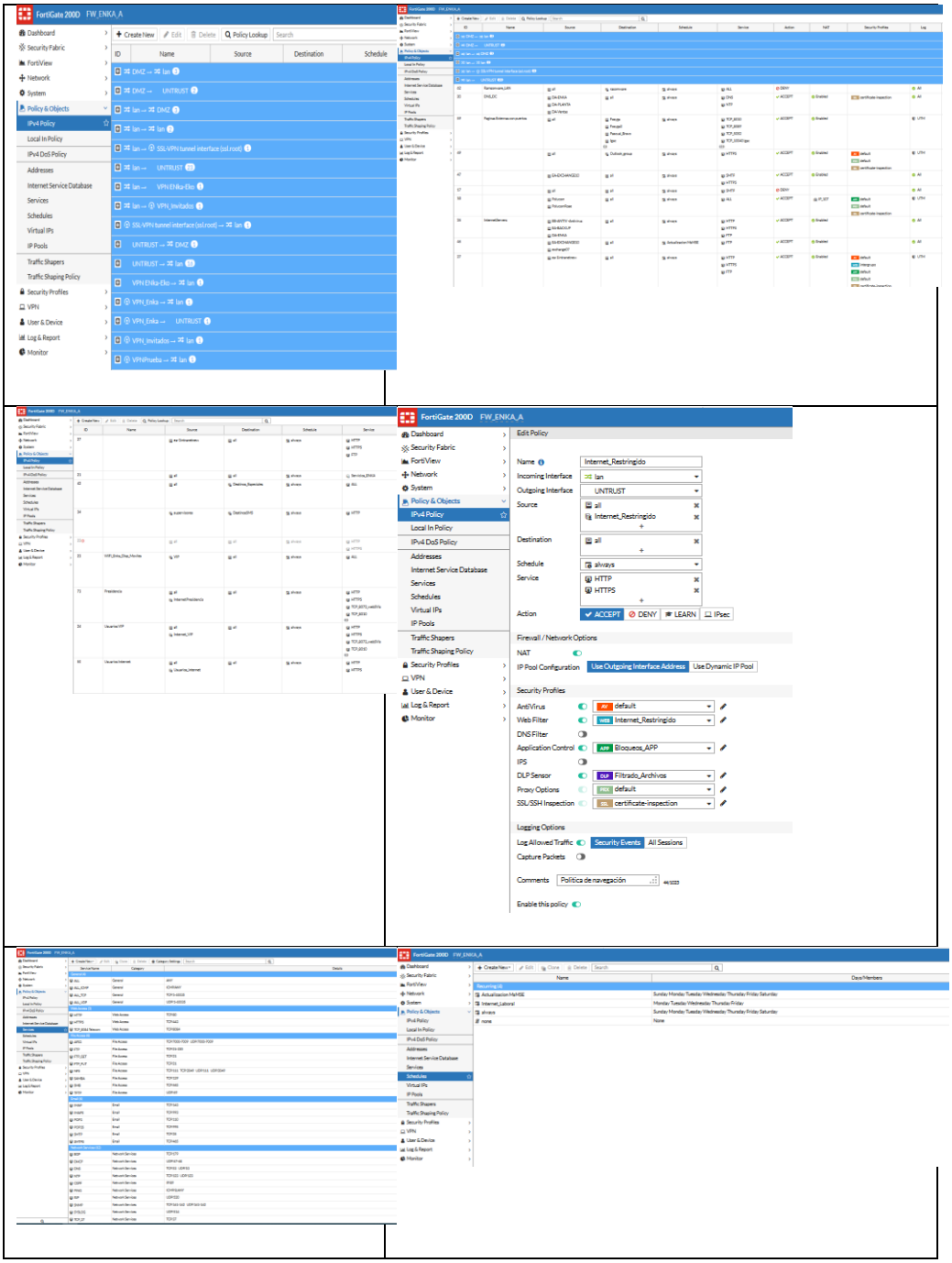
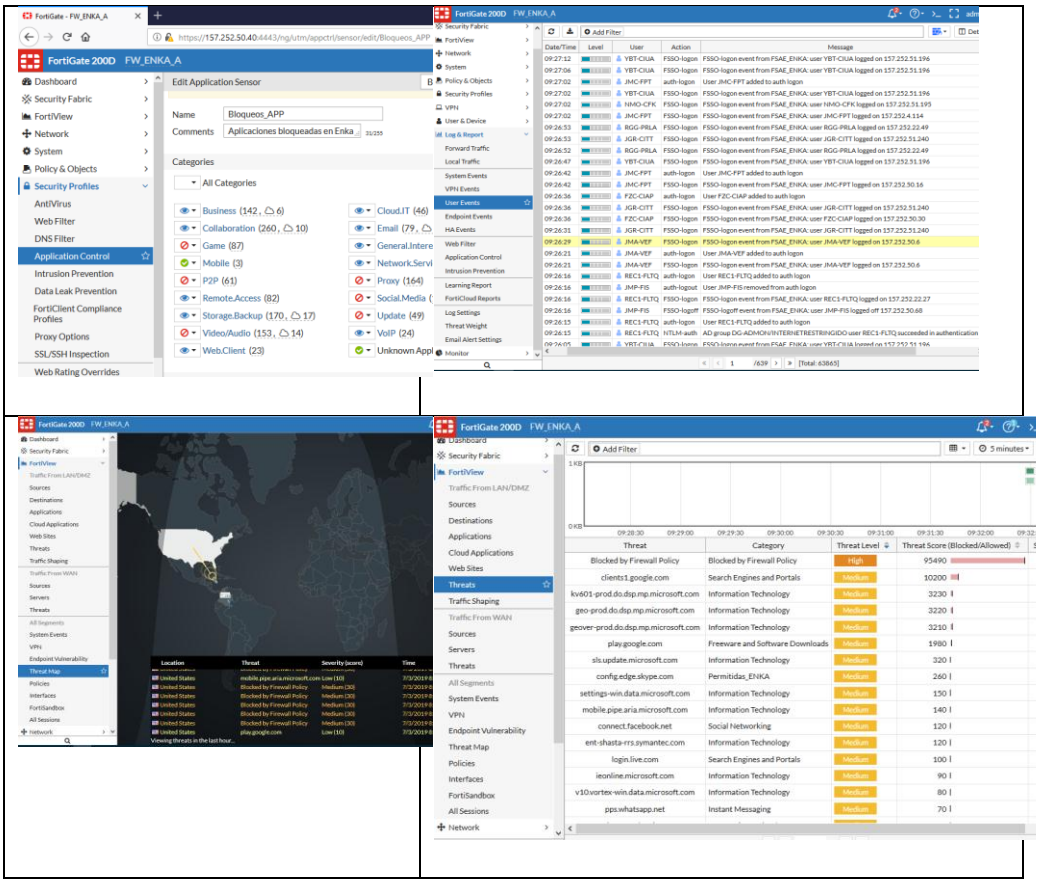


