DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) CON BASE LOS LINEAMIENTOS Y LAS COMUNICACIONES EMITIDAS POR LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA, SEGÚN CIRCULAR EXTERNA 029 DE 2014 PARA EL INSTITUTO FINANCIERO PARA EL DESARROLLO DEL HUILA- INFIHUILA.

CARLA PATRICIA TRUJILLO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
PROYECTO
NEIVA 2019

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) CON BASE LOS LINEAMIENTOS Y LAS COMUNICACIONES EMITIDAS POR LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA, SEGÚN CIRCULAR EXTERNA 029 DE 2014 PARA EL INSTITUTO FINANCIERO PARA EL DESARROLLO DEL HUILA- INFIHUILA.

CARLA PATRICIA TRUJILLO HERNANDEZ

Trabajo presentado como requisito para el título de Especialista en Seguridad Informática

Director Ing. Fernando Zambrano Hernández

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
NEIVA 2019

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

Neiva Huila, 2019

DEDICATORIA

Este proyecto de especialización en seguridad Informática lo dedico en primera instancia a Dios padre todo poderoso, que nos das a diario sabiduría y discernimiento para tomar las mejores decisiones en todos los ambientes de nuestras vidas, también doy gracias a esta dedicatoria a mi familia que siempre están ahí para apoyarme en todas las circunstancias de la vida y cumplir mis metas propuestos en mi existencia.

AGRADECIMIENTOS

Agradezco a la Universidad Nacional Abierta y a Distancia por la oportunidad de ingresar en la especialización de seguridad Informática, también al tutor: Fernando zambrano por su valiosa colaboración, tiempo y dedicación, a las dudas e inquietudes que he tenido a la hora empezar a desarrollar este Diseño de sistema de gestión de seguridad de la información (SGSI) con base los lineamientos y las comunicaciones emitidas por la superintendencia financiera de Colombia, según circular Externa 029 de 2014 para el Instituto Financiero para el desarrollo del Huila- INFIHUILA.

RESUMEN

El Instituto Financiero para el desarrollo del Huila -INFIHUILA, es una institución financiera calificada por la Sociedad Calificadora de Valores ***Valué and Risk Rating S.A*** la cual se ha puesto en la tarea de trabajar en su certificación ante la Superintendencia financiera de Colombia, basando en los parámetros contemplados en la circular externa 029 de 2014 emanada por dicha entidad. el proyecto aplicado se basa en el diseño un sistema de Gestión de la Seguridad de la Información, en la cual se delinearán canales, medios, seguridad y calidad en el manejo de los datos.

El sistema de Gestión de Seguridad de la Información SGSI, abarca distintas fases, las cuales son el diagnostico o auditorias de dominios, implementación de la metodología MAGERIT la cual monitorea los activos de la entidad minimizando amenazas, evaluando controles, implementación de políticas, procedimientos y capacitación al usuario en temas de seguridad de la información. Como consecuencia de la implementación de dicho diseño se generará integridad, disponibilidad y confiabilidad de la información.

Palabras clave: SGSI, Gel, ética hacking, Incidentes de seguridad, metodologías, MINTIC.

ABSTRACT

The Financial Institute for the development of Huila -INFIHUILA, is a financial institution qualified by the Value and Risk Rating SA Qualification Society which has been put in the task of working on its certification before the Financial Superintendence of Colombia, based on the parameters contemplated in external circular 029 of 2014 issued by said entity. The project applied is based on the design of an Information Security Management system, in which channels, media, security and quality in data management will be delineated.

The SGSI Information Security Management system covers different phases, which are the diagnosis or audit of domains, implementation of the MAGERIT methodology which monitors the assets of the entity minimizing threats, evaluating controls, implementation of policies, procedures and user training on information security issues. Because of the implementation of said design, integrity, availability and reliability of the information will be generated.

Keywords: SGSI, Gel, ethics hacking, Security incidents, methodologies, MINTIC.

CONTENIDO

pág.

