DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICABLES PARA LA EMPRESA GRUPO EMPRESARIAL ARDILA & ASOCIADOS ALINEADAS A LA NORMA ISO27001:2013

EDWIN JAVIER VARÓN PERALTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ, COLOMBIA

2015

DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICABLES PARA LA EMPRESA GRUPO EMPRESARIAL ARDILA & ASOCIADOS ALINEADAS A LA NORMA ISO27001:2013

EDWIN JAVIER VARÓN PERALTA

TESIS DE GRADO PARA OPTAR POR EL TÍTULO:

ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTOR DE PROYECTO:

ING. ERIKA LILIANA VILLAMIZAR TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ, COLOMBIA

2015

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá, 7 de Noviembre de 2015

DEDICATORIA.

Este trabajo se los dedico a mis padres ya que gracias a ellos, a su dedicación, su tenacidad y entusiasmo han hecho posible este título.

AGRADECIMIENTOS.

Agradezco a todas las personas que a lo largo del posgrado han hecho parte de este proceso de aprendizaje personal y profesionalmente, que con sus aportes han ayudado de diversas maneras al proceso que con este trabajo no termina si no que hasta ahora empieza.

También mis más sinceros afectos y gratitud a la universidad nacional y abierta y a distancia (UNAD), que ha hecho realidad lo que para mí antes eran sueños.

1. CONTENIDO.

2. ÍNDICE DE TABLAS.

3. ÍNDICE DE FIGURAS.

4. LISTA DE ANEXOS.

5. GLOSARIO.

Acciones legales: La acción jurisdiccional es el derecho de acceso a los juzgados y tribunales solicitando que ejerzan la potestad de juzgar y hacer ejecutar lo juzgado.

Activo de información: Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información

Tipos de Acceso: Se definen valores de privilegios, de esta forma hay usuarios que pueden administrar las contraseñas del sistema. Otros usuarios pueden administrar la aplicación de respaldo. Cada uno de estos privilegios puede ser asignado a ciertos usuarios

Criptografía: técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados

Sistemas: Un sistema es un objeto complejo cuyos componentes se relacionan con al menos algún otro componente; puede ser material o conceptual.

Aplicaciones: Es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos.

Sistemas: Un sistema es un objeto complejo cuyos componentes se relacionan con al menos algún otro componente; puede ser material o conceptual.

Procedimientos Operativos: son documentos que recogen la interrelación en el tiempo que existen entre diferentes departamentos, normalizando los procedimientos de actuación y evitando las indefiniciones e improvisaciones que pueden producir problemas o deficiencias en la realización del trabajo.

Código malicioso: se trata de un tipo de amenaza que no siempre puede bloquearse con un software antivirus por sí solo.

Copia de seguridad: es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

La transferencia de archivos: Es decir, es una convención o una norma que controla o permite la transferencia de archivos entre dos o más computadoras o usuarios

Auditoria: Es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, que puede ser una persona, organización, sistema, proceso, proyecto o producto

Licencia de software: es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario (usuario consumidor /usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

6. INTRODUCCIÓN.

En el mundo de hoy la seguridad informática ha adquirido mucha importancia, donde el concepto de que la información es el activo más valioso de cualquier empresa o persona, las soluciones de seguridad informática son frecuentemente implementadas en ambientes empresariales para minimizar problemas de seguridad y evitar pérdidas no deseadas de la información. Por tal razón, dentro de la empresa Grupo Empresarial Ardila y Asociados empresa del sector privado se requiere la implementación de soluciones que mitiguen los inconvenientes de seguridad que puedan garantizar la Disponibilidad, Integridad y la confiabilidad en la información.

Con el desarrollo del presente proyecto se diseñaran las políticas de seguridad de la empresa Grupo Empresarial Ardila y Asociados, el proyecto no solo se limitara a las políticas también vamos a crear una conciencia a los empleados del grupo empresarial sobre seguridad informática y a la gerencia se le darán herramientas de seguridad y manejo de información; creando políticas de manejo y almacenamiento de la información.

Para la realización de este proyecto se utilizará la norma ISO 27001 versión 2013 donde se proporcionan los lineamientos para la gestión de la seguridad en la información en cualquier empresa.

7. PLANTEAMIENTO DEL PROBLEMA.

GRUPO EMPRESARIAL ARDILA & ASOCIADOS es una empresa del área de la ingeniería Civil específicamente en la construcción, en la actualidad se encuentra en crecimiento haciéndose más competitiva dentro de su ramo, esto hace que se adopten nuevas estrategias con el fin de garantizar el éxito.

La empresa está adoptando herramientas de optimización de procesos y de seguridad informática enfocados al cumplimiento de la Visión, Misión, Valores etc., que permitan resguardar la información de la empresa y crear buenas prácticas de seguridad informática.

El problema radica en las malas prácticas del uso del almacenamiento de información, no existe seguridad en el almacenamiento, no se realizan backup, no existen control de acceso para controlar la reproducción de la información.

Otro problema radica en el hecho que la empresa tiene proyectos en distintas partes del país por periodos cortos (de 3 a 6 meses), los ingenieros residentes de los proyectos, como también técnicos y auxiliares de obra maneja la información en sus portátiles y medios extraíbles con el riesgo que se pierda la información que se encuentra en estos medios, también se corre el riesgo de no actualizar la información que se encuentra en los servidores de la empresa.

8. FORMULACIÓN DEL PROBLEMA.

¿Cómo mejorar en la empresa Grupo Empresarial Ardilla & Asociados la seguridad de la información?

9. JUSTIFICACIÓN.

El presente proyecto tiene como finalidad diseñar las políticas de seguridad de la empresa Grupo Empresarial Ardila & Asociados, crearles a sus empleados una conciencia en seguridad de la información y a la gerencia darle unas herramientas de control para el manejo de información; creando políticas de manejo, almacenamiento, creación y eliminación de información creando un entorno seguro mediante el manejo de la las políticas que se van a diseñar.

Es importante la realización de este proyecto debido a que el nivel de riesgo en el que se encuentra la empresa Grupo Empresarial Ardila & Asociados es muy alto debido a que no tienen ninguna política de seguridad informática y esto constituye un alto riesgo de perder sus activos de información, siendo potencialmente víctimas de extorciones proporcionadas por la información de la misma empresa, también pudiendo ser víctimas de robo de información de procesos y clientes que se puedan vender a empresas que sean competencia de la empresa Grupo Empresarial Ardila & Asociados; al crear las políticas de empresa Grupo Empresarial Ardila & Asociados se obtiene el beneficio de crear ambientes informáticos más seguros minimizando el riesgo de pérdida de información dando a la gerencia y a los clientes tanto internos como externos confiabilidad en el manejo de los activos de la información.

Este proyecto se va a orientar solo en la ciudad de Bogotá, debido a que en esta ciudad reposan los archivos de información a objeto de la empresa Grupo Empresarial Ardila & Asociados.

Finalmente el proyecto pretende buscar soluciones a un bajo costo para le empresa con recursos innovadores y enfocándonos en la conciencia del talento humano.

10. OBJETIVOS.

10.1 OBJETIVO GENERAL.

Diseñar las políticas de seguridad de la información aplicables a la entidad Grupo Empresarial Ardila y Asociados. Norma técnica colombiana norma ISO 27001:2013.

10.2 OBJETIVOS ESPECÍFICO.

- Realizar un análisis de la situación actual de seguridad de la información en la empresa Grupo Empresarial Ardila y Asociados.

- Identificar los activos de información críticos de la empresa Grupo empresarial Ardila y asociados.

- Realizar un análisis de riesgos de los activos de información de la empresa Grupo Empresarial Ardila y Asociados.

- Proponer las medidas de seguridad del control de acceso aplicables a la empresa Grupo Empresarial Ardila & Asociados buscando tener un control de la misma.

11. TITULO DEL PROYECTO.

Diseño de las políticas de seguridad de la información aplicables para la empresa grupo empresarial Ardila & asociados alineadas a la norma ISO 27001:2013.

12. LÍNEA DE INVESTIGACIÓN.

El presente anteproyecto se inscribe dentro del área de la ingeniería electrónica, telecomunicaciones y redes, en la línea 1: Infraestructura tecnológica y seguridad en redes. También se aborda el área de Ingeniería Industrial con la Línea 1: Modelos de gestión organizacional.

13. TEMA OBJETO DE ESTUDIO.

La presente propuesta se enmarca dentro del tema de seguridad de la información.

14 MARCO REFERENCIAL.

14.1 MARCO TEÓRICO.

El cumulo de información que se maneja al interior de las organizaciones por la implementación de diversas herramientas que se ejecutan de manera continua en sus sistemas de información, bases de datos, aplicativos corporativos y a través de la web, sin dejar de lado los medios físicos donde se almacena la información pertinente a la empresa; toda esta información es el insumo propio de las empresas para el cumplimento de sus objetivos y metas además de las que se han trazado y están las que están incluidos en su misión y su visión como organización[1].

La información tiene además la función de hacer mover de manera operacional la empresa, ya que a través de la información que se maneja a diario, mantiene funcionando la organización además permite cierto nivel de progreso gracias a la implantación de mejoras que se pueden lograr con un constante monitoreo en la documentación, así como en la sistematización de todos y cada uno de los procesos operativos y funcionales, teniendo como eje principal la seguridad de la información.

14.1.1 Seguridad de la información.

En este contexto dado la seguridad de la información se puede definir como un estado de no vulnerabilidad de la información, es decir mantenerla fuera de todo riesgo, daño o peligro.

Las vulnerabilidades es todas aquellas amenazas que tiene el entorno al manipular las información y puedan alterar la información.

Garantizar un nivel de protección total es imposible[2], debido a que esta información es manipulada por Humanos y siempre existe el factor humano de

[1] ISO 14001. Aplicación de un plan de manejo ambiental en cualquier organización del sector público o privado. Términos de uso información
Organización Internacional para Normalización (International Organización for Standardization - ISO)

[2] ISO 2700. Sistema de gestión de seguridad de la información. Términos de uso información iso27000.es ©, 2012

error que nos deja la ventana libre para cualquier vulnerabilidad; “Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene[3]”.

Lo importante es enfatizar que el la empresa que adopte en su misión, visión y objetivos la seguridad informática va a garantizar minimizar daños a la información va a garantizar la continuidad del negocio y va a dar credibilidad a sus clientes de una información veraz y oportuna.

La seguridad de la información es importante en negocios tanto del sector público como del privado para proteger las infraestructuras críticas. En ambos sectores, la seguridad de información permitirá, lograr el gobierno electrónico o el comercio electrónico, evitando y reduciendo los riesgos relevantes. La interconexión de las redes públicas y privadas y el compartir los recursos de información aumentan la dificultad de lograr el control de los accesos.[4]

14.1.2 Amenazas de la información.

• Externas: Intrusión a las redes de la organización o instalaciones físicas, por ejemplo: spam, hackers, suplantación de identidad, fraude, espionaje, sabotaje, robo de información, entre otras.[5]

• Internas: Generadas al interior de la organización, principalmente por el conocimiento de los colaboradores. Ejemplo: Alteración de la información, divulgación de la información, fraudes, robo, sabotaje, uso no autorizados de sistemas informáticos, uso de imagen corporativa sin autorización, etc. [6]

---

[3] RUIZ L. Hernando. RESOLUCIÓN 160-005326 Política de Seguridad de la información Superintendencia de Sociedades. 2008.
[4] ISO/IEC 27002:2013. . Sistema de gestión de seguridad de la información. Términos de uso información
iso27000.es ©, 2013
[5] COLOMBIA. ICONTEC. Compendio: Sistema de gestión de la seguridad de la información (SGSI) Norma Técnica Colombiana, 2009.
[6] COLOMBIA. ICONTEC. Compendio: Sistema de gestión de la seguridad de la información (SGSI) Norma Técnica Colombiana, 2009.

• Naturales: son generadas por desastres naturales, como inundaciones, huracanes, terremotos, incendios, etc.[7]

14.1.3 Análisis de Riesgos Informáticos.

Un riesgo informático es el hecho no deseado que suceda con nuestra información, por eso debemos tener claro los riesgos que poseen nuestra información para con eta información saber si se pueden minimizar, eliminar o controlar, para llegar a determinar los riesgos se debe hacer la tarea de determinar, analizar, evaluar y clasificar los activos de información más importantes según la criticidad de los mismos proceso que se llama metodología de análisis de riesgos la cual explicaremos a continuación.

14.1.4 Metodología de Análisis de Riesgos.

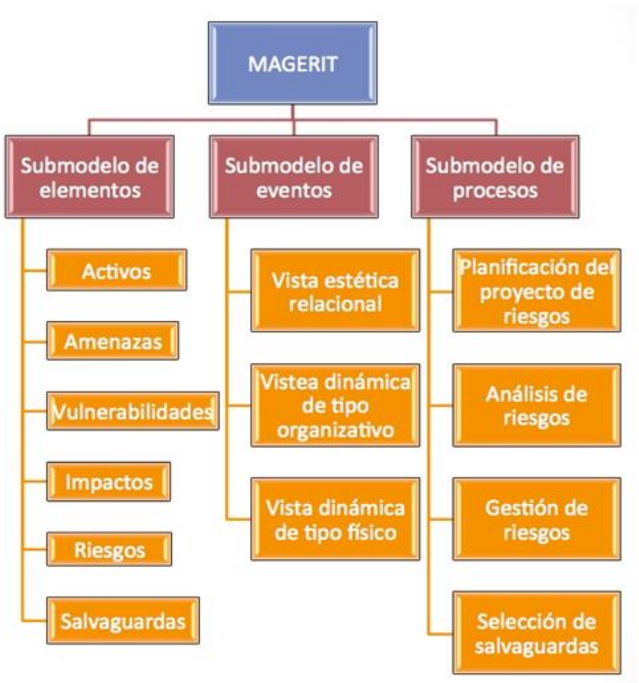
Son metodologías o técnicas ya planteadas que se utilizan para determinar los posibles riesgos de un activo de información y qué medidas se pueden adoptar para que el daño sea el mínimo en este activo.

La metodología que el proyecto adopta es MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información): El esquema completo de Etapas, Actividades y Tareas del Sub-modelo de Procesos de MAGERIT[8] el cual puede aplicarse o no en su totalidad, dependiendo de la complejidad misma del proyecto es el siguiente:

[7] COLOMBIA. ICONTEC. Compendio: Sistema de gestión de la seguridad de la información (SGSI) Norma Técnica Colombiana, 2009.

[8] BOLAÑOS, María C y ROCHA G. Mónica. 25 de marzo de 2014. Auditoria de SI. Magerit V3(Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).[en línea]: http://asijav.weebly.com/auditoria-de-sistemas-de-informacioacuten/magerit-v3-metodologa-deanlisis-
y-gestión-de-riesgos-de-los-sistemas-de-información.

Figura 1 Esquema MAGERIT.



Fuente: Auditoria del SI Magerit.

14.1.5 Serie ISO 27000.

Para poder llevar a cabo el resguardo de la información vamos a utilizar las normas ISO 2700 donde se proporcionan los lineamientos para la gestión de la seguridad en la información en cualquier empresa; para efectos de este trabajo nos enfocaremos en 3 de estas normas que mencionamos a continuación.

- ISO 27001: Publicada el 15 de Octubre de 2005. En esta norma encontraremos los requisitos del sistema de gestión de seguridad de la información y es a la cual se certifican por auditores externos los SGSI de las organizaciones. [9]

[9] ISO/IEC 27001:2013. . Sistema de gestión de seguridad de la información. Términos de uso información
iso27001.es ©, 2013

- ISO 27002: Desde el 1 de Julio de 2007, En esta norma encontraremos una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. [10]

- ISO 27005: Publicada el 4 de Junio de 2008. En esta norma encontraremos las directrices para la gestión del riesgo en la seguridad de la información. [11]

[10] ISO/IEC 27002:2013. . Sistema de gestión de seguridad de la información. Términos de uso información
iso27002.es ©, 2013
[11] ISO/IEC 27005:2013. . Sistema de gestión de seguridad de la información. Términos de uso información
iso27005.es ©, 2013

14.2 MARCO CONCEPTUAL.

Como se ha mencionado anteriormente el activo más importante que tiene una organización es la información y por consiguiente se deben tener lineamientos claros para tener seguridad en estos activos, lineamientos claros en la manipulación, almacenamiento y eliminación de los mismos.

También se debe tener en cuenta que con el avance de la tecnología existe diversidad de dispositivos de electrónicos que nos permiten la manipulación y almacenamiento de los activos de información, y que por lo tanto también es más fácil un eventual ataque.

Para la empresa grupo empresarial Ardila y asociados la gestión de la seguridad debe ser planteada tanto en la parte lógica como física planeando políticas de seguridad informática, planes de contingencia y aplicación de normas internas que nos permitan la protección d los activos de información.