Figura 12: Políticas y objetos del Firewall




FortiGate 200D FW_ENKA_A
Edit Application Sensor
Name Bloqueos_APP
Comments Aplicaciones bloqueadas en Enka
Categories
All Categories
Business (142 , 6)
Collaboration (260 , 10)
Game (87)
Mobile (3)
P2P (61)
Remote.Access (82)
Storage.Backup (170 , 17)
Video/Audio (153 , 14)
Web.Client (23)
Cloud.IT (46)
Email (79 ,
General.Intere
Network.Servi
Proxy (164)
Social.Media
Update (49)
VoIP (24)
Unknown Appl
Security Profiles
AntiVirus
Web Filter
DNS Filter
Application Control
Intrusion Prevention
Data Leak Prevention
FortiClient Compliance Profiles
Proxy Options
SSL/SSH Inspection
Web Rating Overrides
Threat Map
FortiView
Traffic From LAN/DMZ
Traffic From WAN
Sources
Destinations
Applications
Cloud Applications
Web Sites
Threats
Traffic Shaping
Servers
All Segments
System Events
VPN
Endpoint Vulnerability
Policies
Interfaces
FortiSandbox
All Sessions
Network
Add Filter
5 minutes
Threat
Category
Threat Level
Threat Score (Blocked/Allowed)
Blocked by Firewall Policy
Search Engines and Portals
Information Technology
Freeware and Software Downloads
Social Networking
Instant Messaging
Permitidas_ENKA

5. Recomendaciones

- Enka de Colombia cuenta con un sistema de Gestión de seguridad acorde las necesidades del entorno.
- Se puede observar una adecuada gestión de los procesos y la documentación permitiendo mantener vigente y actualizados los sistemas de seguridad y el personal
- No se evidencia brechas de seguridad significativas que puedan exponer la información y la seguridad en informática.
- Contar con un analista de seguridad dedicado exclusivamente a las funciones de seguridad y Hacking.
- Contratar personal calificado para la planeación, ejecución y control de los proyectos sugeridos en la tabla 3.

6. Conclusiones

- Ampliar el sistema de seguridad perimetral que permita mantener un control sobre las aplicaciones web que se exponen en Internet.
- Continuar desarrollando la aplicación ajustada a las necesidades de la compañía que permita mantener un monitoreo y controle del estado del backup de los usuarios y servidores.
- Adquirir una plataforma de monitoreo en tiempo real de los componentes de la infraestructura y la red.

7. Referencias bibliográficas

Agudelo, D. F. (2014). *El Riesgo y la falta de políticas de seguridad informática una amenaza para las empresas certificadas BASC.* . Universidad Militar Nueva Granada .

Dayal E. (2014). *Plantilla Project charter –templater.docs-Eric-dayal-. Recuperado de:* http://www.hitdocs.com/project-charter-template-docx

ISO/IEC, 2. (2013). *Information Technology – Security Techniques – Information Security* (segunda ed.). Switzerland.

ISO/IEC, 2. (2013). *Information Technology – Security Techniques –Code of practice for* (Segunda ed.).