LISTADO DE FIGURAS

LISTADO DE TABLAS

INTRODUCCION

El presente trabajo se realiza como necesidad del instituto Financiero para el Desarrollo del Huila -**INFIHUILA** el crecimiento continuo en sus servicios a sus diferentes clientes u entidades, y así mismo fortalecer el área de tecnología. Para ello se es conveniente la contratación de perfiles capacitados en temas de seguridad, que tienen como finalidad estar atentos a las diferentes amenazas, También es necesario la implementación de mecanismos o herramientas como el Sistema de Gestión de Seguridad de la Información (SGSI), el riesgo está siempre latente. La confidencialidad, integridad y disponibilidad de la información en la organización, es fundamental para el aumento de su competitividad.

El Instituto Financiero para el Desarrollo del Huila **-INFIHUILA** Distingue los datos como un segmento fundamental en el cumplimiento directo de los objetivos caracterizados por la metodología de la entidad, razón por la cual es vital para la organización construir un sistema en el que se garantice que los datos estén suficientemente asegurados de manera autónoma en la forma como se cuida, maneja, mueve o guarda la información.

La seguridad de la información es una prioridad para INFIHUILA por consiguiente se es necesario la implementación del “Sistema de Gestión de Seguridad de la Información” el cual instaura la forma más apropiada de conocer los aspectos de seguridad de la información mediante el enlace de los recursos humanos y técnicos, protegidos por medidas administrativas, que certifiquen la renovación de controles seguros para alcanzar el nivel de seguridad preciso en comunicación con los objetivos de la entidad territorial, de forma que se conserve perpetuamente el riesgo por debajo del nivel asumible.

Este proyecto se presenta como una propuesta metodológica de implementación, análisis de riesgos, vulnerabilidades y tratamiento de ellos mismos.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

El INFIHUILA un instituto de Fomento y desarrollo que propende por el mejoramiento económico y social de los municipios del Departamento del Huila. Es instituto descentralizado de carácter departamental, localizado en la ciudad de Neiva, dotado de personería jurídica, autonomía administrativa y patrimonio propio, adscrito al despacho del gobernador[1].

En ese momento, si bien los hechos demuestran que el Instituto Financiero para el Desarrollo del Huila- INFIHUILA está dirigido por el lineamiento del Concejo directivo, hay que tener presente que la Superintendencia Financiera de Colombia "SFC", puso en conocimiento a todos INFIS la importancia ser certificados Sopena de ir desmontando gradualmente los recursos de los institutos lo cual trae como consecuencia su liquidación. por lo tanto la Superintendencia Financiera de Colombia ha puesto en conocimiento a todos los INFIS la circular externa 029 del 2014 y circular externa 034 del 2013, con modificaciones al decreto 029 del 2018 en las cuales se presenta las directrices; canales, medios, seguridad y calidad en el manejo de información.

Siguiendo las exigencias de la Superintendencia Financiera de Colombia "SFC" se ha de trabajar en el diseño de un Sistema de Gestión de Seguridad de la Información "SGSI" basado en las normas ISO 27001 para garantizar la Integridad, Confiabilidad y Accesibilidad de la Información con las cuales permitirá minimizar riesgos ante el

[1] (Instituto Financiero para el Desarrollo del Huila, s.f.)

desarrollo de nuevas tecnologías.

1.2 DESCRIPCIÓN DEL PROBLEMA

Teniendo en cuenta lo citado en el párrafo anterior, es importante buscar una ayuda que le permita a la organización tomar las decisiones correctas, adecuadas y afortunadas con respecto a la seguridad de los datos, como lo indica el rápido avance de los marcos de datos en todo el mundo y de esta manera convertirse en una Contribución vital para garantizar la infraestructura y los procedimientos, a la luz de las mejores prácticas de flujo y reflujo. Para abordar este problema para el Instituto Financiero para el desarrollo del Huila - **INFIHUILA**, es importante tener consultorías y estancias sobre modelos de seguridad de informática, que deben incorporar modificaciones y actualizaciones a los acuerdos, directrices, métodos y medidas, y además exposiciones, preparación para todos los funcionarios de la organización.

2. FORMULACION DEL PROBLEMA

¿Cómo mediante un diseño de Sistema de Gestión de la Seguridad de la Información se puede facilitar el proceso de certificación y vigilancia del Instituto Financiero para el Desarrollo del Huila-INFIHUILA?