14.2.1 Características de un Sistema Seguro:

- **Confidencialidad:** Los activos de información serán accesibles a los usuarios que tengan autorización.

- **Integridad:** Los activos de información sólo pueden ser creados y modificados por los usuarios autorizados.

- **Disponibilidad:** Los usuarios deben tener disponibles los activos de información cuando ellos lo requieran. No tiene sentido tener los activos de información resguardados si los usuarios que la requieran no pueden tener acceso a ella en el momento que ellos la necesiten.

- **Control de acceso a los recursos:** Tener el control de quienes acceden a los activos de información, para saber quién modifica, consulta o elimina un activo.

- **Auditoría:** Inspección o verificación para poder determinar qué es lo que está ocurriendo con los activos de información, qué es lo que hace cada uno de los usuarios, los tiempos y fechas de dichas acciones.

- **Metodología de auditoría**: Da los lineamientos claros de las actividades que se deben efectuar a realizar el proceso de revisión preliminar, revisión de controles, diagnósticos y comparación de estados actuales en los activos de información, dando como resultado informes que presentan los resultados de la aplicación metodológica.

- **Magerit:** Es una metodología que es una guía de referencia para realizar procesos de análisis de riesgos al igual que provee lineamientos para la gestión de riesgos en sistemas informáticos y todos los aspectos que giran alrededor de ellos en las organizaciones para lograr muchas de las metas planteadas al interior de las mismas y buscando cumplir las políticas de buen gobierno[12]. El proyecto que se va a realizar se basa en la metodología Magerit para efectuar el proceso de análisis de riesgos y asa identificar los activos de información, las amenazas de los activos, para poder determinar los riesgos, impactos potenciales y planes de mitigación de dichos riesgos

- **SGSI[13]:** Un Sistema de gestión de la seguridad de la información, es un sistema el cual se encarga de proporcionar cantidad de mecanismos y herramientas basados en la norma ISO 27001 y tiene como fin conocer al interior de la entidad los riegos a los que puede estar expuesta la información, define estrategias para gestionar los riesgos y debe ser un marco de referencia para la entidad la cual debe garantizar el conocimiento de dichas estrategias por todo el personal, estrategias que debe estar sujetas a revisión y auditorias constante con el fin de planes de mejoras.

[12] DIAN http://www.dian.gov.co/descargas/operador/documentos/2015/Analisis_de_Riesgo_En_5_Pasos.pdf

[13] COLOMBIA. ICONTEC. Compendio: Sistema de gestión de la seguridad de la información (SGSI) Norma Técnica Colombiana, 2009.

14.3 MARCO CONTEXTUAL.

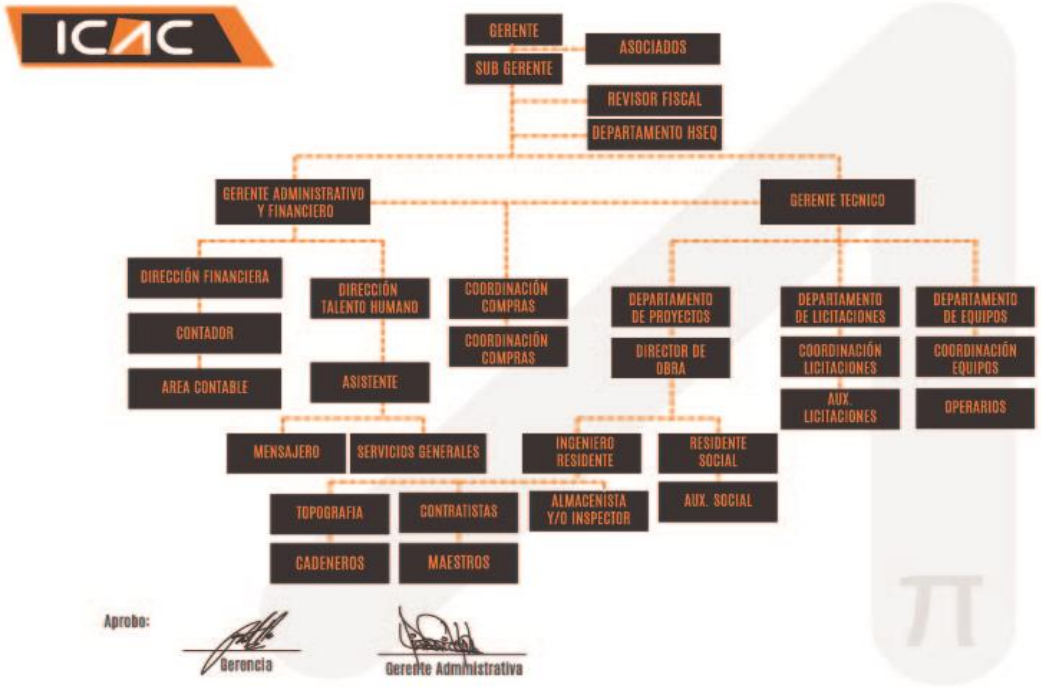
14.3.1 ESTRUCTURA ORGANIZACIONAL.

14.3.1.1 Personal.

La organización está constituida por profesionales de la ingeniería civil con una gran experiencia acumulada a lo largo de múltiples proyectos. Además cuenta con un selecto grupo de profesionales asociados, de todas las ramas de la ingeniería, la arquitectura y la economía, quienes trabajan para proyectos específicos, los cuales tienen a su vez un gran conocimiento en la ejecución, desarrollo y entrega de un amplio número de obras y consultorías, montajes y demás.

14.3.1.2 Organigrama.

Figura 2 Organigrama Grupo empresarial Ardila y asociados.



Fuente: Grupo Empresarial Ardila y Asociados.

14.3.2 UBICACIÓN.

La organización se encuentra ubicada en la carrera 81 C # 24C-11, en la ciudad de Bogotá Colombia sede donde se centraliza la organización de cada uno de los proyectos.

14.3.3 Objeto Social.

La empresa tiene como objeto principal las siguientes actividades:

- La prestación de servicios en todas las ramas de la ingeniería y la arquitectura.
- La construcción de obras y montajes de ingeniería en todas las ramas y fases.
- La ejecución de diseños y proyectos de ingeniería y arquitectura en todas sus fases.
- La elaboración de estudios técnicos y económicos.
- Realizar Consultorías e Interventoría a cualquier tipo de proyectos relacionados con la Ingeniería Civil.

14.3.3.1 Áreas de Actividad.

Las áreas donde la empresa puede prestar sus servicios, incluyen Obras de Saneamiento Básico como son: la Construcción de Acueductos y Alcantarillados, proyectos Viales, Proyectos de vivienda, Consultorías e interventorías y asesoría técnica o de asistencia tecnológica, con actividades tales como:

- Gerencia de Proyectos y/u obras.
- Montajes.
- Diseños.
- Interventorías y/o Inspecciones de Calidad.

- Estudios, Asesorías.
- Construcción.

14.3.3.2 Calidad de los Trabajos.

La organización cumple con los programas de ejecución, las especificaciones técnicas de proyectos, el presupuesto contratado, además asegura y lleva a cabo control de calidad, mediante ensayos de laboratorio, pruebas y demás controles necesarios.

14.3.4 MISIÓN.

Ingenieros Constructores Asociados de Colombia S.A.S y Rogelio Ardila Torres somos una organización con más de 15 años de experiencia en el campo de la ingeniería, especializados en construcción, interventoría, diseño, urbanismo y mantenimiento en el sector civil e hidrocarburos, así como suministro y alquiler de equipo pesado. Asesoramos proyectos con tecnología de punta para generar polos de desarrollo con responsabilidad socio-ambiental, contamos con personal calificado y con experiencia en los diferentes campos de la ingeniería. Versión 5 del 2 de noviembre de 2013.

14.3.5 VISIÓN.

Ingenieros constructores asociados de Colombia S.A.S y Rogelio Ardila Torres en el 2020 ampliaremos la cobertura y nos consolidaremos como empresas líderes en el sector de la ingeniería a nivel nacional, cumpliendo estándares de calidad para asumir proyectos de gran escala. Versión 5 del 2 de noviembre de 2013.

14.3.6 VALORES.

- **HONESTIDAD:** Conjunto de conductas de nuestro personal que generan confiabilidad y compromiso ante la sociedad y nuestra organización.

- **RESPETO:** Compromiso de nuestros colaboradores para la interacción con la sociedad.

- **ETICA:** Columna vertebral de nuestra razón de ser, guiada por nuestros valores.

- **CUMPLIMIENTO:** Compromiso para con nuestros clientes y razón de ser de nuestra actividad diaria.

14.3.7 RESPONSABILIDAD SOCIAL EMPRESARIAL.

Las organizaciones tiene como objeto reconocer e incorporar una relación permanente entre la empresa y grupos de interés, de esta forma armonizar el desarrollo y de ejecución de proyectos, garantizando un dimensión de rentabilidad económica protección de derechos humanos, laborales, bienestar social y la protección ambiental del entorno.

Los instrumentos que abordan el tema de RSE a nivel interno de la gestión empresarial, en las condiciones de trabajo y en las relaciones laborales son los siguientes:

- Políticas de RSE
- Valores y transparencia
- Cumplimiento y compromisos de RSE
- Generación de empleo
- Remuneración y beneficios
- Capacitación y desarrollo profesional
- Prevención de riesgos
- Trato laboral

- Protección del personal
- Medio ambiente y comunidad

14.4 MARCO LEGAL.

- **Ley 603 de 2000 – Derechos de Autor -** La Ley 603 del 2000 obliga a las empresas a presentar un detallado informe de gestión, en donde se resalten el tipo de software que usa la compañía, con el fin de proteger la propiedad intelectual y evitar el incremento de la piratería en nuestro país. (Senado de la República de Colombia, 2000)

- **LEY 1273 DE 2009 -** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Senado de la República de Colombia, 2009)

- **LEY ESTATUTARIA 1581 DE 2012 -** Por medio de esta ley se dictan disposiciones generales para la protección de datos personales. Esta ley protege el actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades.

- **Ley 1341 de 2009 – Ley Tic de Colombia** – Esta ley pretende impulsar el desarrollo y fortalecimiento del sector de las Tecnologías de la Información y las Comunicaciones, promover la investigación e innovación buscando su competitividad y avance tecnológico conforme al entorno nacional e internacional. (Senado de la República de Colombia, 2009)

- **Decreto 2755 de 2003, Artículos 15, 16, 17 y 18:** Reglamenta el artículo 207-2 del Estatuto Tributario y establece **el** procedimiento y los requisitos para obtener el beneficio (Ministerio del Interior y la Justicia de la República de Colombia, 2003)

- **Decreto 1360 de 1989:** Reglamenta la inscripción del software en el Registro Nacional del Derecho de Autor y de acuerdo con lo expresado en el artículo 16 del decreto 2755. (Presidencia de la República de Colombia, 1989)

15. PRESUPUESTO.

Estos serían los costos financieros del proyecto discriminados por cuadros en los gasto que creí pertinentes para la elaboración de eses proyecto.

Tabla 1 Descripción de los Gastos de Personal.

Participante	FORMACIÓN	FUNCIÓN	DEDICACIÓN HORAS	DEDICACIÓN No. MESES	RECURSOS		TOTAL
Nombre		.			FUENTE 1	FUENTE 2	TOTAL
Edwin Javier Varón Peralta	Ingeniero de Sistemas	Desarrollo del proyecto	240	3 meses	No aplica	COP 6.000.000	COP 6.000.000
Comité Seguridad de la Información	1 Abogado 1 Ingenieros de sistemas Gerente Admón. Revisor fiscal Director de Recursos Humanos	Revisión del documento.	8	3 semanas	No genera costos para el proyecto		
TOTAL						COP 6.000.000	

Fuente: El autor

Es importante mencionar que los gastos de personal son nulos esto se debe a que todo el personal a intervenir ya cuenta con una vinculación en la empresa grupo empresarial Ardila y asociados lo que debemos hacer es crear el comité de políticas de seguridad informática pero este personal ya lo cuenta la empresa.

Tabla 2 Descripción de los Gastos Equipos a Utilizar.

EQUIPO	JUSTIFICACIÓN	UNIDAD(ES) A LA CUAL PERTENECE		Horas de asignación al proyecto	Valor Unitario	Valor total
		Fuente 1	Fuente 2			
Computador	Equipo para registrar toda la información		Propiedad del responsable del proyecto	240	No Aplica	No Aplica
Equipos donde se almacena la información	Equipos objeto de estudio	Propiedad de la Entidad		8	COP 10.000.000	
TOTAL					COP 10.000.000	

Fuente: El autor

Tabla 3 Descripción de Gastos Materiales.

BIBLIOGRAFÍA	JUSTIFICACIÓN	UNIDAD(ES) A LA CUAL PERTENECE		Horas de asignación al proyecto	Valor Unitario	Valor total
		Fuente 1	Fuente 2			
Materiales de oficina	Se requieren elementos como esferos, lápices, borradores y hojas entre otros	Entidad beneficiada con el proyecto	Recursos Propios	Sin determinar		COP 100.000
TOTAL				No Genera costos para el proyecto		

Fuente: El autor

Tabla 4 Descripción de Gastos Bibliografía.

BIBLIOGRAFÍA	JUSTIFICACIÓN	UNIDAD(ES) A LA CUAL PERTENECE		Horas de asignación al proyecto	Valor Unitario	Valor total
		Fuente 1	Fuente 2			
Acceso a Internet	Se requiere tener información actualizada	Entidad beneficiada con el proyecto	Acceso Wi - Fi desde la casa	50 horas	COP 2000	COP 100.000
TOTAL				100.000		

Fuente: El autor

Tabla 5 Descripción de Gastos Software.

SOFTWARE	JUSTIFICACIÓN	UNIDAD(ES) A LA CUAL PERTENECE		Horas de asignación al proyecto	Valor Unitario	Valor total
		Fuente 1	Fuente 2			
Windows y office	Software para creación de la documentación	Entidad beneficiada con el proyecto	Software adquirido con anterioridad	50	COP 10.000	COP 50.000
TOTAL				50.000		

Fuente: El autor

Tabla 6 Descripción De Gastos Servicios Técnicos.

SERVICIOS TÉCNICOS	JUSTIFICACIÓN	UNIDAD(ES) A LA CUAL PERTENECE		Horas de asignación al proyecto	Valor Unitario	Valor total
		Fuente 1	Fuente 2			
Ingenieros de sistemas	Equipos objeto de estudio	Entidad beneficiada con el proyecto		No Genera costos para el proyecto		No Genera costos para el proyecto
TOTAL				No Genera costos para el proyecto		

Fuente: El autor

15.1 Presupuesto Global.

Luego de tener todos los puntos anteriores como lo muestra la siguiente tabla 7 el costo total aproximado del proyecto es de COP[14] - 100.000.

Tabla 7 Presupuesto Global de la Propuesta por Fuentes de Financiación.

RUBROS	FUENTES DE FINANCIACIÓN		TOTAL
	Entidad beneficiada con el proyecto Fuente 1	Responsable del proyecto Fuente 2	
PERSONAL	X	X	No genera costos para el proyecto
EQUIPO	X	X	10.000.000
MATERIALES			COP 200.000
BIBLIOGRAFÍA	X	X	No genera costos para el proyecto
SOFTWARE	X	X	50.000
SERVICIOS TÉCNICOS	X		6.000.000
TOTAL			COP 16.250.000

Fuente: El autor

[14]El peso colombiano es la unidad monetaria de curso legal en la República de Colombia. Su abreviación formal es COP (ISO 4217).

16. METODOLOGÍA.

En el proyecto de grupo empresarial Ardila y asociados se va a utilizar la metodología PHVA, de la forma en la que se va a utilizar es la siguiente:

- **PLANIFICAR**: En esta etapa se definen los objetivos y cómo lograrlos, esto de acuerdo a políticas de la organización y necesidades del grupo empresarial Ardila y asociados.