3. JUSTIFICACION

El Instituto Financiero para el Desarrollo del Huila - INFIHUILA urge certificarse dando cumplimiento a las exigencias de la Superintendencia Financiera de Colombia “SFC” en cuanto al diseño de un Sistema de Gestión de Seguridad de la Información para así garantizar su normal funcionamiento, adquiriendo nuevos recursos y extender más créditos de fomento para el desarrollo del Departamento, y a la vez sea responsivo a las nuevas tecnologías siempre conservando los pilares de la seguridad Informática que son confiabilidad, integridad, disponibilidad y calidad de la información.

4. OBJETIVO

Diseñar un Sistema de Gestión de Seguridad de la Información al instituto Financiero para el desarrollo del Huila - INFIHUILA, con base en los lineamientos y las comunicaciones emitidas por la Superintendencia Financiera de Colombia “SFC”, según circular Externa 029 de 2014 y la circular 034 de 2013.

4.1 OBJETIVOS ESPECÍFICOS

- Realizar diagnóstico inicial sobre la infraestructura tecnológica al instituto financiero para el desarrollo del Huila.
- Establecer canales, medios, seguridad y calidad en el manejo de información para la infraestructura tecnológica del Instituto.
- Identificación de activos de información con la correspondiente matriz de Riesgos aplicable a la entidad.
- Implementar políticas de seguridad de la información aplicables para el Instituto Financiero para el Desarrollo del Huila –“INFIHUILA”.
- Sensibilizar y concientizar al usuario de la importancia de la seguridad de la información para continuo mejoramiento del INFIHUILA.

5. ALCANCE

El alcance del proyecto incorpora el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para todos los procesos del Instituto Financiero para el Desarrollo del Huila - **INFIHUILA**, que debe alinearse con los objetivos vitales Del Instituto.

Razón que el Instituto debe apoyar el tema de seguridad de la Información como su principal prioridad, y deberá ser adoptado por todos sus funcionarios de acuerdo con el nivel de responsabilidades definidas para cada uno, garantizando un alto nivel de protección y seguridad de la información.

6. MARCO REFERENCIAL

ANTECEDENTES

Nombre de la organización: Instituto Financiero para el desarrollo del Huila - **INFIHUILA**

7. MARCO CONTEXTUAL

El sistema de gestión de la información se desarrollará en el instituto financiero para el desarrollo del Huila - **INFIHUILA**, se va a realizar como medida de protección y prevención del sistema de información ya que es un sistema débil y vulnerable a amenazas.

Que es el Infihuila?

El INFIHUILA Instituto de Fomento y Desarrollo que propende por el mejoramiento económico y social de los municipios del Departamento del Huila.[2]

En el año 2020, seremos reconocidos como el instituto de fomento y desarrollo líder en la prestación de servicios financieros para inversiones públicas y

[2] (Instituto Financiero para el Desarrollo del Huila, s.f.)

acompañamiento empresarial al sector productivo en el ámbito nacional.

los primeros años de la década de los setenta y con el único fin de dar respuesta a las necesidades de los municipios del Departamento del Huila, principalmente en lo atinente al desarrollo económico, social y cultural, un puñado de dirigentes políticos junto con los gobernantes territoriales de entonces, con visión futurista de la región y del país, entre ellos los señores: don Héctor Polanía Sánchez, conocedor como el que más de los municipios huilenses sobre todo de sus necesidades, en compañía de doña Elcira Olaya de Cleves, José Lizardo Ribera, Hernando Gómez Trujillo, Ismael Quintero G., Carlos F. Falla Yepes y Jesús Vargas Valencia, entre otros, tienen la acertada iniciativa de crear un ente con recursos del departamento que permitiera identificar las necesidades de inversión de capital fijo de las localidades, que hiciera créditos con garantía para desarrollar proyectos de infraestructura y sobre todo que prestara asistencia técnica y administrativa con el fin de capacitarlos para planear y ejecutar su propio desarrollo.[3]

Con esa idea y sin descuidar detalle, el Gobierno Departamental creó El Instituto de Desarrollo Municipal del Huila, asignándole la sigla: "IDEHUILA", presentó a la Asamblea el proyecto de ordenanza, la cual fue aprobada por unanimidad concretándose en la Ordenanza No. 001 del 08 de agosto de 1972, creando un instituto descentralizado de carácter departamental, localizado en la ciudad de Neiva, dotado de personería jurídica, autonomía administrativa y patrimonio propio, adscrito al despacho del gobernador.

Así mismo pensó en la parte económica del nuevo ente, luego entonces cavilando

[3] (Instituto Financiero para el Desarrollo del Huila, s.f.)

en su patrimonio, en el mismo acto administrativo previno el capital del IDEHUILA el cual sería basado por los bienes muebles e inmuebles de propiedad del Departamento, el producto por la venta de algunos de ellos, lo mismo algunas acciones públicas y privadas. Así mismo, y con el fin de proyectar su sostenibilidad financiera la hace partícipe anual de un porcentaje del presupuesto departamental. Para complementar sus ingresos, autoriza recibir donaciones públicas y privadas en aportes y subvenciones de la nación, y aportes de los municipios del Huila, y el producto de las rentas que adquiriría a futuro por razón de la prestación de sus servicios. El instituto para cumplir a cabalidad con los planes y programas que le han sido asignados la ordenanza autoriza al gobernador para que gestione, contrate y reciba un préstamo por valor de $30´000. 000.oo con destino a la capitalización del IDEHUILA.[4]

La ordenanza también previene su estado estructural y funcional y dice que el instituto será dirigido y administrado por una Junta Directiva como su máximo organismo, constituido por 7 miembros (El gobernador quien presidirá la junta, el Secretario de Hacienda, el Jefe de Planeación, tres diputados y el Contralor del Departamento), y por un gerente que será de libre nombramiento y remoción del gobernador, los funcionarios administrativos y operativos los podrá crear la junta cuando los juzgue necesarios, a iniciativa del gerente. De todas maneras su quehacer cotidiano estará direccionado por un reglamento interno que le permita desarrollar su hoja de ruta.[5]

Todo estaba dado para que iniciara sus labores la nueva entidad departamental, entonces, el gobernador Don Héctor Polanía Sánchez, mediante decreto número

[4] (Instituto Financiero para el Desarrollo del Huila, s.f.)

[5] (Instituto Financiero para el Desarrollo del Huila, s.f.)

590 del 3 de Octubre de 1972, encarga de la Gerencia del Instituto de Desarrollo Municipal del Huila (IDEHUILA), al entonces jefe de la Oficina de Planeación doctor JAIRO TORO RODRÍGUEZ, que le daría direccionamiento y fortalecería la base institucional del IDEHUILA. Mediante decreto departamental 188 de 1973 emitido el 4 de Abril, se dicta el Estatuto Orgánico del IDEHUILA, reglamentando la Ordenanza No. 01 del mismo año, en donde reafirma el nombre del instituto recientemente creado, define su objeto, funciones, patrimonio, obligaciones del nuevo ente, el organismo directivo y la secretaría general; el IDEHUILA se reacomoda a los nuevos tiempos, es así como mediante decreto No. 580 del mismo año se hacer reforma al primer decreto en el sentido de hacer unas importantes modificaciones tanto la parte funcional como estructural.[6]

El objeto del "INFIHUILA", Es cooperar en el desarrollo económico, social y cultural, mediante la prestación de servicios de financiación, garantía, acompañamiento empresarial y eventualmente de otros, a favor de proyectos de infraestructura económica y de servicios que se adelanten en los municipios del departamento del Huila y demás departamentos del país, para la creación, fomento y fortalecimiento del sector productivo.[7]

Misión[8]

Somos un instituto de Fomento y Desarrollo, que propende por el mejoramiento económico y social de los municipios del departamento del Huila y demás

[6] (INFIHUILA, s.f.)

[7] (Instituto Financiero para el Desarrollo del Huila, s.f.)

[8] Documento sacado de las políticas del Institutito, la Misión, Visión etc.

Departamentos del país, mediante la presentación de servicios financieros y el acompañamiento al sector productivo.