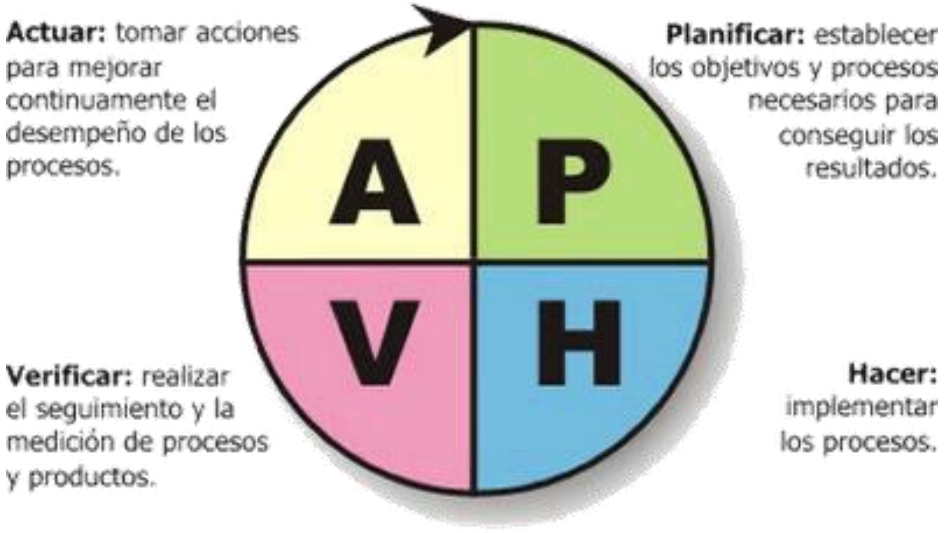
  También hay que tener encuentra que esta etapa es muy importante porque esta va hacer la base de las 3 etapas siguientes.

- **HACER**: En esta etapa es la más sencilla pero la que conlleva más tiempo debido que aquí vamos a ejecutar lo planificado. En estas dos etapas se tomara como eje central la elaboración del proyecto en el Grupo Empresarial Ardila y Asociados, sin embargo se va a abordar las dos siguientes fases como concejos hacia el grupo empresarial.

- **VERIFICAR**: En esta etapa se va a comprobar que los objetivos planteados en la fase de planificación, esta fase de verificación se hace seguimiento y medición de procesos por medio de auditorías internas y externas, las cuales dejaremos mencionadas como anexo.

- **ACTUAR**: Mediante este paso se realizan las acciones para el mejoramiento del desempeño de los procesos, se corrigen las desviaciones, se estandarizan los cambios, se realiza la formación y capacitación requerida y se define como monitorearlo.

Figura 3 Ciclo PHVA.

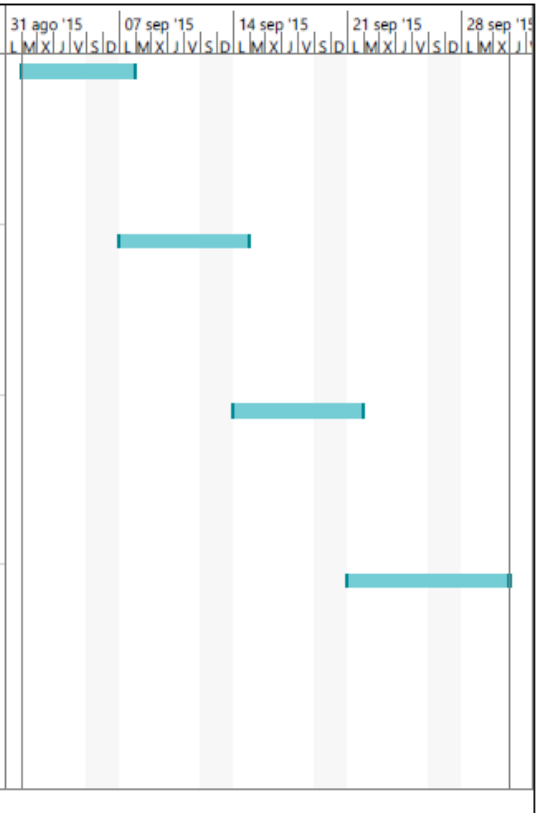


Fuente: http://www.blog-top.com/el-ciclo-phva-ejemplo-de-aplicacion-de-esta-herramienta-de-calidad.

17. CRONOGRAMA.

Figura 4 Descripción del cronograma.

Id	Nombre de tarea	Duración	Comienzo	Fin
1	Realizar un análisis de la situación actual de seguridad de la información en la empresa Grupo Empresarial Ardila y Asociados	5 días	mar 01/09/15	lun 07/09/15
2	Identificar los activos de información críticos de la empresa Grupo empresarial Ardila y asociados	6 días	lun 07/09/15	lun 14/09/15
3	Realizar un análisis de riesgos de los activos de información de la empresa Grupo Empresarial Ardila y Asociados.	6 días	lun 14/09/15	lun 21/09/15
4	Proponer las medidas de seguridad del control de acceso aplicables a la empresa Grupo Empresarial Ardila & Asociados buscando tener un control de la misma	8 días	lun 21/09/15	mié 30/09/15



Fuente: el autor.

18. DESARROLLO DEL PROYECTO.

18.1 Reunión de apertura gerencial.

Se realiza la reunión de apertura el día 28 de septiembre de 2015 en el cual se evidencia gran interés de la gerencia por preservar la información tanto física como digital evitando fuga de las misma, también se expresa mucha preocupación en este momento por perdida de información por medios extraíbles y por internet.

Se determinan los elementos con los que se cuentan para la elaboración del proyecto, y los elementos más relevantes para tener en cuenta, la gerencia de la empresa se muestra muy interesada en el proyecto pero se evidencia que los recursos económicos son muy limitados debido a que esta es una empresa pequeña.

18.2 Análisis de la situación actual de seguridad de la información en la empresa Grupo Empresarial Ardila y Asociados.

En el análisis inicia se determina que no existe ningún modelo de Sistema de gestión de la seguridad de la información, lo cual implica que no cuentan con ninguna políticas de administración de la información ni tampoco se cuenta con procesos para gestionar la accesibilidad de la información, en este momento se va a buscar crear políticas en busca de asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos fuga y perdida de la información.

Se concientiza a la gerencia que este proceso debe ser un proceso por largo para adaptar a los usuarios a los cambios internos de la organización así como los externos del entorno.

En el sistema de gestión de calidad de la empresa grupo empresarial Ardila y asociados el único tema que se encontró sobre salvaguardar la información es la siguiente:

- Físicamente: Se distribuye la información por cada proyecto que tiene la empresa y se almacenan en AZ según sea el caso, Contabilidad, Correspondencia, Contractuales

- Digitalmente: De la misma manera se distribuye la información en la red, se tienen creadas carpetas por departamentos y consorcios; en las carpetas del departamento no hay un esquema o directriz para guardar información, en las carpetas de cada proyecto se guardan según la siguiente distribución, sin embargo cualquier usuario puede modificar, eliminar esta documentación.
  La distribución es la siguiente:

    - Ficha técnica del contrato
    - Contractuales
    - Recursos Humanos
    - Compras
    - Gestión Técnica
    - Correspondencia
    - Diseños
    - Informes
    - Mails
    - Fotos

En el grupo empresarial Ardila y asociados se cuentan con los siguientes activos informáticos

- 1 servidor de almacenamiento de datos (sin configurar)
- 1 servidor con mysql para base de datos
- 20 computadores de escritorio
- Plan de ETB con 1 Ips fijas

- 1 router cisco para configurar red. (Sin configurar)

18.3 Identificación de los activos de información críticos de la empresa Grupo empresarial Ardila y asociados.

El primer paso en el Grupo Empresarial Ardila y Asociados es la identificación de activos, Según el siguiente listado.

Figura 5 Descripción de los activos en Grupo Empresarial Ardila y Asociados.

Fuente: Aplicativo ear / pilar.

Tabla 8 Activos sistema de información Grupo empresarial Ardila y asociados.

Tipo de Activo	Nombre	Proceso	Propietario del activo	Sistema de información Relacionado	Clasificación de la información	Áreas Asociadas	Criticidad			
							Conf	Integ	Disp	Total
Activos de la información	Información financiera	Contabilidad	Ardila y Asociados		Pública no clasificada	gerencia y contabilidad	7	10	9	**8,667**
	Información del departamento de licitaciones (Hojas de vida, certificaciones y balances de socios y profesionales presentados en cada licitación)	Licitaciones	Ardila y Asociados y Socios		Pública no clasificada	Contratación y gerencia	7	10	8	**8,333**
	Información Contractual (Contratos, Correspondencia enviada y recibida)	Administrativo	Ardila y Asociados y proveedores		Pública no clasificada	Contabilidad, licitaciones, recursos Humanos, HSEQ, Gerencia, Proceso Operativo	9	10	9	**9,333**
	Información de Recursos Humanos (Hojas de Vida de trabajadores, Capacitaciones)	Recursos Humanos	Ardila y Asociados		Pública no clasificada	Gerencia, Calidad, Recursos Humanos	9	9	9	**9**
	Información de Calidad (Inspecciones, reportes, Manuales, Documentos y formatos)	Calidad	Ardila y Asociados		Pública no clasificada	Contabilidad, licitaciones, recursos Humanos, HSEQ, Gerencia, Proceso Operativo	9	10	10	**9,667**
Activos de software	KAWAK	Calidad	Ardila y Asociados		Pública no clasificada	Contabilidad, licitaciones, recursos Humanos, HSEQ, Gerencia, Proceso Operativo	9	9	8	**8,667**
	Elisa	Contabilidad	Ardila y Asociados		Pública no clasificada	gerencia y contabilidad	10	10	10	**10**
Activos físicos	servidores	Sistemas	Ardila y Asociados		Pública no clasificada	Contabilidad, licitaciones, recursos Humanos, HSEQ, Gerencia, Proceso Operativo	10	8	10	**9,333**

Tipo de Activo	Nombre	Proceso	Propietario del activo	Sistema de información Relacionado	Clasificación de la información	Áreas Asociadas	Criticidad			
							Conf	Integ	Disp	Total
Activos físicos	equipos de computo	Sistemas	Ardila y Asociados		Pública no clasificada	Contabilidad, licitaciones, recursos Humanos, HSEQ, Gerencia, Proceso Operativo	7	8	9	**8**
	Archivos físico	Administrativo	Ardila y Asociados		Pública no clasificada	Contabilidad, licitaciones, recursos Humanos, HSEQ, Gerencia, Proceso Operativo	7	8	7	**7,333**
Servicios	correo	Sistemas	Proveedor		Pública no clasificada	Contabilidad, licitaciones, recursos Humanos, HSEQ, Gerencia, Proceso Operativo	8	9	8	**8,333**
	internet	Sistemas	Proveedor		Pública no clasificada	Contabilidad, licitaciones, recursos Humanos, HSEQ, Gerencia, Proceso Operativo	8	8	9	**8,333**
Personas	Coordinador de Sistemas	Sistemas	Ardila y Asociados		Pública no clasificada	Sistemas	8	8	8	**8**
	Revisor Fiscal	Contabilidad	Ardila y Asociados		Pública no clasificada	Contabilidad	8	8	7	**7,667**
	Contador	Contabilidad	Ardila y Asociados		Pública no clasificada	Contabilidad	9	10	9	**9,333**
	Auxiliar Contable	Contabilidad	Ardila y Asociados		Pública no clasificada	Contabilidad	9	8	9	**8,667**
	Auxiliar de licitaciones	Licitaciones	Ardila y Asociados		Pública no clasificada	Licitaciones	9	9	9	**9**
	Coordinador de licitaciones	Licitaciones	Ardila y Asociados		Pública no clasificada	Licitaciones	9	10	9	**9,333**
	Auxiliar Administrativo	Administrativo	Ardila y Asociados		Pública no clasificada	Administrativo	8	8	8	**8**

Tipo de Activo	Nombre	Proceso	Propietario del activo	Sistema de información Relacionado	Clasificación de la información	Áreas Asociadas	Criticidad			
							Conf	Integ	Disp	Total
	Director HSEQ	Calidad	Ardila y Asociados		Pública no clasificada	Calidad	8	8	7	**7,667**
	Director de Recursos Humanos	Recursos Humanos	Ardila y Asociados		Pública no clasificada	Recursos Humanos	9	9	9	**9**
	Gerencia	Gerencia	Ardila y Asociados		Pública no clasificada	Gerencia	10	10	10	**10**
	Gerencia Administrativa	Gerencia	Ardila y Asociados		Pública no clasificada	Gerencia	10	10	10	**10**
	Ingenieros Civiles	Operativo	Ardila y Asociados		Pública no clasificada	Operativo	9	10	9	**9,333**
	Auxiliares de Obra	Operativo	Ardila y Asociados		Pública no clasificada	Operativo	8	8	7	**7,667**
Imagen Reputación	Logo	Administrativo	Ardila y Asociados		Pública no clasificada	Contabilidad , licitaciones, recursos Humanos , HSEQ, Gerencia, Proceso Operativo	8	10	9	**9**
	Instalaciones	Administrativo	Ardila y Asociados		Pública no clasificada	Contabilidad , licitaciones, recursos Humanos , HSEQ, Gerencia, Proceso Operativo	8	10	9	**9**

Fuente: El autor

Se cuentan los activos de información que se evidencian en el levantamiento de la información, los activos esenciales del grupo empresarial Ardila y asociados entre los cuales se muestran los activos de información que se maneja, el personal con el que cuenta la organización, las aplicaciones con que cuenta el grupo empresarial, los servicios donde intervienen la información, los equipos informáticos que tiene la entidad, las instalaciones físicas y el core del negocio de la empresa.

18.4 Análisis de riesgos de los activos de información de la empresa Grupo Empresarial Ardila y asociados

En el grupo empresarial Ardila y asociados se evidencian los siguientes riesgos eminentes de los activos de información.

- **Perdida equipo de cómputo.**

  Los ingenieros que trabajan en obra, guardan sus archivos en computadores, y muchas veces no actualizan la red o no tienen acceso a ella, y si se les pierde el portátil, con ellos la información.

- **Perdida de información confidencial.**

  En licitaciones en las cuales participa la empresa se manejan muchos archivos los cuales la mayoría son confidenciales tales como certificaciones, cedulas, balances, extractos bancarios. Según antecedentes ha habido ex funcionarios que se han llevado esta información.

- **Perdida de información.**

  Posibles pérdidas de información por accesos permitidos por red a archivos que no se deberían tener acceso.

- **Falta de copias de seguridad.**

  No existen ni políticas, ni procedimientos para realizar copias de seguridad en los archivos ni en servidores.

- **Fuga de información.**

  No se tiene control de información en los formatos que utiliza la compañía debido a que no se encuentran políticas de usuario en los archivos compartidos, ni políticas de firma digital de archivos en los cuales los formatos puedan ser editados y plagiados

- **Acceso a redes y a servicios en red.**

  El modem y router es directamente del proveedor, y con este modem se tiene configurado el Wifi, lo que constituye un riesgo de seguridad debido a que desde una conexión por medio de Wifi se puede tener acceso al router

- **Controles contra códigos maliciosos.**

  Se ha encontrado archivos con contenido no laboral como videos y música compartido en la red lo cual fuera de gastar recursos innecesarios generan un peligro de virus y acceso no permitidos a equipos.

Tomando los peligros mencionados anteriormente vamos a proceder a valorar estos peligros y darle una ponderación a cada uno de ellos para evidenciar el estado de vulnerabilidad del grupo empresarial Ardila y asociados.

Valoración.

El Grupo Empresarial Ardila y Asociados se preocupa por la confiabilidad de su información esta preocupación se debe a los altos factores de manipulación del dato debido a la complejidad del proceso y las cantidad de personas que participan en el mismo.

También hay una especial sensibilidad relativa a la disponibilidad de la información necesaria en las obras y la generada en la misma.

La confidencialidad y pertinencia del de los archivos como la calidad del dato se considera prioritaria debido a que con estos archivos se generan nuevos contratos y cuentas de cobros.

Las bases de datos se hospedan en el servidor alojado en el centro de cómputo del Grupo Empresarial Ardila y Asociados el cual es multipropósito ya que este se comparte para la aplicación de Kawak como el dominio y otro servidor con la base de datos de Mysql alojando los datos de contabilidad; sin copias de seguridad exponiendo a la empresa a perdida de información.

En el tema de las personas encargadas de la dirección del Grupo Empresarial Ardila y Asociados pretende mantener estable el grupo de directivos debido a la alta rotación del personal en el Grupo Empresarial Ardila y Asociados y pérdida de confianza en el mercado por este motivo.

Las comunicaciones resultan ser uno de los temas de vital importancia en la disponibilidad de la información en las obras para tener disponibilidad en la documentación, pero no es solo pertinencia de la comunicación, también es pertinente tener la disponibilidad de equipos de cómputo y de lugares físicos para poder procesar la información.

En vista de todo ello, se ha consensuado la siguiente valoración de los activos del sistema. Sólo se han valorado explícitamente los activos superiores del árbol de dependencias, que quedan de la siguiente manera:

Figura 6 Descripción de la valoración de los dominios en Grupo Empresarial Ardila y Asociados.

activo / dominio de seguridad	[D]	[I]	[C]	[A]	[T]
[AA1] Edwin Javier Varon					
[essential] Activos esenciales	[9]	[9]	[10]	[10]	[9]
ip [Gestion] Gestion	[9]	[9]	[10]	[10]	[9]
is [Informacion] Informacion	[7]	[7]	[7]	[5]	[9]
Dominios de seguridad					
[base] Base	[9]	[9]	[10]	[10]	[9]

Fuente: Aplicativo ear / pilar.