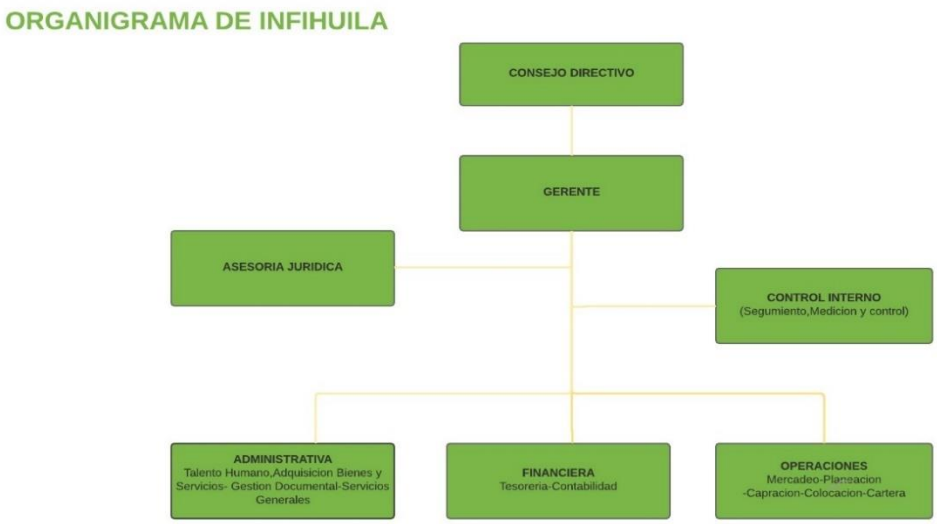
Visión

En el año 2020 seremos reconocidos como el instituto de Fomento y Desarrollo Líder en la prestación de servicios financieros para inversiones públicas y acompañamiento empresarial al sector productivo en el ámbito Nacional.[9]

7.1 EL ORGANIGRAMA ACTUAL DE LA ORGANIZACIÓN ES EL SIGUIENTE:

EL INFIHUILA ha diseñado para la gestión, ejecución y operación de los procesos descritos en el punto precedente, la siguiente Estructura Organizacional

Figura 1 Organigrama Instituto Financiero para el Desarrollo del Huila- INFIHUILA



a,

y

[9] (Instituto Financiero para el Desarrollo del Huila, s.f.)

Control Interno), 4 profesionales universitarios (Tesorería, Contabilidad, Talento Humano, Mercadeo) y 2 auxiliares administrativos (Gestión Documental, Servicios Generales). El recurso humano se encuentra además compuesto por 20 contratistas que prestan sus servicios de apoyo en los diferentes procesos Estratégicos, Misionales y de Apoyo de la entidad.

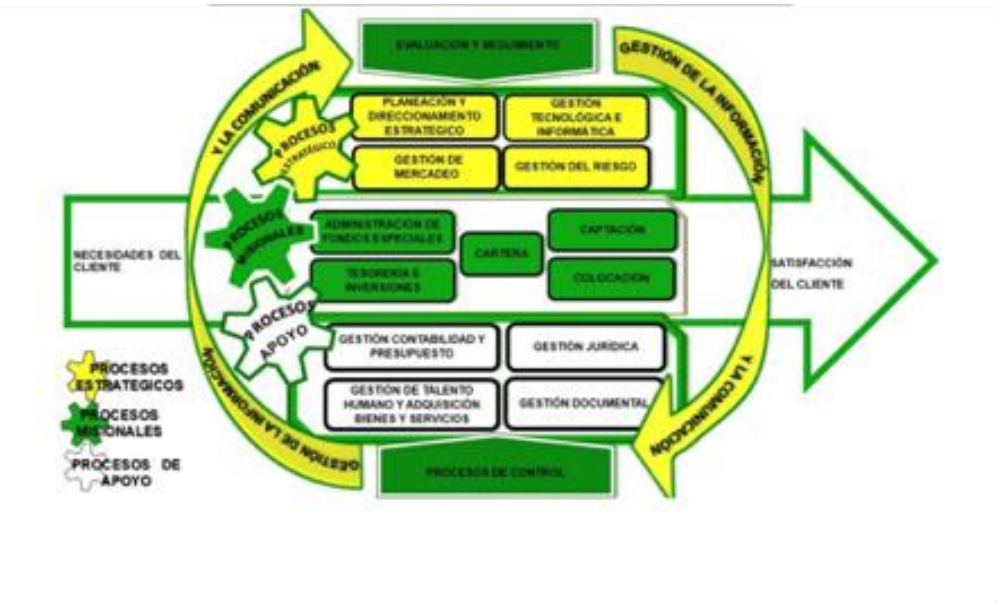
8. MAPA DE PROCESOS

El Mapa de Procesos de EL INFIHUILA refleja la transformación que ha venido desarrollando la Entidad frente a la necesidad de cambio y evolución que demandan los agresivos requerimientos de los entes de control como son Contraloría, Superfinanciera, control interno etc. en productos y/o servicios financieros de calidad y personalizados; situación que obliga a una mejora integral, proactiva y continua, de la Organización como al desarrollo del RRHH adscrito / vinculado a ésta y una labor más incluyente que permita mayor participación del ciudadano. [10]

Producto de lo anterior, el instituto a través de su Manual de Calidad adoptó el siguiente Mapa de Procesos Institucional

[10] (Instituto Financiero para el Desarrollo del Huila, s.f.)

Figura 2 Mapa de Procesos Instituto Financiero para el Desarrollo del Huila- INFIHUILA



8.1 RETOS ACTUALES Y CAMBIOS A FUTURO

El infihuila, al igual que otros institutos financieros territoriales afronta un periodo de transición que empieza en el año 2013 cuando se definen las necesidades de supervisión por parte de esta entidad la súper financiera de Colombia SFC y posteriormente se establecen una serie de requisitos y tiempo para dicha transición a ser entidad Vigilada por la SFC. estos cambios implicaron además (desde el año 2013) que se debía proceder a obtener calificación de riesgo de largo y corto plazo por parte de las firmas calificadoras autorizadas en el país con el fin de poder seguir operando y cumplir los requisitos establecidos con el proceso de transición comentado.

8.2 REQUERIMIENTOS TECNOLOGICOS Y PERATIVOS EXIGIDOS POR LA SUPERFINANCIERA

"Para la realización de las actividades objeto de supervisión los INFIS deben contar con:

*2.9.1. **Una plataforma tecnológica** para su operación, la cual debe estar acordó y con el tamaño de la entidad.*

*2.9.2. La implementación de los **requerimientos mínimos de seguridad y calidad** que le aplican en el manejo de información de las actividades supervisadas.*

*2.9.3. Un **plan de conservación, custodia y seguridad de la información,** tanto documental como electrónica.*

*2.9.4. Un **plan de contingencia y continuidad del negocio** que tenga como finalidad primordial prevenir y solucionar los problemas, fallas e incidentes que se puedan presentar en cualquiera de los sistemas de información que se tengan dispuestos en la operación de las actividades supervisadas, de tal manera que se garantice la realización de las actividades objeto de supervisión.*

*2.9.5. **La descripción de los procesos** para cada una de las actividades objeto de supervisión, con sus respectivos procedimientos y soporte tecnológico.*

*2.9.6. **Mecanismos para la administración del riesgo operativo** a que se exponen las actividades objeto de supervisión, con el fin de gestionarlos y minimizar la probabilidad o impacto en los casos que se materialicen.*

*2.9.7. **La información de aquellas actividades objeto** de supervisión que pretendan ser **contratadas con terceros,** indicando el objeto de la respectiva contratación, los requisitos a exigir a la firma a contratar, el detalle de las funciones que se contratarían externamente, los controles y áreas encargadas del seguimiento a dichos contratos. Esta información debe ser remitida a la SFC con 15 días de antelación al inicio del contrato."*[11]

[11] (SFC, 2014)

9. MARCO TEORICO

El Instituto Financiero para el Desarrollo del Huila “INFIHUILA” es una entidad descentralizada del Departamento del Huila localizado en la ciudad de Neiva, dotado de personería jurídica, autonomía administrativa y patrimonio propio, adscrito al despacho del gobernador.