Al utilizar la herramienta Pilar y valorar los activos del grupo empresarial Ardila y asociados se evidencia una valoración altísima de los activos de información como

lo podemos ver en la imagen anterior los activos de gestión son con los que se debe tener una disposición altísima.

En los archivos de información perteneciente a los archivos de gestión la valoración de 1 a 10 se encuentra la siguiente:

- Disponibilidad con una valoración de 9/10
- Integridad con una valoración de 9/10
- Confidencialidad con una valoración de 10/10
- Autenticidad con una valoración de 10/10
- Trazabilidad con una valoración de 9/10

Mientras que en los archivos netos de información de la entidad la valoración es más baja la valoración de 1 a 10 se encuentra la siguiente:

- Disponibilidad con una valoración de 7/10
- Integridad con una valoración de 7/10
- Confidencialidad con una valoración de 7/10
- Autenticidad con una valoración de 5/10
- Trazabilidad con una valoración de 9/10

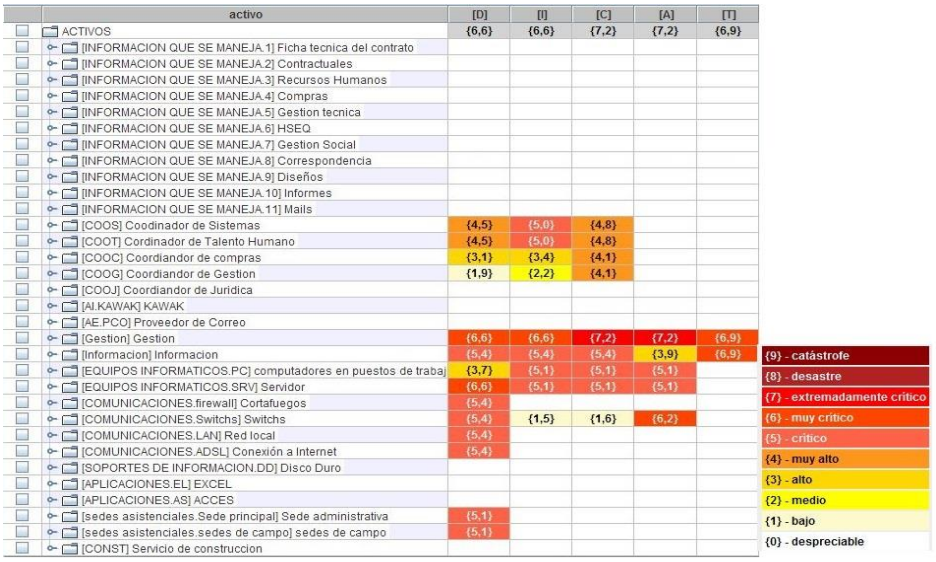
Para un total de archivos de información distribuido de la siguiente forma:

- Disponibilidad con una valoración de 9/10
- Integridad con una valoración de 9/10
- Confidencialidad con una valoración de 10/10
- Autenticidad con una valoración de 10/10
- Trazabilidad con una valoración de 9/10

18.5 riesgos de la información.

En el análisis hecho a los activos de información que se maneja en Grupo Empresarial Ardila y Asociados y Utilizando el programa Pilar que se basa en MAGERIT - versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información os da como resultado el siguiente cuadro de riesgos por áreas y por activos de información.

Figura 7 Descripción de los riesgos en Grupo Empresarial Ardila y Asociados.



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{6,6}	{6,6}	{7,2}	{7,2}	{6,9}
[INFORMACION QUE SE MANEJA_1] Ficha tecnica del contrato					
[INFORMACION QUE SE MANEJA_2] Contractuales					
[INFORMACION QUE SE MANEJA_3] Recursos Humanos					
[INFORMACION QUE SE MANEJA_4] Compras					
[INFORMACION QUE SE MANEJA_5] Gestion tecnica					
[INFORMACION QUE SE MANEJA_6] HSEQ					
[INFORMACION QUE SE MANEJA_7] Gestion Social					
[INFORMACION QUE SE MANEJA_8] Correspondencia					
[INFORMACION QUE SE MANEJA_9] Diseños					
[INFORMACION QUE SE MANEJA_10] Informes					
[INFORMACION QUE SE MANEJA_11] Mails					
[COOS] Coodinador de Sistemas	{4,5}	{5,0}	{4,8}		
[COOT] Cordinador de Talento Humano	{4,5}	{5,0}	{4,8}		
[COOC] Coordiandor de compras	{3,1}	{3,4}	{4,1}		
[COOG] Coordiandor de Gestion	{1,9}	{2,2}	{4,1}		
[COOJ] Coordiandor de Juridica					
[AI.KAWAK] KAWAK					
[AE.PCO] Proveedor de Correo					
[Gestion] Gestion	{6,6}	{6,6}	{7,2}	{7,2}	{6,9}
[Informacion] Informacion	{5,4}	{5,4}	{5,4}	{3,9}	{6,9}
[EQUIPOS INFORMATICOS.PC] computadores en puestos de trabaj	{3,7}	{5,1}	{5,1}	{5,1}	
[EQUIPOS INFORMATICOS.SRV] Servidor	{6,6}	{5,1}	{5,1}	{5,1}	
[COMUNICACIONES.firewall] Cortafuegos	{5,4}				
[COMUNICACIONES.Switchs] Switchs	{5,4}	{1,5}	{1,6}	{6,2}	
[COMUNICACIONES.LAN] Red local	{5,4}				
[COMUNICACIONES.ADSL] Conexión a Internet	{5,4}				
[SOPORTES DE INFORMACION.DD] Disco Duro					
[APLICACIONES.EL] EXCEL					
[APLICACIONES.AS] ACCES					
[sedes asistenciales.Sede principal] Sede administrativa	{5,1}				
[sedes asistenciales.sedes de campo] sedes de campo	{5,1}				
[CONST] Servicio de construccion					

{9} - catástrofe
{8} - desastre
{7} - extremadamente crítico
{6} - muy crítico
{5} - crítico
{4} - muy alto
{3} - alto
{2} - medio
{1} - bajo
{0} - despreciable

Fuente: Aplicativo ear / pilar.

En el cuadro anterior se evidencia que hay riegos altos debido a las faltas de políticas de la información, por eso se plantean como objetivo principal en este proyecto el diseño Política de seguridad para la empresa, las cuales veremos a continuación.

18.6 ANÁLISIS DEL ESTADO ACTUAL DE LA EMPRESA

Tabla 9 Análisis de seguridad para el grupo empresarial Ardila y asociados.

<table>
<tr><td>A.7</td><td colspan="3">SEGURIDAD DE LOS RECURSOS HUMANOS.</td></tr>
<tr><td>A.7.2</td><td colspan="3">Durante la ejecución del empleo.</td></tr>
<tr><td colspan="4">Objetivo: Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.</td></tr>
<tr><td rowspan="6">A.7.2.1</td><td rowspan="6">Responsabilidades de la Dirección</td><td rowspan="6">Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.</td><td>APLICA</td></tr>
<tr><td>SI NO</td></tr>
<tr><td>se deben aplicar a cada uno de los empleados políticas de seguridad informática con el fin de preservar la información y los activos de la institución</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI NO</td></tr>
<tr><td>con este manual se integran las políticas necesarias para el grupo empresarial Ardila y asociados</td></tr>
<tr><td rowspan="6">A.7.2.2</td><td rowspan="6">Toma de conciencia, educación y formación de la Seguridad de la Información.</td><td rowspan="6">Control: Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.</td><td>APLICA</td></tr>
<tr><td>SI NO</td></tr>
<tr><td>se nota desconocimientos de los procesos de la organización por eso se requiere hacer conciencia y divulgación de las políticas de la información</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI NO</td></tr>
<tr><td>se establecen capacitaciones a los</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td colspan="2">empleados antiguos y a los nuevos</td></tr>
<tr><td rowspan="5">A.7.2.3</td><td rowspan="5">Proceso disciplinario.</td><td rowspan="5">Control: Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">no existen sanciones legales en los contratos de los empleados por mal manejo de activos de información</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">implementación de sanciones legales a los empleados según las normas existentes en Colombia</td></tr>
<tr><td>A.7.3</td><td colspan="4">Terminación y cambio de empleo.</td></tr>
<tr><td colspan="5">Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.</td></tr>
<tr><td rowspan="5">A.7.3.1</td><td rowspan="5">Terminación o cambio de responsabilidades de empleo</td><td rowspan="5">Control: Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se debe guardar un tiempo prudente de sigilo profesional en los procesos de la empresa grupo empresarial Ardila y asociados</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Implementación de sanciones legales a los empleados según las normas existentes en Colombia</td></tr>
<tr><td>A.8</td><td colspan="4">GESTIÓN DE ACTIVOS</td></tr>
<tr><td>A.8.1</td><td colspan="4">Responsabilidad por los Activos.</td></tr>
<tr><td colspan="5">Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.</td></tr>
</table>

<table>
<tr><td rowspan="6">A.8.1.3</td><td rowspan="6">Uso Aceptable de los Activos</td><td rowspan="6">Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Manual del buen uso de los activos de información</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se debe hacer un manual de divulgación para el buen uso de los activos de información</td></tr>
<tr><td rowspan="6">A.8.1.4</td><td rowspan="6">Devolución de Activos.</td><td rowspan="6">Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Control de entrega de activos</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">se hace entrega formal al área de sistemas de los activos asignados al empleado del grupo empresarial Ardila y asociados</td></tr>
<tr><td>A.8.2</td><td colspan="3">Clasificación de la Información.</td></tr>
<tr><td colspan="4">Objetivo: Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.</td></tr>
<tr><td rowspan="6">A.8.2.1</td><td rowspan="6">Clasificación de la Información</td><td rowspan="6">Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Esto nos permitirá saber el valor de cada activo de información y el valor critico de cada activo</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">niveles de acceso a la información por medio de su clasificación</td></tr>
</table>

<table>
<tr><td>A.9</td><td colspan="3">CONTROL DE ACCESO</td></tr>
<tr><td>A.9.1</td><td colspan="3">Requisitos del negocio para control de acceso</td></tr>
<tr><td colspan="4">Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.</td></tr>
<tr><td rowspan="6">A.9.1.1</td><td rowspan="6">Política de control de acceso</td><td rowspan="6">Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El control de acceso físico y lógico con principios del menor privilegio permite tener un control sobre los riesgos de diseminación de información o acceso físico a los activos a personas no autorizadas.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Aunque se mantienen controles físicos y lógicos que garantizan el acceso con menor privilegio, no está documentada en una política de seguridad de la información.</td></tr>
<tr><td rowspan="6">A.9.1.2</td><td rowspan="6">Acceso a redes y a servicios en red</td><td rowspan="6">Control: Sólo se debe permitir acceso a los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Las redes y servicios de red proveen acceso a diferentes servicios dentro de la organización al personal autorizado.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Las redes están segmentadas en VLANS y el acceso a ella está protegido a personas no autorizadas.</td></tr>
</table>

<table>
<tr><td>A.9.2</td><td colspan="3">Gestión de Acceso de Usuarios.</td></tr>
<tr><td colspan="4">Objetivo: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.</td></tr>
<tr><td rowspan="5">A.9.2.1</td><td rowspan="5">Registro y cancelación del registro de usuarios</td><td rowspan="5">Control: Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">El control de acceso físico y lógico nos permite restringir accesos a la información de usuarios que ya no se encuentren en la organización</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="4">pare ello se manejan los usuarios del dominio de la organización</td></tr>
<tr><td rowspan="5">A.9.2.2</td><td rowspan="5">Suministro de acceso de usuarios</td><td rowspan="5">Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Con este tenemos un registro de accesos y modificaciones de la información</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="4">Entrega de Activos de información y usuarios</td></tr>
<tr><td rowspan="5">A.9.2.6</td><td rowspan="5">Cancelación o ajuste de los derechos de acceso.</td><td rowspan="5">Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Con este tenemos un registro de accesos y modificaciones de la información</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="4">Modificación de Activos de información y usuarios</td></tr>
</table>

<table>
<tr><td>A.9.4</td><td colspan="3">Control de Acceso a Sistemas y Aplicaciones.</td></tr>
<tr><td colspan="4">Objetivo: Prevenir el uso no autorizado de sistemas y aplicaciones.</td></tr>
<tr><td rowspan="5">A.9.4.1</td><td rowspan="5">Restricción de acceso a información.</td><td rowspan="5">Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.</td><td>APLICA</td></tr>
<tr><td>SI NO</td></tr>
<tr><td>El control de acceso a los aplicativos internos de la organización y aplicaciones de apoyo</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI NO</td></tr>
<tr><td>A.9.4.3</td><td>Sistema de Gestión de Contraseñas.</td><td>Control: los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.</td><td>APLICA
SI NO
Este control nos va a permitir garantizar contraseñas seguras y de difícil acceso en caso de ataque
IMPLEMENTA
SI NO
por medio del dominio garantizar el cambio de contraseñas de los usuarios</td></tr>
<tr><td>A.10</td><td colspan="3">CRIPTOGRAFÍA</td></tr>
<tr><td>A.10.1</td><td colspan="3">Controles Criptográficos.</td></tr>
<tr><td colspan="4">Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.</td></tr>
<tr><td>A.10.1</td><td></td><td></td><td>APLICA</td></tr>
</table>

	Política sobre el uso de controles Criptográficos.	***Control***: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.	**SI**	**NO**
			El control de acceso a información compartida con los consorciados y personas externa de la organización	
			IMPLEMENTA	
			SI	**NO**
			se debe crear una llave publica y una privada para compartir la información	
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL**			
A.11.2	**Equipos**			
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
A.11.2.5	Retiro de Activos.	***Control***: Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	**APLICA**	
			SI	**NO**
			El control de ubicación de cada uno de los activos de la información	
			IMPLEMENTA	
			SI	**NO**
			Aunque se crean controles por medio de identificación de los activos de la información, con sus respectiva ubicación	
A.11.2.6.	Seguridad de equipos y activos fuera del predio.	***Control***: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.	**APLICA**	
			SI	**NO**
			Este control nos permite garantizar la privacidad de la información contenidos en medios que se encuentran por fuera de la institución.	
			IMPLEMENTA	

			SI	**NO**
			Encriptar información contenido en medios extraíbles	
A.11.2.7.	Disposición segura o reutilización de equipos.	***Control***: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o reusó.	**APLICA**	
			SI	**NO**
			Controla el acceso no autorizado a información contenida en activos de información	
			IMPLEMENTA	
			SI	**NO**
			entrega de activos cuando el empleado se retira o hay cambio de activos	
A.12	**SEGURIDAD DE LAS OPERACIONES**			
A.12.1	**Procedimientos operacionales y responsabilidades.**			
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
A.12.1.1	Procedimientos de operación documentadas.	***Control***: Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.	**APLICA**	
			SI	**NO**
			Permite controlar desconocimiento de diversas situaciones que se puedan plantear dentro de la organización.	
			IMPLEMENTA	
			SI	**NO**
			se divulgan los manuales de procedimientos de la organización	
A.12.1.2.	Gestión de Cambios.	***Control***: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de	**APLICA**	
			SI	**NO**
			Permite controlar desconocimiento de diversas situaciones que se puedan	

		procesamiento de información que afectan la seguridad de la información.	plantear dentro de la organización.
			IMPLEMENTA
			SI / **NO**
			se divulgan los manuales de procedimientos de la organización
A.12.2	**Protección contra códigos maliciosos.**		
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.			
A.12.2.1	Controles contra códigos maliciosos.	***Control***: Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	**APLICA**
			SI / **NO**
			El control nos permite tener medidas para prevenir y responder ante ataque de virus
			IMPLEMENTA
			SI / **NO**
			Se implementa antivirus y Firewall corporativo en el grupo empresarial Ardila y asociados
A.12.3	**Copias de Respaldo.**		
Objetivo: Proteger contra la pérdida de datos.			
A.12.3.1.	Copias de respaldo de la información.	***Control***: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	**APLICA**
			SI / **NO**
			El control permite tener respuesta ante daños físicos y lógicos de activos de información
			IMPLEMENTA
			SI / **NO**
			Mantener copias de seguridad de cada uno de los equipos, imágenes de los servidores y dbexport

			de las base de datos de la organización,
A.12.4	**Registro y Seguimiento.**		
Objetivo: Registrar eventos y generar evidencia.			
A.12.4.2	Protección de la información de registro.	***Control***: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	**APLICA** **SI** / **NO** El control nos permite evitar violaciones a los privilegios de acceso a los equipos de la organización **IMPLEMENTA** **SI** / **NO** El control de instalación de software y modificaciones en los equipos por medio de niveles de usuarios y deshabilitar el usuario administrador
A.12.4.3.	Registros del administrador y del operador.	***Control***: Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.	**APLICA** **SI** / **NO** permite encontrar alteraciones en privilegios otorgados en los equipos pertenecientes al sistema de información **IMPLEMENTA** **SI** / **NO** realizar revisiones periódicas de los equipo que componen el sistema de información
A.12.4.4	Sincronización de relojes.	***Control***: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de	**APLICA** **SI** / **NO** este control nos permite identificar horas exactas de