El Instituto permite identificar las necesidades de inversión de capital fijo de las localidades, que hiciera créditos con garantía para desarrollar proyectos de infraestructura y sobre todo que prestara asistencia técnica y administrativa con el fin de capacitarlos para planear y ejecutar su propio desarrollo.[12]

Las actividades desarrollas por el instituto son:

- Créditos de fomento
- Créditos de tesorería
- Operaciones de sustitución de deuda pública.
- Créditos por la línea de redescuento
- Administración de recursos en depósito
- Administración de recursos por convenio
- Servicios de cooperación y negocios internacionales
- Servicios de investigación, promoción y desarrollo de proyectos
- Factoring con garantía (descuentos de actas y facturas)

[12] (Instituto Financiero para el Desarrollo del Huila, s.f.)

9.1 PORTAFOLIO DE SERVICIOS

ADMINISTRACIÓN DE PAGOS: El Instituto administra dineros con la destinación específica y se compromete a realizar todos los pagos a los proveedores y contratistas. [13]

RECAUDO, ADMINISTRACIÓN Y PAGO: Servicio mediante el cual recaudamos y administramos recursos financieros con una destinación específica y realizamos los pagos en forma eficiente y oportuna, de acuerdo con el mandato del cliente. [14]

9.2 ADMINISTRACIÓN DE RECURSOS PARA PROYECTOS ESPECIALES:

Oferta cuya finalidad es la administración de los recursos financieros; veedurías administrativas; acompañamiento en la ejecución de proyectos (Interventorías) y gerencia de proyectos, entre otros. [15]

[13] (Instituto Financiero para el Desarrollo del Huila, s.f.)

[14] (Instituto Financiero para el Desarrollo del Huila, s.f.)

[15] (Instituto Financiero para el Desarrollo del Huila, s.f.)

10. MARCO LEGAL

A continuación, estas son algunas leyes y normatividad que rigen en Colombia

Decreto 2573 de 2014 Capitulo 2

Es un marco de componentes, instrumentos y responsabilidades para el cumplimiento normativo en los servicios de gestión, seguridad de la información, gobierno en línea. Estrategias que serán desarrolladas y facilitarán en la masificación de oferta y demanda.

Ley 1273 de 2009:

Ley que organiza las violaciones informáticas en Colombia, la cual amplifica dos nuevos capítulos al Código Penal Colombiano:

- Capitulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

- Capitulo Segundo: De los atentados informáticos y otras infracciones. Como se puede ver en el primer capítulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.[16]

[16] (Valencia, s.f.) normatividad dada en Bogotá por el ministerio del Interior.

Ley 603 de 2000:

Esta ley relata la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales. [17]

Por la cual se establecen las prácticas ordinarias del Hábeas Data y se reglamenta la administración de la información comprendida en bases de datos propias, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se decretan otras pericias.

Ley 1273 del 5 de enero del 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. [18]

Ley 527 Ley 527 de 1999 (Comercio electrónico)
Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.[19]

[17] https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

[18] https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

[19] (MINTIC, s.f.)

Decreto 1704 de 2012
Interceptación Legal de comunicaciones [20]

NTC ISO/IEC 27005
catálogo de amenazas y vulnerabilidades

NTC ISO 31000
Gestión del riesgo

NTC 5722
Requisitos para que las empresas implanten, mantengan y mejoren un sistema de gestión de continuidad de negocio.[21]

ISO IEC/27031
Conceptos y principios de la disponibilidad de tecnología de información y comunicación (TIC) para la continuidad del negocio.[22]

ISO IEC/27032
Estandarización de los lineamientos para aplicar y mejorar el estado de ciberseguridad.

ISO IEC/27035
Gestión de incidentes de seguridad de la información.

[20] https://www.mintic.gov.co/portal/604/articles-3559_documento.pdf
[21] (MINTIC, s.f.)
[22] (MINTIC, s.f.)

ISO IEC/27014:2013

conceptos y principios para el gobierno de la seguridad de la información.