<table>
<tr><td></td><td></td><td>seguridad se deben sincronizar con una única fuente de referencia de tiempo.</td><td>modificaciones o ataques</td></tr>
<tr><td></td><td></td><td></td><td>IMPLEMENTA</td></tr>
<tr><td></td><td></td><td></td><td>SI | NO</td></tr>
<tr><td></td><td></td><td></td><td>sincronizar los relojes de los equipos al servidor</td></tr>
<tr><td>A.12.5.</td><td colspan="3">Control de Software Operacional.</td></tr>
<tr><td colspan="4">Objetivo: Asegurarse de la integridad de los sistemas operacionales.</td></tr>
<tr><td rowspan="4">A.12.5.1.</td><td rowspan="4">Instalación de software en sistemas operativos.</td><td rowspan="4">Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>El control de programas instalados y manejo de licencias</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>se debe crear un procedimiento para la instalación de software en cabeza del área de sistemas</td></tr>
<tr><td>A.12.6.</td><td colspan="3">Gestión de vulnerabilidad técnica.</td></tr>
<tr><td colspan="4">Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.</td></tr>
<tr><td rowspan="4">A.12.6.2.</td><td rowspan="4">Restricciones sobre la instalación de Software.</td><td rowspan="4">Control: Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>permite el control de instalación de software no autorizados</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Manejo de usuarios de dominio para restringir permisos de instalación de software.</td></tr>
<tr><td>A.13</td><td colspan="3">SEGURIDAD DE LAS COMUNICACIONES.</td></tr>
</table>

A.13.1	**Gestión de Seguridad de Redes.**		
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.			
A.13.1.1.	Controles de redes.	***Control***: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	**APLICA** **SI** / **NO** El control de acceso por medio de redes diferentes para garantizar el trafico fiable entre las redes **IMPLEMENTA** **SI** / **NO** se crean diferentes tipos de redes aislando los servidores
A.13.1.3.	Separación en las redes.	***Control***: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	**APLICA** **SI** / **NO** permite el control de acceso a routers y mantiene aisladas los accesos a las mismas **IMPLEMENTA** **SI** / **NO** se crean tres redes diferentes y se separan las mismas para tener accesos diferentes
A.13	**SEGURIDAD DE LAS COMUNICACIONES.**		
A.13.2	**Transferencia de información.**		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			
A.13.2.3.	Mensajes electrónicos.	***Control***: Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	**APLICA** **SI** / **NO** permite controlar el flujo de información saliente del grupo

<table>
<tr><td></td><td></td><td></td><td>empresarial Ardila y asociados</td></tr>
<tr><td></td><td></td><td></td><td>IMPLEMENTA</td></tr>
<tr><td></td><td></td><td></td><td>SI | NO</td></tr>
<tr><td></td><td></td><td></td><td>mediante correo corporativo</td></tr>
<tr><td rowspan="5">A.13.2.4.</td><td rowspan="5">Acuerdos de confidencialidad o de no divulgación.</td><td rowspan="5">Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Control de información mediante el sigilo profesional</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
Incluir en los contratos cláusulas de sigilo profesional mediante las normas existentes en este momento en Colombia</td></tr>
<tr><td>A.14</td><td colspan="3">ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.</td></tr>
<tr><td>A.14.2.</td><td colspan="3">Seguridad en los procesos de desarrollo y de soporte.</td></tr>
<tr><td colspan="4">Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.</td></tr>
<tr><td rowspan="5">A.14.2.7.</td><td rowspan="5">Desarrollo contratado externamente.</td><td rowspan="5">Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>El control de acceso a los activos de información de aplicativos de la entidad y aplicativos de apoyo del grupo empresarial Ardila asociados.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
Revisión periódica del software de la organización y software de apoyo.</td></tr>
</table>

<table>
<tr><td>A.18</td><td colspan="3">CUMPLIMIENTO.</td></tr>
<tr><td>A.18.1.</td><td colspan="3">Cumplimiento de requisitos legales y contractuales.</td></tr>
<tr><td colspan="4">Objetivo: Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.</td></tr>
<tr><td rowspan="6">A.18.1.2.</td><td rowspan="6">Derechos de Propiedad Intelectual.</td><td rowspan="6">Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Con este controlar preservamos el derecho de autor de la organización, y de los proveedores de software contratados por la organización.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Procedimientos de compra de software, de revisión de los activos del sistema de información y sanciones legales vigentes</td></tr>
<tr><td rowspan="6">A.18.1.4.</td><td rowspan="6">Privacidad y protección de la información identificable personalmente.</td><td rowspan="6">Control: Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">controla la perdida y adulteración de la información</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Procedimientos de almacenamiento a los activos del sistema de información y sanciones legales vigentes en caso de violaciones</td></tr>
</table>

Fuente: El autor

18.7 POLÍTICAS DE LA EMPRESA.

18.7.1 POLÍTICA DE RECURSOS HUMANOS.

Tabla 10 Descripción de política de recursos humanos.

Nombre del documento:	**Política de Recursos Humanos**
Elaborado por:	Edwin Javier Varón
Revisado por:	Duvan Vargas
Elaborado para la empresa:	Grupo empresarial Ardila y Asociados
Fecha:	21/10/2015

Fuente: Aplicativo ear / pilar.

Descripción de la política:

La política de recursos humanos comprende las directivas que constituyen una base para la gestión eficaz de los recursos humanos del grupo empresarial Ardila y Asociados

Alcance:

Para todos los funcionarios, contratistas, pasantes, proveedores, personal externo del grupo empresarial Ardila y asociados

Aplicable.

Terminación y cambio de empleo

Durante la ejecución del empleo

Responsabilidades.

De la dirección:

Garantizar la toma de conciencia de los funcionarios en relación a la seguridad de la información y los lineamientos de recurso humano.

Promover la educación y formación de la Seguridad de la Información.

Tomar las medidas disciplinarias cuando sea requerido.

Responsabilidades del área de recurso humano:

Contar con un proceso formal de capacitaciones para que los empleados tengan conocimiento y tomen conciencia de políticas y procedimientos pertinentes a su cargo pero también Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

Difundirse los lineamientos de seguridad y políticas de seguridad dela información al momento de ingreso de cualquier empleado de la organización.

Contribuir activamente a la calidad de la gestión de los recursos humanos en toda la Empresa, proponiendo políticas apropiadas y velando con equidad por la coherencia de su aplicación.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Cualquier forma de intolerancia, de acoso o de discriminación será considerada como la expresión de una falta de respeto elemental y no será tolerada. Este principio debe ser aplicado a todos los niveles y en toda circunstancia sin excepción alguna.

La transparencia y la honestidad en las relaciones profesionales son condiciones sine qua non para toda comunicación eficaz.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

18.7.2 POLÍTICA DE GESTIÓN DE ACTIVOS.

Tabla 11 Descripción de política de Gestión de activos.

Nombre del documento:	**Política de Gestión de activos**
Elaborado por:	Edwin Javier Varón
Revisado por:	Duvan Vargas
Elaborado para la empresa:	Grupo empresarial Ardila y Asociados
Fecha:	21/10/2015

Fuente: Aplicativo ear / pilar.

Descripción de la política:

La política de **Gestión de activos** comprende las directivas que constituyen una base para la gestión eficaz de los activos del grupo empresarial Ardila y Asociados

Alcance:

Para todos los funcionarios, contratistas, pasantes, proveedores, personal externo del grupo empresarial Ardila y asociados

Aplicable.

Responsabilidad por los Activos.

Clasificación de la Información.

Responsabilidades.

De la dirección:

Garantizar la toma de conciencia de los funcionarios en relación a la seguridad de la información y los activos a cargo de cada uno de sus empleados.

Promover el buen uso de los activos de información.

Clasificar y asignar los activos de información.

Tomar las medidas disciplinarias cuando sea requerido.

Responsabilidades del área de inventarios:

Contar con un proceso formal de entrega de asignación de activos, mantener procedimientos actualizados de la entrega y recibo de activos de información, también Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación hacia estos activos.

Deben difundirse los lineamientos de seguridad y políticas de seguridad dela información al momento de ingreso de cualquier empleado de la organización.

Contribuir activamente a la preservación de los activos de información, proponiendo actividades apropiadas y velando con equidad por la coherencia de su aplicación.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Velar por el cuidado de los activos asignados al funcionario, cualquier daño del activo debe ser restaurado por el funcionario, este principio debe ser aplicado a todos los niveles y en toda circunstancia sin excepción alguna.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

18.7.3 POLÍTICA DE CONTROL DE ACCESO.

Tabla 12 Descripción de política de control de acceso.

Nombre del documento:	**Política de Control de acceso**
Elaborado por:	Edwin Javier Varón
Revisado por:	Duvan Vargas
Elaborado para la empresa:	Grupo empresarial Ardila y Asociados
Fecha:	21/10/2015

Fuente: Aplicativo ear / pilar.

Descripción de la política:

La política de Control de acceso comprende las directivas de Limitar el acceso a información y a instalaciones de procesamiento de información

Alcance:

Para todos los funcionarios, contratistas, pasantes, proveedores, personal externo del grupo empresarial Ardila y asociados

Aplicable.

Terminación y cambio de empleo

Durante la ejecución del empleo

Requisitos del negocio para control de acceso

Gestión de Acceso de Usuarios.

Control de Acceso a Sistemas y Aplicaciones.

Responsabilidades

De la dirección:

Garantizar que los activos de información tengan características de administración de usuarios, y tener los medios para permitir la gestión de los mismos.

Promover la educación y formación de la seguridad en los usuarios y contraseñas.

Tomar las medidas disciplinarias cuando sea requerido.

Responsabilidades del área de sistemas:

contar con un proceso formal de capacitaciones para que los empleados tengan conocimiento y tomen conciencia de la importancia de los manejos de usuarios y contraseñas, también se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

Deben difundirse los lineamientos de seguridad de usuarios y cambio de contraseñas al momento de ingreso de cualquier empleado de la organización.

Responsabilidades de los empleados, Contratistas, usuarios de aplicaciones tercer izadas visitantes externos y demás incluidos en el alcance:

No prestar los usuarios asignados y cambiar las claves de acceso con regularidad.

Preservar los activos de información con responsabilidad

Difundir los lineamientos de seguridad de usuarios y cambio de contraseñas al momento que sea requerido.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

18.7.4 POLÍTICA DE CRIPTOGRAFÍA.

Tabla 13 Descripción de política de Criptografía.

Nombre del documento:	**Política de Criptografía**
Elaborado por:	Edwin Javier Varón
Revisado por:	Duvan Vargas
Elaborado para la empresa:	Grupo empresarial Ardila y Asociados
Fecha:	21/10/2015

Fuente: Aplicativo ear / pilar.

Descripción de la política:

La política de criptografía comprende las directivas de asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.

Alcance:

Para todos los funcionarios, contratistas, pasantes, proveedores, personal externo del grupo empresarial Ardila y asociados

Aplicable.

- Controles Criptográficos.

Responsabilidades.

De la dirección:

Proveer los medios necesarios para realizar archivos criptográficos.
Garantizar las firmas de los archivos encriptados

Promover la educación y formación de criptografía en la entidad.

Tomar las medidas disciplinarias cuando sea requerido.

Responsabilidades del área de sistemas:

Mantener actualizada las llaves públicas y privadas para firmar los archivos que sean necesarios.

Contribuir activamente en la calidad de firma de archivos, proponiendo políticas apropiadas y velando con equidad por la coherencia de su aplicación.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Hacer buen uso de los archivos firmados en la entidad, Cuando se genere envío de información confidencial a través de cualquier medio electrónico debe aplicar el cifrado de la información o buscar quien le pueda proveer el cifrado a la misma.

No alterar ningún cifrado de la información que exista en la institución.

Contribuir activamente a mantener la criptografía a cualquier archivo del grupo empresarial Ardila y Asociados, si fuese testigo de cualquier evento que ponga en peligro el cifrado de algún archivo de la institución se encuentra en la obligación de denunciar el hecho ante el área de sistemas o en gerencia.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

18.7.5 POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL.

Tabla 14 Descripción Política de Seguridad Física Y ambiental

Nombre del documento:	**Política de Seguridad física y ambiental.**
Elaborado por:	Edwin Javier Varón
Revisado por:	Duvan Vargas
Elaborado para la empresa:	Grupo empresarial Ardila y Asociados
Fecha:	21/10/2015

Fuente: Aplicativo ear / pilar.

Descripción de la política:

La política de recursos Seguridad física y ambiental. Comprende las directivas que constituyen una base para la gestión eficaz de los recursos físicos del grupo empresarial Ardila y Asociados

Alcance:

Para todos los funcionarios, contratistas, pasantes, proveedores, personal externo del grupo empresarial Ardila y asociados

Aplicable.

Equipos de información

Responsabilidades.

De la dirección:

Garantizar la prestación de equipos de cómputo y herramientas necesarias para que los empleados puedan proteger los activos de información.

Promover la educación y formación de la preservación de equipos.

Contar con un sistema de reciclable que sea amigable con el medio ambiente

Tomar las medidas disciplinarias cuando sea requerido.

Responsabilidades del área de inventarios:

Contar con un proceso formal de preservación de activos de información, y comunicado para emprender acciones contra empleados que hayan cometido una violación preservación de la información.

Difundir procesos y procedimientos para la preservación de la información.

Contribuir activamente en el proceso de reciclaje de activos, proponiendo políticas apropiadas y velando con equidad por la coherencia de preservación del medio ambiente.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Preservar la información que sea perteneciente al grupo empresarial Ardila y Asociados.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

18.7.6 POLÍTICA DE SEGURIDAD DE LAS OPERACIONES.

Tabla 15 Descripción Seguridad de las Operaciones.

Nombre del documento:	**Política de Seguridad de las operaciones**
Elaborado por:	Edwin Javier Varón
Revisado por:	Duvan Vargas
Elaborado para la empresa:	Grupo empresarial Ardila y Asociados
Fecha:	21/10/2015

Fuente: Aplicativo ear / pilar.

Descripción de la política:

La política de Seguridad de las operaciones comprende las directivas que constituyen una base para las copias de seguridad eficaz de activos de información pertenecientes al grupo empresarial Ardila y Asociados

Alcance:

Para todos los funcionarios, contratistas, pasantes, proveedores, personal externo del grupo empresarial Ardila y asociados

Aplicable.

- Protección contra códigos maliciosos.
- Copias de Respaldo
- Registro y Seguimiento.
- Control de Software Operacional.

- Gestión de vulnerabilidad técnica.

Responsabilidades.

De la dirección:

Proveer herramientas necesarias para la protección, conservación y extracción de los activos de la información

Promover la educación y formación de la seguridad de las operaciones en la institución.

Tomar las medidas disciplinarias cuando sea requerido.

Responsabilidades del área de sistemas:

Contar con un proceso formal de copias de seguridad, auditorias y protección a los activos de la información del grupo Empresarial Ardila y Asociados.

Mantener actualizados los sistemas de información, con un antivirus y sistema de monitoreo para los sistemas de información de la entidad.

Deben difundirse los procedimientos y políticas del manejo de la información al momento de ingreso de cualquier empleado de la organización.

Contribuir activamente a la calidad de la gestión de los recursos de información en toda la Empresa, proponiendo políticas apropiadas y velando con equidad por la coherencia de su aplicación.

Responsabilidades de los empleados, y demás incluidos en el alcance:

No poner en peligro los sistemas de información del grupo empresarial Ardila y asociados, con archivos externos a la institución

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

18.7.7 POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES.

Tabla 16 Descripción política de Seguridad de las comunicaciones.

Nombre del documento:	**Política de Seguridad de las comunicaciones**
Elaborado por:	Edwin Javier Varón
Revisado por:	Duvan Vargas
Elaborado para la empresa:	Grupo empresarial Ardila y Asociados
Fecha:	21/10/2015

Fuente: Aplicativo ear / pilar.

Descripción de la política:

La política de Seguridad de las comunicaciones comprende las directivas que aseguran la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte en el grupo empresarial Ardila y Asociados.

Alcance:

Para todos los funcionarios, contratistas, pasantes, proveedores, personal externo del grupo empresarial Ardila y asociados

Aplicable.

- Gestión de Seguridad de Redes
- Transferencia de información

Responsabilidades

De la dirección:

Garantizar las herramientas necesarias para la gestión de redes y gestión de correos electrónicos.

Promover la educación y formación en el manejo y envió de la información.

Tomar las medidas disciplinarias cuando sea requerido.

Responsabilidades del área sistemas:

Gestionar y controlar las redes del grupo empresarial para proteger la información en sistemas y aplicaciones, también se deben separar en las redes según Los grupos de servicios de información, usuarios y sistemas de información.

Gestionar y controlar apropiadamente la información incluida en los mensajes electrónicos para evitar fugas de la información.

Identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Hacer buen uso de los correos electrónicos y redes del grupo empresarial Ardila y asociados

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

18.7.8 POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

Tabla 17 Descripción política de adquisición, desarrollo y manteniendo de sistemas.

Nombre del documento:	**Política de Adquisición, desarrollo y mantenimiento de sistemas**
Elaborado por:	Edwin Javier Varón
Revisado por:	Duvan Vargas
Elaborado para la empresa:	Grupo empresarial Ardila y Asociados
Fecha:	21/10/2015

Fuente: Aplicativo ear / pilar.

Descripción de la política:

La política de Adquisición, desarrollo y mantenimiento de sistemas comprende las directivas que constituyen actividad de desarrollo de sistemas subcontratados del grupo empresarial Ardila y Asociados

Alcance:

Para todos los funcionarios, contratistas, pasantes, proveedores, personal externo del grupo empresarial Ardila y asociados

Aplicable.

Seguridad en los procesos de desarrollo y de soporte.

Responsabilidades.

De la dirección:

Garantizar los pagos a contratos con terceros.

Tomar las medidas disciplinarias cuando sea requerido.

Garantizar la oportuna contratación de terceros cuando esto sea requerido.

Responsabilidades del área de sistemas:

Debe levantarse un requerimiento de información cuando sea requerida la contratación de un tercero.

Se debe hacer un proceso de auditorías al servicio que va a proveer el tercero.

Se debe tener un contrato de soporte con los servicios tercerizados.

Se debe hacer seguimiento al cumplimiento del contrato adquirido con el tercero y es responsabilidad del área de sistemas cumplir los deberes a los que se encuentre obligados en este contrato; pero también es responsabilidad del área hacer cumplir los deberes con la finalidad que se contrató a este tercero.

contar con un proceso formal de capacitaciones para que los empleados tengan conocimiento y tomen conciencia de políticas y procedimientos pertinentes a su cargo pero también Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

Deben difundirse los lineamientos de seguridad y políticas de seguridad dela información al momento de ingreso de cualquier empleado de la organización.

Contribuir activamente a la calidad de la gestión de los recursos humanos en toda la Empresa, proponiendo políticas apropiadas y velando con equidad por la coherencia de su aplicación.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Cualquier forma de intolerancia, de acoso o de discriminación será considerada como la expresión de una falta de respeto elemental y no será tolerada. Este principio debe ser aplicado a todos los niveles y en toda circunstancia sin excepción alguna.

La transparencia y la honestidad en las relaciones profesionales son condiciones obligatorias para toda comunicación eficaz entre los funcionarios tercerizados y los empleados del grupo empresarial Ardila y asociados.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

18.7.9 POLÍTICA DE CUMPLIMIENTO.

Tabla 18 Descripción política de cumplimiento

Nombre del documento:	**Política de Cumplimiento.**
Elaborado por:	Edwin Javier Varón
Revisado por:	Duvan Vargas
Elaborado para la empresa:	Grupo empresarial Ardila y Asociados
Fecha:	21/10/2015

Fuente: Aplicativo ear / pilar.

Descripción de la política:

La política de Cumplimiento comprende las directivas que constituyen el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados del grupo empresarial Ardila y Asociados.

Alcance:

Para todos los funcionarios, contratistas, pasantes, proveedores, personal externo del grupo empresarial Ardila y asociados

Aplicable.

Cumplimiento de requisitos legales y contractuales

Responsabilidades.

De la dirección:

Garantizar la adquisición de software original en la institución.

Promover la educación y formación del software del grupo empresarial Ardila y asociados.

Tomar las medidas disciplinarias cuando sea requerido.

Responsabilidades del área de sistemas:

Garantizar y verificación la instalación de las licencias requeridas en los sistemas de información

Hacer auditorias periódicas a los activos de información para garantizar su licenciamiento, en el caso de no contarse licencias para estos garantizar su desinstalación.

Responsabilidades de los empleados, y demás incluidos en el alcance:

No instalar software sin previa autorización del área de sistemas.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

18.8 Propuesta de las medidas de seguridad del control de acceso aplicables a la empresa Grupo Empresarial Ardila & Asociados buscando tener un control de la misma.

Se debe asegurar el acceso de usuarios autorizados y evitar el acceso a no autorizados a los activos de información del grupo empresarial Ardila y asociados.

- **Registros de usuarios.**

  Debe existir un proceso formal de registro modificación y cancelación con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.

- **Gestión de contraseñas para los usuarios.**

  La asignación de contraseñas se debe asignar por medio del dominio de la institución y se debe cambiar cada tres meses la misma por parte de los usuarios.

- **Revisión de los derechos de acceso de los usuarios.**

  Se debe por parte del área de sistemas hacer una auditoria cada dos meses de los permisos y roles de cada uno de los usuarios del grupo empresarial Ardila y asociados.

- **Uso de los accesos a servicios de red.**

Se debe dan los permisos a los usuarios a los servicios de red que ellos necesiten

- **Autenticación de usuarios para conexiones externas.**

  Se debe contar con un sistema de seguridad perimetral para garantizar el acceso a equipos por medio remoto, no se debe permitir la instalación de ningún programa que permita el acceso remoto a ningún equipo, y solo deben estar autorizados los usuarios de sistemas para tener acceso remoto a las maquinas.

- **Identificación de los equipos en las redes.**

  Se debe tener debidamente identificados los equipos con nombres nemotécnicos que permitan saber la ciudad del equipo y área del mismo.

- **Separación de redes.**

  Las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información, para ello se debe separa las redes de wiffi en los invitados y los usuarios del grupo empresarial Ardila y asociados, también se deben crear vlans en la cuales se dividan los servidores, los equipos del área administrativa y los del área de servicios.

18.9 MODELO DE SEGURIDAD DE LA INFORMACIÓN DEL GRUPO EMPRESARIAL ARDILA Y ASOCIADOS.

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración del GRUPO EMPRESARIAL ARDILA Y ASOCIADOS con respecto a la protección de los activos de información (los funcionarios, la información, los procesos, las tecnologías de información incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos.

El GRUPO EMPRESARIAL ARDILA Y ASOCIADOS, para el cumplimiento de su misión, visión, objetivo estratégico y apegado a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos tecnológicos.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del GRUPO EMPRESARIAL ARDILA Y ASOCIADOS

- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad.

- Esta política aplica a toda la entidad, sus funcionarios, terceros, aprendices, practicantes, proveedores del GRUPO EMPRESARIAL ARDILA Y ASOCIADOS y la ciudadanía en general.

Nivel de cumplimiento.

- Todas las personas cubiertas por el alcance y aplicabilidad se espera que se adhieran en un 100% de la política.

A continuación se establecen las 9 políticas de seguridad que soportan el SGSI del GRUPO EMPRESARIAL ARDILA Y ASOCIADOS:

- GRUPO EMPRESARIAL ARDILA Y ASOCIADOS ha decidido Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan con la **seguridad de los recursos humanos**.

- GRUPO EMPRESARIAL ARDILA Y ASOCIADOS ha hecho **Gestión de activos** el cual Identifica los activos organizacionales y definir las responsabilidades de protección apropiada y asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.

- GRUPO EMPRESARIAL ARDILA Y ASOCIADOS **implementará control de acceso** Identificando los activos organizacionales y definir las responsabilidades de protección apropiada y asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.

- GRUPO EMPRESARIAL ARDILA Y ASOCIADOS Asegura el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información. Por medio de su política de **Criptografía.**

- GRUPO EMPRESARIAL ARDILA Y ASOCIADOS Previene la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización, por medio de su política **Seguridad física y ambiental.**

- GRUPO EMPRESARIAL ARDILA Y ASOCIADOS Asegura las operaciones correctas y seguras de las instalaciones de procesamiento de información para Protegerla contra la pérdida de datos; Registra eventos y generar evidencia con su política de **Seguridad de las operaciones.**

- GRUPO EMPRESARIAL ARDILA Y ASOCIADOS Asegura la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa con su política **Seguridad de las comunicaciones.**

- GRUPO EMPRESARIAL ARDILA Y ASOCIADOS Asegura que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información. con su política **Adquisición, desarrollo y mantenimiento de sistemas.**

- GRUPO EMPRESARIAL ARDILA Y ASOCIADOS Evita violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad. con su **política de Cumplimiento.**

19. Ejecución de auditoria interna SGSI.

19.1 Informe de auditoría interna.

GENERALIDADES.

Las auditorias se realizan con el fin de comprobar que todos los procesos cumplen los requisitos establecidos en el Manual de calidad, en los procedimientos y demás documentos del Sistema Integrado de Gestión de la Calidad y generan y conservan los registros necesarios al realizar sus actividades.

Se pretende que oportuna e internamente se detecten las desviaciones que pudieran existir y se tomen las acciones necesarias, antes de que afecten al servicio.

Las auditorías internas comprenden las siguientes etapas: programación, apertura, desarrollo, cierre, reporte y seguimiento.

19.2 PERFIL DE LOS AUDITORES INTERNOS DE CALIDAD.

- Educación: Como mínimo nivel técnico.

- Formación: Curso de Auditor Interno de Calidad mínimo 24 horas.

- Experiencia: Mínimo 6 meses como funcionario o contratista en auditoria en la Ciudad de Bogotá.

- Habilidades:
  - Planificación y organización del trabajo.
  - Puntualidad y buen manejo del tiempo.
  - Facilidad de expresión verbal y escrita dada la necesidad de preparar informes y de expresar oralmente ideas y resultados a los auditados y/o jefes inmediatos.

- Capacidad de análisis, de tal forma que pueda relacionar los datos y hechos que encuentra en una auditoria, con base en un razonamiento lógico para llegar a conclusiones basadas en evidencia objetiva.
- Mantener la confidencialidad y seguridad de la información.

19.3 PROGRAMACIÓN.

El programa anual de Auditorías Internas de Calidad, será definido por el Jefe de la Oficina de Planeación y aprobado por el Comité de Calidad. El programa de Auditorías será revisado cuando sea necesario e incluir las auditorías adicionales convenientes.

El Programa Anual de Auditorias de Calidad se define y modifica de acuerdo con las siguientes consideraciones:

- Todos los procesos deben ser auditados como mínimo una vez al año, excepto aquellos que presenten un mayor número de hallazgos de la auditoria.

- Cambios organizacionales: (retiro de personas “claves”, fusión/ creación/ comisión de cargos, elevada rotación del personal).

- Resultados no satisfactorios de auditorías internas o externas anteriores.

- Hallazgos detectados en la revisión por la gerencia.

- Aumento de quejas y reclamos.

- Solicitud para la realización de auditoría que no se encuentre establecida en el Programa Anual pero que se considere necesaria y oportuna ya sea por el Dueño

del Proceso, Jefes de áreas o Responsable del Sistema Integrado de Gestión de la Calidad.

El Jefe de la Oficina de Planeación notificará el Programa de Auditorías mediante carta a todos los responsables de los procesos.

PREPARACIÓN DEL PLAN DE AUDITORIAS.

En el Programa de Auditorías se establece el equipo auditor que realizará las auditorías a cada uno de los procesos que conforman el Sistema Integrado de Gestión de la Calidad. El equipo auditor designado para realizar la auditoria a cada uno de los procesos debe elaborar el Plan de Auditoría en el formato Plan de Auditoría, previa revisión de la documentación del proceso asignado.

El Plan de Auditorias debe ser presentado por el equipo auditor al Responsable del Proceso para su revisión y aprobación.

19.4 ELABORACIÓN DE LAS LISTAS DE VERIFICACIÓN.

El equipo auditor debe preparar la Auditoria del proceso designado elaborando el Formato de Lista de Verificación para Auditorías Internas para lo cual debe considerar.

· Los requisitos y normas le aplican al proceso a auditar.

· Caracterización, procedimientos, instructivos y otros documentos del proceso

· Antecedentes de otras auditorias;

· Indicadores de gestión y desempeño del proceso

· Formatos de No Conformidades u Observaciones;

· Información de las No Conformidades, Acciones Preventivas - Correctivas que se han presentado en las áreas y/o actividades a auditar.

Las listas de verificación sirven como guía, pero de ninguna manera limitan el alcance establecido para cada actividad, pudiendo ser modificadas de acuerdo a la manera como se vaya desarrollando la auditoria, llevando a investigaciones más profundas y/o ligeramente fuera del alcance original.

Las listas de verificación son los documentos en los cuales se documentan los resultados obtenidos al realizar la auditoria, en cada área y en cada actividad. Contienen instrucciones claras y precisas de lo que se pretende verificar, de tal manera que un auditor al leerla, perciba claramente todo lo que debe investigar.

19.5 EJECUCIÓN DE AUDITORIA.

19.5.1 Reunión de Apertura

El propósito de la reunión de apertura es:

· Presentar a los miembros del equipo auditor.

· Revisar el alcance y los objetivos de la auditoría.

· Mostrar un breve resumen de los métodos y procedimientos a ser usados.

· Establecer los canales de comunicación oficial entre el equipo auditor y el auditado.

· Confirmar que los recursos y facilidades necesarias para el equipo auditor estén disponibles.

· Confirmar las fechas y horas para las reuniones de cierre e intermedias entre el equipo auditor y el auditado.

· Aclarar cualquier detalle confuso del plan de auditoría.

19.5.2 Recolección de evidencias o desarrollo de auditoria.

El equipo auditor ejecuta la auditoria, revisando y examinando las evidencias objetivas de la realización de actividades como registros, reportes, certificaciones, calificaciones, capacitación, entrenamiento, etc.; Evidenciando si el proceso es adecuado y cumple con los requisitos.

En caso de detectar una probable no conformidad u observación, se agotan todas las posibilidades antes de documentarla como tal, consultando con el resto del

grupo, identificando el origen, las consecuencias presentes y futuras, así como si se tratara de un problema puntual o genérico.

Las no conformidades y observaciones se registran, anotando todos los datos y describiendo clara y precisamente la situación que ocasiona la no conformidad o la observación. También se anotan los detalles que se puedan comprobar (documentos, fechas, miembros y números entre otros).

El seguimiento de puntos abiertos de auditorías anteriores debe ser documentado en un lugar específico de la lista de verificación, para indicar el estado real que presentan estos puntos.

19.5.3 Reunión de Cierre.

Al término de la auditoría, y previamente a la preparación del informe, el equipo auditor se reúne con los representantes del proceso auditado, con el propósito principal de presentar en forma general los resultados de la auditoría y sus conclusiones, considerando la efectividad del Sistema Integrado de Gestión de la Información. El auditor líder es el portavoz del equipo, pero podrá solicitar la intervención de cualquiera de los miembros del grupo auditor para reforzar aspectos particulares.

19.6 INFORME DE LA AUDITORIA INTERNA DE CALIDAD.

El equipo auditor debe reunirse y elaborar el Informe de Auditorías Internas de Calidad, donde evidencian los resultados encontrados en la ejecución de la auditoria. El equipo auditor debe presentar a más tardar al tercer (3) día después de haber realizado la auditoria el informe al dueño del proceso para que este lo revise y firme. Una vez firmado por el Responsable del proceso el Equipo auditor debe remitirlo a la Oficina de Planeación para su consolidación y seguimiento.

19.7 INFORME FINAL DEL CIERRE DE LA AUDITORIAS.

La Oficina de Planeación, reúne los informes elaborados por cada auditor, y con ellos construye un reporte final, pudiendo auxiliarse en esta integración de uno o varios auditores participantes, pero manteniendo la responsabilidad de la

elaboración y conclusión del reporte. Este reporte se consigna en el formato Informe de Cierre de Auditoria.

19.8 SEGUIMIENTO.

Los Responsables de los procesos, deben establecer las acciones correctivas y preventivas para las no conformidades u observaciones detectadas por los auditores y de esta forma evitar que se vuelvan a repetir.

Se programará una auditoria de seguimiento para verificar el cierre de las no conformidades detectadas cerrando las acciones correctivas y/o preventivas generadas para las no conformidades u observaciones existentes diligenciando el Formato de Acción Preventiva

20. CONCLUSIONES.

- Se Diseña las políticas de seguridad de la información para la empresa Grupo Empresarial Ardila, donde se estipula de manera específica cada una de las medidas técnicas y de gestión del grupo empresarial para garantizar la seguridad en la información que maneja la organización.

- Se Realizó un análisis de la situación actual en cuanto a la seguridad de la información del Grupo Empresarial Ardila y Asociados, donde se evidencia las falencias de seguridad en la empresa, y se generan estrategias y políticas para subsanar debilidades y generar a la Organización óptimos métodos de seguridad informática.

- Se realizó un análisis de las vulnerabilidades en los accesos a los documentos de la empresa Grupo Empresarial Ardila y Asociados, donde se crean políticas para mitigar estas debilidades; restringiendo el acceso a la información por nivel de usuario, donde se vela por la confidencialidad de la información y donde se disminuyen la mayoría de ataques posibles que se realizan utilizando empleados de la compañía.

- Se identificó los riesgos más relevantes en la empresa Grupo Empresarial Ardila & Asociados con la ayuda de la herramienta pilar basada en la metodología Magerit, la cual nos permite hacer planes de mitigación de riesgos.

- Se Realizó un plan de auditorías internas para de la empresa Grupo Empresarial Ardila & Asociados, para que con estas se garantice la continuidad del plan de seguridad informática y así mismo que cumplan con la gestión de calidad de la misma, contribuyendo de esta forma a la reducción de costos.

- Se configuraron los Router de la empresa Grupo Empresarial Ardila & Asociados con el fin de controlar el acceso a las redes WIFI en el grupo empresarial, donde el uso de las TIC'S son hoy en día una de las vulnerabilidades principales y que los empleados muchas veces lo desconocen, con esta estrategia podemos garantizar un mejor manejo de las redes inalámbricas de la organización.

- En el análisis que se realiza a la empresa Ardila y asociados podemos evidenciar una visión más real del estado de seguridad en la entidad lo cual permite conocer y estimar los puntos críticos donde se debían enfocar los esfuerzos y recursos para disminuir los riesgos de seguridad informática.

- Una de las fuentes de amenaza más frecuente es el error humano, lo cual para el Grupo Empresarial Ardila y Asociados fue uno de sus puntos críticos, para evitar esto se ha configurado un dominio, control parental y permisos de usuarios, con el objetivo de resguardar la información existente en el grupo empresarial; también se crearon políticas de usuarios y de administración de la seguridad informática, y por último se crearon planes de auditorías para vigilar el cumplimiento de estas políticas con esto se busca reducir potenciales problemas al futuro y mejorar la seguridad en la entidad.

21. BIBLIOGRAFÍA.

- *COLCONECTADA, NORMAS ICONTEC. http://www.colconectada.com/normas-icontec/* 02 DE 04 DE 2015 http://www.colconectada.com/normas-icontec/ (último acceso: 02 de 04 de 2015).
- *ASOCIADOS*, *GRUPO EMPRESARIAL ARDILA Y ASOCIADOS.www.grupoardila.com.co* 10 de 04 de 2015 www.grupoardila.com.co (último acceso: 10 de 04 de 2015).
- *NORMAS APA, American Psychological AssociationNormas APA* 08 de 01 de 2010 http://normasapa.com/que-son-las-normas-apa/ (último acceso: 25 de 04 de 2015).
- *ACISA,Asociacion Colombiana de Ingenieros de Sistemas ACISAsociacion Colombiana de Ingenieros de Sistemas ACIS* 25 de 04 de 2015 http://www.acis.org.co/index.php?id=1634 (último acceso: 25 de 04 de 2015).
- *UPCT, Canal UPCT de la Universidad Politécnica de Cartagena Metodología de investigación*.Fuentes de información para la investigación*Metodología de investigación.Fuentes de información para la investigación*CartagenaMurciaCanal UPCT (último acceso: 21 de 04 de 2015).
- *COMUNIDAD PARA PROFESIONALES DE LA SEGURIDAD, Community Quals BlogCommunity Quals Blog* 08 de 10 de 2012 https://community.qualys.com/welcome (último acceso: 06 de 04 de 2015).
- *CORTE CONSTITUCIONAL, Corte Constitucional Corte Constitucional* 18 de 08 de 2012 http://www.corteconstitucional.gov.co/relatoria/1992/T-444-92.htm (último acceso: 14 de 04 de 2015).
- *EAN, EAN Escuela de Administración de Negocios. 13 de 08 de 2014 http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.*http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012..pdf;jsessionid=7A998747D496DE3D601DA6852780C40F?sequence=1 (último acceso: 22 de 03 de 2015).
- *INCIBE - Instituto Nacional de Ciberseguridad INCIBE - Instituto Nacional de Ciberseguridad .* 01 de 01 de 2015 :///C:/Users/80048906/Downloads/cn_malware_moviles.pdf (último acceso: 26 de 03 de 2015).
- *INSPITING A SAFE AND SECURE CYBER WORLD ISC(2)INSPITING A SAFE AND SECURE CYBER WORLD ISC(2)* 01 de 04 de 2015 https://www.isc2.org/cissp/default.aspx (último acceso: 25 de 04 de 2015).
- *MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS,ministerio de Hacienda y Administraciones Públicas.* 18 de 08 de 2012 http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Document

acion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf (último acceso: 13 de 04 de 2015).

- *NORMASAPA ,normasapa.* 25 de 04 de 2015.http://normasapa.com (último acceso: 25 de 04 de 2015).

- *PASOS DE UN ANTEPROYECTO, pasos de un anteproyecto,* 25 de 04 de 2015. https://plus.google.com/101956551767119288842/posts/VT5KQKFthoY?pid=6060803176863952434&oid=101956551767119288842 (último acceso: 25 de 04 de 2015).

- *DECRETO 4062 DE 2011, DECRETO 4062 DE 2011.*Por el cual se crea la Unidad Administrativa Especial Migración Colombia, se establece su objetivo y estructura. DECRETO 4062 DE 2011EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA (último acceso: 25 de 04 de 2015).

- *UNIVERSIDAD A DISTANCIA, UNAD. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA*. *Recursos compartidos unad.* 29 de 09 de 2014. http://66.165.175.235/campus18_20142/file.php/596/entorno_de_conocimiento/Investigacion_en_seguridad_informatica.pdf (último acceso: 29 de 09 de 2014).

- UNIVERSIDAD DE LAS CALIFORNIAS INTERNACIONAL, Universidad de las Californias Internacional TTESIS Qué es el Marco Teórico*TTESIS Qué es el Marco Teórico.mpg*MexicoUDCcampus Virtual (último acceso: 25 de 04 de 2015).

- *UNIVERSIDAD NACIONAL,Universidad Nacional* 19 de 02 de 2015. http://www.dnic.unal.edu.co/docs/guia_para_elaborar_politicas_v1_0.pdf (último acceso: 25 de 04 de 2015).

- *PÚBLICAS, MINISTERIO DE HACIENDA Y ADMINISTRACIONES. ministerio de Hacienda y Administraciones Públicas.* 10 de 10 de 2012. http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf (último acceso: 10 de 10 de 2012).

- NACIONAL, UNIVERSIDAD. *UNIVERSIDAD NACIONAL.* 01 de 12 de 2013. http://www.dnic.unal.edu.co/docs/guia_para_elaborar_politicas_v1_0.pdf (último acceso: 01 de 12 de 2013).

- WIKI, WIKIPEDIA. *WIKIPEDIA.* 21 de 09 de 2015. https://es.wikipedia.org/wiki/ISO/IEC_27001 (último acceso: 22 de 09 de 2015).

- WIKI, WIKIPEDIA. WIKIPEDIA. 21 de 09 de 2015. https://es.wikipedia.org/wiki/Magerit_(metodolog%C3%ADa) (último acceso: 23 de 09 de 2015).

- ADMINISTRACIONELECTRONICA.*ADMINISTRACIONELECTRONICA.* 21 de 09 de 2015. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VgMVmvl_Oko (último acceso: 23 de 09 de 2015).

- MSNSEGURIDAD, MSNSEGURIDAD. *MSNSEGURIDAD.* 21 de 09 de 2015. http://msnseguridad.blogspot.com/2012/08/seguridad-informatica-la-seguridad.html (último acceso: 23 de 09 de 2015).

- WIKI, WIKIPEDIA. *WIKIPEDIA.* 21 de 09 de 2015. http://es.wikipedia.org/wiki/Acciones_legales (último acceso: 17 de 10 de 2015).

- WIKI, WIKIPEDIA. *WIKIPEDIA*. 21 de 09 de 2015. https://camiloangel.wordpress.com/2010/09/03/%C2%BFque-es-un-activo-de-informacion/ (último acceso: 17 de 10 de 2015).

- WIKI, WIKIPEDIA*. WIKIPEDIA*. 21 de 09 de 2015. https://es.wikipedia.org/wiki/Criptograf%C3%Ada (último acceso: 17 de 10 de 2015).

- WIKI, WIKIPEDIA*. WIKIPEDIA*. 21 de 09 de 2015. http://es.wikipedia.org/wiki/Sistemas (último acceso: 17 de 10 de 2015).

- WIKI, WIKIPEDIA. *WIKIPEDIA*. 21 de 09 de 2015. https://es.wikipedia.org/wiki/Aplicaci%C3%B3n_inform%C3%A1tica (último acceso: 17 de 10 de 2015).

- REDEURO, REDEURO. *SISTEMA CALIDAD*. 21 de 09 de 2015. http://www.redeuroparc.org/sistema_calidad_turistica/ManualGuiaparalaelaboraciondeProcedimientosO.pdf (último acceso: 17 de 10 de 2015).

- KASPERSKY, KASPERSKY. *CENTER*. 21 de 09 de 2015. http://latam.kaspersky.com/mx/internet-security-center/definitions/malicious-code (último acceso: 17 de 10 de 2015).

- WIKI, WIKIPEDIA. *WIKIPEDIA*. 21 de 09 de 2015. https://es.wikipedia.org/wiki/Copia_de_seguridad (último acceso: 17 de 10 de 2015).

- WIKI, WIKIPEDIA. *WIKIPEDIA*. 21 de 09 de 2015. https://es.wikipedia.org/wiki/Transferencia_de_archivos (último acceso: 17 de 10 de 2015).

- WIKI, WIKIPEDIA. *WIKIPEDIA*. 21 de 09 de 2015. https://es.wikipedia.org/wiki/Auditor%C3%Ada (último acceso: 17 de 10 de 2015).

- WIKI, WIKIPEDIA. *WIKIPEDIA*. 21 de 09 de 2015. https://es.wikipedia.org/wiki/Licencia_de_software (último acceso: 17 de 10 de 2015).

- MINTIC, MINTIC. *MINTIC*. 21 de 09 de 2015. http://css.mintic.gov.co/ap/gel4/images/Modelo_Seguridad_Informacion_2_01.pdf (último acceso: 17 de 10 de 2015).

- MINTIC, MINTIC. *MINTIC*. 21 de 09 de 2015. http://css.mintic.gov.co/ap/gel4/images/SeguridaddelaInformacion2_0_Anexo7_Clasificacion-de-Activos.pdf (último acceso: 17 de 10 de 2015).

- MINTIC, MINTIC. *MINTIC*. 21 de 09 de 2015. http://css.mintic.gov.co/ap/gel4/images/ResumenEjecutivo_Seguridad.pdf (último acceso: 17 de 10 de 2015).

20. ANEXOS.

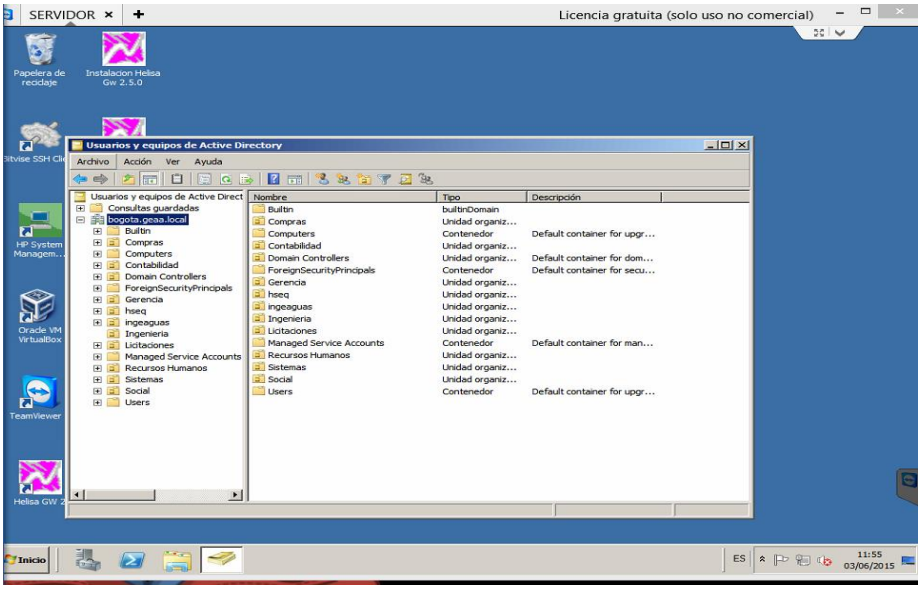
Anexo A: Control de acceso aplicables a la empresa Grupo Empresarial Ardila & Asociados.

En los siguientes anexos vamos a dar ejemplos de cómo se puede implementar las políticas de seguridad planteada en el proyecto en el numeral 18.7

1.1 Configuración de dominio.

Se crea un dominio llamado Bogotá en el directorio activo y se crean los grupos de trabajo requeridos anteriormente por la empresa; los cuales son: compras, Contabilidad, Gerencia, Hseq, Ingeniería, Licitaciones, Recursos Humanos, Sistemas, Social.

Figura 8 Configuración de carpetas Dominio del Grupo Empresarial Ardila y Asociados.

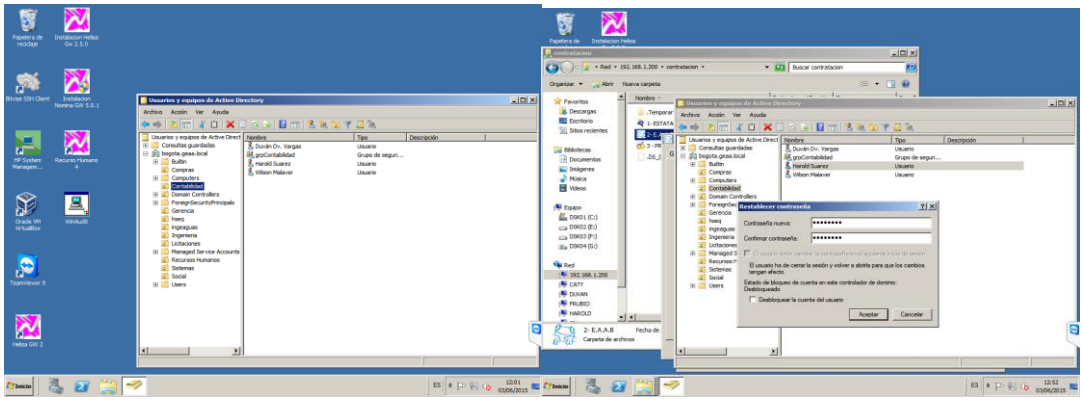


Fuente: Servidor grupo empresarial Ardila y asociados.

1.2 Configuración de usuarios.

Son creados los usuarios por dependencias en el directorio Activo

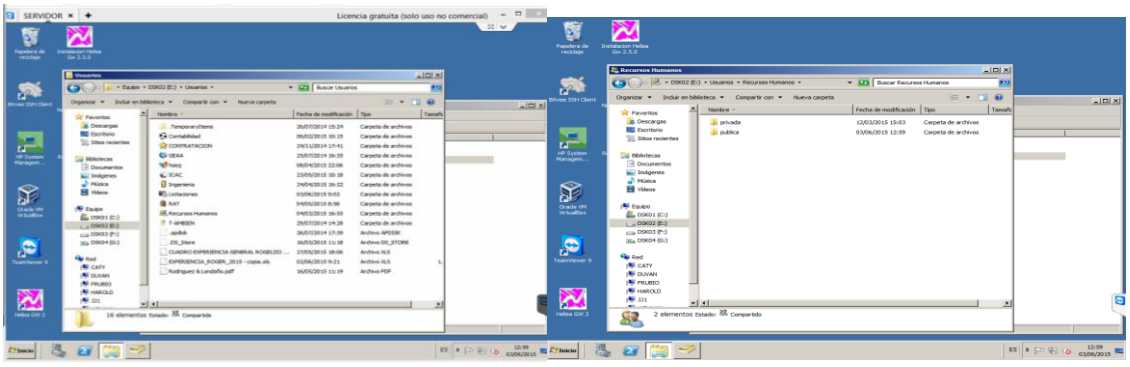
Figura 9 Configuración de usuarios Dominio del Grupo Empresarial Ardila y Asociados.



Fuente: Servidor grupo empresarial Ardila y asociados.

Se crean carpetas por grupo de trabajo, en cada una de ellas se encuentra una carpeta privada por el grupo (solo la pueden ver miembros de ese grupo) y una pública para aquellos archivos que son compartidos por todos los grupos.

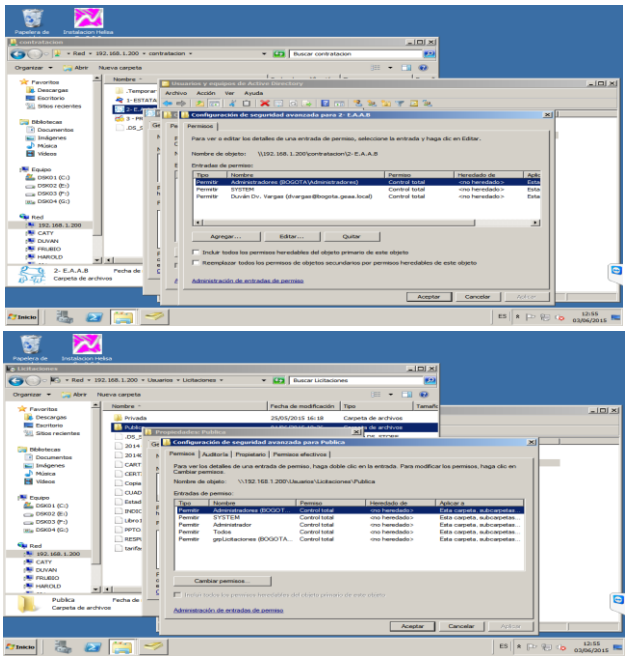
Figura 10 Configuración de grupos de usuarios Dominio del Grupo Empresarial Ardila y Asociados.



Fuente: Servidor grupo empresarial Ardila y asociados.

Se crean permisos de lectura y escritura y ejecución, según el perfil de cada usuario o cada grupo

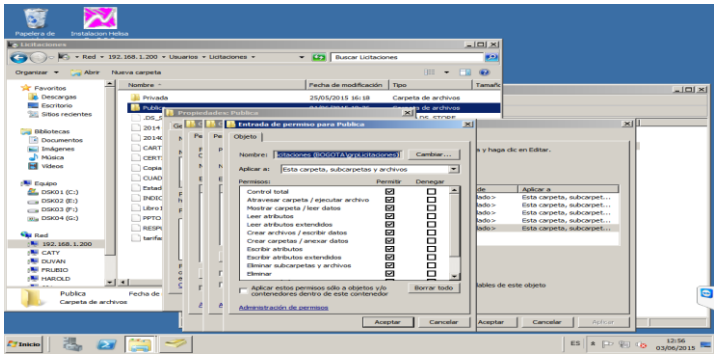
Figura 11 Configuración de permisos de usuarios Dominio del Grupo Empresarial Ardila y Asociados.



Fuente: Servidor grupo empresarial Ardila y asociados.

Por efectos propios del trabajo y actividad económica de la empresa, se manejan un conglomerado empresarial donde se maneja administrativamente 3 empresas y cada nuevo proyecto que ejecutan en un consorcio (Jurídicamente es una nueva empresa). Estas carpetas es necesario que todos los usuarios tengan acceso

Figura 12 Configuración de permisos de grupos Dominio del Grupo Empresarial Ardila y Asociados.

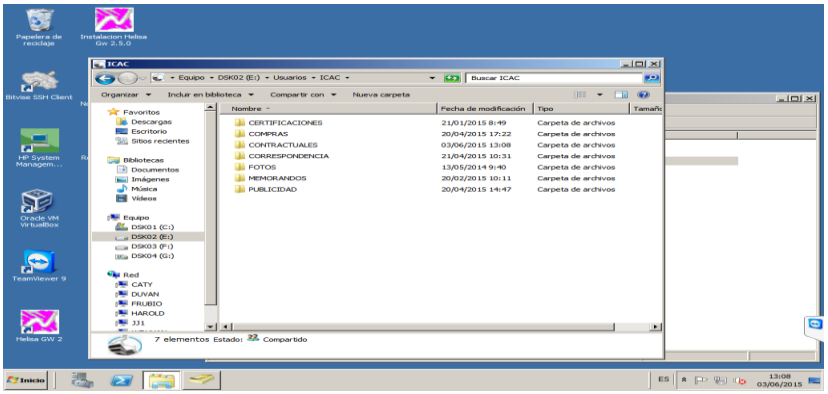


Fuente: Servidor grupo empresarial Ardila y asociados.

1.3 Configuración de carpetas.

En estas carpetas se configuran los permisos de la siguiente manera, Los documentos contractuales y de correspondencia todos los usuarios tienen acceso a crear un nuevo documento, pero no pueden eliminar uno existente. Solo el administrador o el ingeniero encargado del proyecto o persona encargada del proceso.

Figura 13 Configuración de carpetas compartidas en Dominio del Grupo Empresarial Ardila y Asociados.

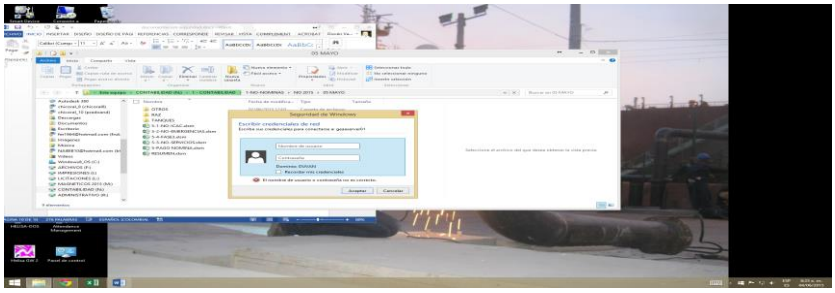


Fuente: Servidor grupo empresarial Ardila y asociados.

1.4 Configuración equipos cliente.

En la configuración de las terminales al acceder al servidor en el equipo cliente se ingresa el usuario y contraseña creada en el servidor para autenticarse y poder acceder a las carpetas a las que tiene acceso.

Figura 14 Configuración de acceso al Dominio del Grupo Empresarial Ardila y Asociados.



Fuente: equipo grupo empresarial Ardila y asociados.

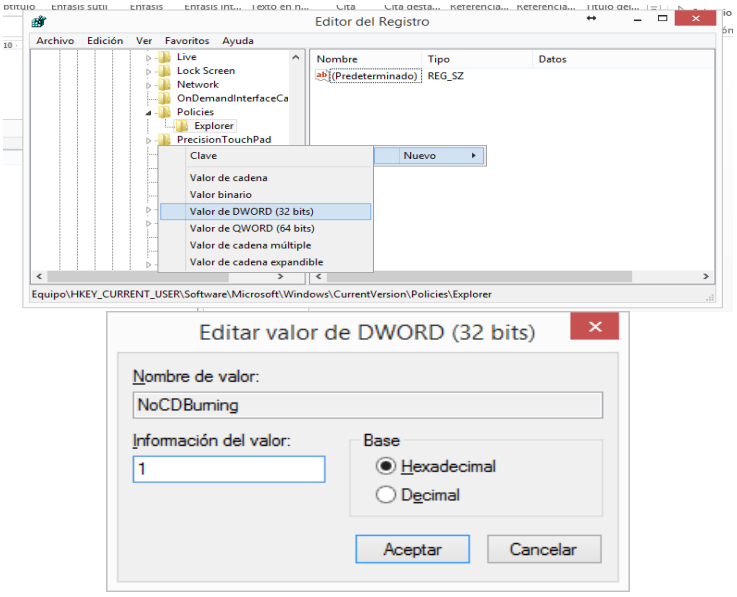
1.5 Bloqueo de grabación por medios extraíbles - CD USB.

1.5.1 Bloqueo de quemado.

Evitar el grabado de CD-DVD con información confidencial y/o estratégica de la entidad (norma ISO-27001 – circular 052), por eso evitaremos que copien documentos a cd y dvd Para desactivar la función de grabación de discos ópticos, deberemos acceder al registro de Windows por lo que se sugiere siempre una copia de seguridad antes de seguir.

- En menú Inicio escribe regedit y presiona Enter y estarás en el editor del registro.
- Buscar la clave HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies
- Crea una nueva clave dentro de **Policies** y nómbrala **Explorer**
- Dentro de la clave Explorer crea un valor DWORD de 32Bits y nómbralo **NoCDBurning**.
- Pincha 2 veces en NoCDBurning y dale un valor decimal 1.
- Cierra el editor del registro.

Figura 15 Configuración de equipos clientes del Grupo Empresarial Ardila y Asociados para medios extraíbles.

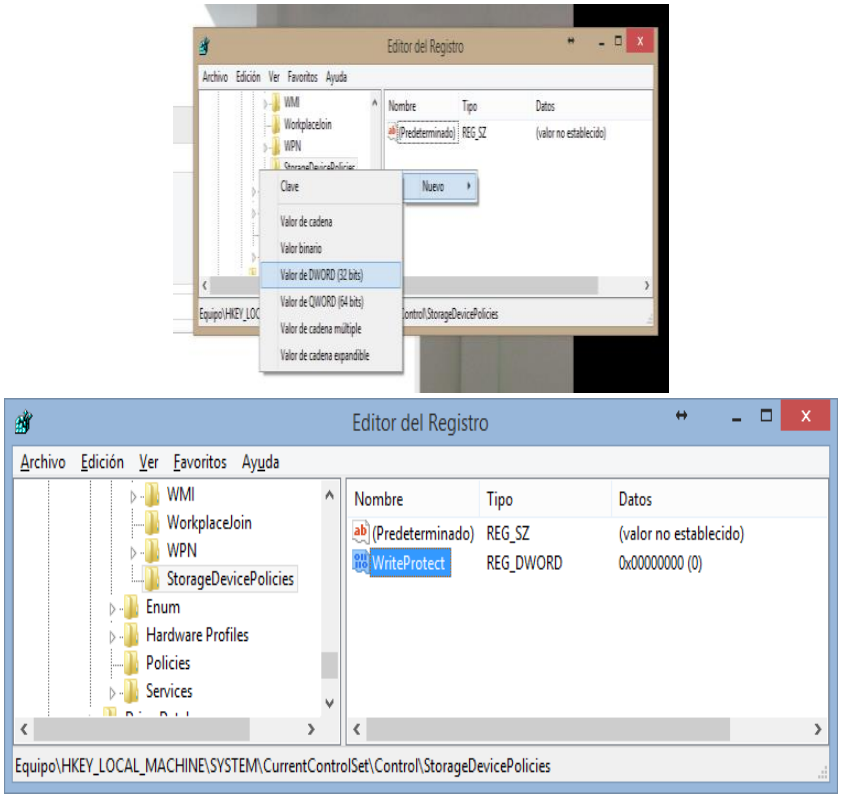


Fuente: equipo grupo empresarial Ardila y asociados.

1.5.2 Boqueo de copia a usb.

Evitar el grabado de extraído de información confidencial y/o estratégica de la entidad (norma ISO-27001 – circular 052) por eso evitaremos que copien documentos de la PC a una USB, para esto Vamos a inicio>ejecutar, y escribes> regedit, y buscamos esta llave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies, en el panel de la derecha debes buscar o crear mediante edición>nuevo una nueva clave DWORD y denominarla WriteProtect, y a continuación deberás introducir cómo valor un 1 (uno) para habilitar la escritura de datos en dispositivos USB o bien un 0 (cero) para deshabilitar dicha escritura. Y así quedaron bloqueados los computadores para copiar archivos a las usb en la empresa Ardila y asociados

Figura 16 Configuración de equipos clientes del Grupo Empresarial Ardila y Asociados para usb.



Fuente: equipo grupo empresarial Ardila y asociados.

1.6 Bloqueo de la tecla Print Script.

Bloqueo selectivo de tecla Print Script (evita capturar información confidencial tomando foto de pantalla) (norma ISO-27001 – circular 052), para esto vamos a crear un archivo en el blog de notas con el siguiente contenido “[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout]
"Scancode
Map"=hex:00,00,00,00,00,00,00,00,04,00,00,00,00,00,2a,e0,00,00,37,e0,\
00,00,54,00,00,00,00,00” y lo vamos a llamar habilitar_bloqueio_printscreen.reg, después de guardarlo lo ejecutamos y con esto evitamos el uso de la tecla Print Script

Figura 17 Configuración de equipos clientes del Grupo Empresarial Ardila y Asociados para no tomar Print Script.

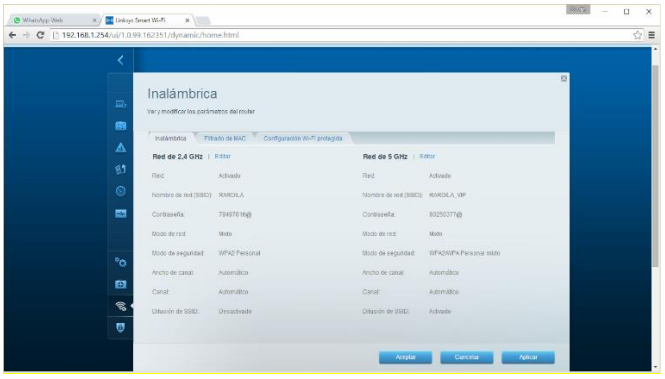
Fuente: equipo grupo empresarial Ardila y asociados.

1.7 Configuración Red.

1.7.1 Configuración Wifi - creación de redes para invitados y usuarios

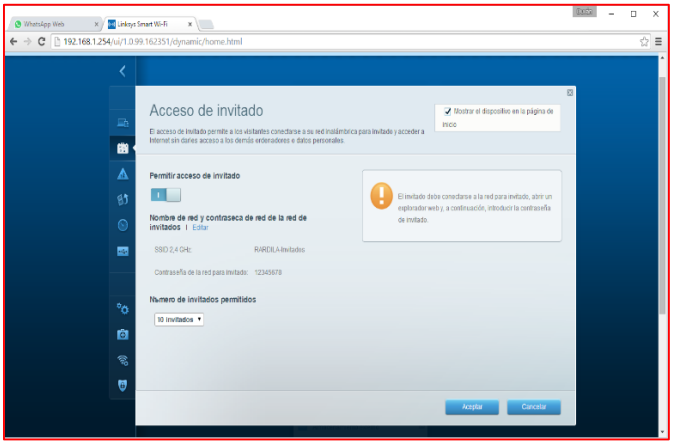
Se solicita al cliente Grupo Empresarial Ardila y Asociados que compre un rourter propio (aparte del operador), se configura el mismo y se dejan dos redes Invitados con un acceso limitado para 20 usuarios y una red oculta y solo se pueden conectar los equipos que tengan filtrado de mac

Figura 18 Configuración de wifi para usuarios e invitados del Grupo Empresarial Ardila y Asociados.



Fuente: Router grupo empresarial Ardila y asociados.

Figura 19 Configuración de números de equipos que acedan a la red de invitados del Grupo Empresarial Ardila y Asociados.

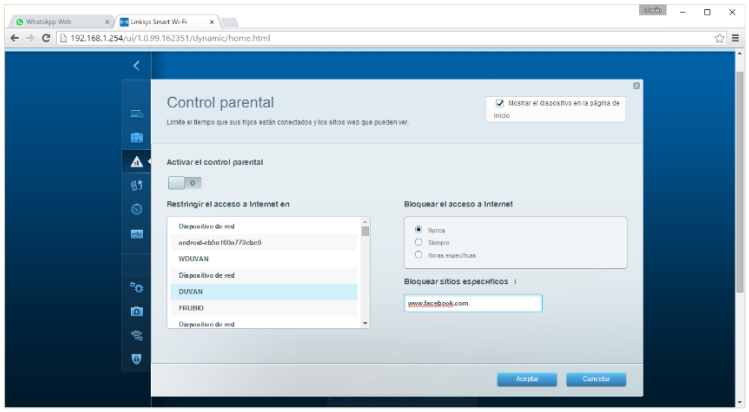


Fuente: Router grupo empresarial Ardila y asociados.

1.8 Bloqueo de acceso a páginas de internet.

El router que se compro tiene control parental con el objetivo de realizar bloqueo en la navegación de páginas que no sean necesarias para la entidad, para evitar tráfico de páginas innecesarias evitar accesos no deseados y optimizar los recursos.

Figura 20 Configuración de equipos clientes del Grupo Empresarial Ardila y Asociados para no tomar Print Script.



Fuente: Router grupo empresarial Ardila y asociados.