Ley 1341 del 30 de julio del 2009:

Por la cual se precisan los manuales y conocimientos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC- se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley 599 de 2000:

Por el cual se expide el Código Penal. En este caso, se mantuvo la estructura del tipo criminal de "infracción de violación ilícita", se hizo el derecho legítimo de los derechos de autor y se consolidaron algunas prácticas de forma indirecta identificadas como violación informática, por ejemplo, oferta, comercio o venta de una propiedad. Instrumento para captar la correspondencia privada entre particulares. El "Acceso dañino a un sistema informático" se resumió, como se persigue: "Art. 195. 195. Cualquier persona que ingrese inapropiadamente a un sistema informático garantizado por un esfuerzo de seguridad o se mantenga en contra del deseo del individuo que tiene el privilegio de rechazarlo. Traerá una multa ".[23]

NORMA ISO/IEC 27001:2013:

[23]http://derechodeautor.gov.co/documents/10181/11769/La+proteccin+del+derecho+de+autor+y+los+derechos+conexos+en+el+ambito+penal+sep+15+de+2010.pdf/75686fc1-c9be-4dc3-b1d5-efcd5f4be949

Es un estándar universal que está conectado para la administración de seguridad de datos. Al tratar con el Sistema de Gestión de Seguridad de la Información (SGSI), el punto es limitar los peligros, por esta razón, se deben desarrollar procedimientos y estrategias para ayudar a la asociación a lograr su brillantez.

DECRETO 052 DE LA SUPERFINANCIERA DE COLOMBIA SFC

Requerimientos SFC para entidades vigiladas en materia tecnológica según circular externa 052 de 2007:

> "2.1.3.2.2. Descripción de la plataforma tecnológica sobre la cual operan las actividades supervisadas, considerando elementos, tales como:
>
> 2.1.3.2.2.1. Equipos centrales.
>
> 2.1.3.2.2.2. Sistemas operativos.
>
> 2.1.3.2.2.3. Sistema de administración de bases de datos.
>
> 2.1.3.2.2.4. Red de comunicaciones.
>
> 2.1.3.2.2.5. Canales mediante los cuales se prestan los servicios, indicando si son propios o se tiene contrato con un tercero.
>
> 2.1.3.2.2.6. Centro de cómputo principal y de contingencia, indicando los controles de seguridad física y de ambiente.
>
> 2.1.3.2.2.7. Controles de seguridad lógica a nivel de sistema operativo y base de datos.
>
> 2.1.3.2.3. Descripción de las aplicaciones que soportan las actividades. supervisadas, indicando el esquema de seguridad de los aplicativos.
>
> 2.1.3.2.4. Plan de conservación, custodia y seguridad de la información tanto documental como electrónica.
>
> 2.1.3.2.5. Estado de la implementación del su numeral 5.2. del Capítulo IV, Título I de la Parte I de esta Circular.
>
> 2.1.3.2.6. Actividades contratadas con terceros, indicando el objeto de la respectiva contratación, los requisitos a exigir a la firma a contratar, el detalle de las funciones que se contraten externamente, los controles y áreas encargadas del seguimiento a dichos contratos.
>
> 2.1.3.2.6. Actividades contratadas con terceros, indicando el objeto de la

respectiva contratación, los requisitos a exigir a la firma a contratar, el detalle de las funciones que se contraten externamente, los controles y áreas encargadas del seguimiento a dichos contratos."[24]

RIESGO DE CIBERSEGURIDAD, SEGURIDAD DE LA INFORMACIÒN, REQUERIMIENTOS MÌNIMOS

"Concepto 2019081599-002 del 26 de julio de 2019 Síntesis: Las entidades vigiladas están obligadas a contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente los riesgos de la seguridad de la información y la ciberseguridad y como mínimo atender las instrucciones contenidas en el Capítulo XXIII de la Circular Básica Contable y Financiera, Capítulo V, Título IV y Capítulo I, Título II de la Parte I de la Circular Básica Jurídica. «(…) comunicación mediante la cual consulta acerca de las medidas de seguridad y obligaciones que deben adoptar los bancos frente a los riesgos presentados en las operaciones realizadas por medio cibernético.[25]

[24] superintendencia financiera de Colombia. Financiera de Colombia. circular externa 034 de 2014.

[25] (Colombia S. d.)Corte Suprema de Justicia, Sala de Casación Civil, mediante la Sentencia C18614-2016 del 19 de diciembre de 2016, con ponencia del Magistrado Dr. Ariel Salazar Ramírez.

11. MARCO CONCEPTUAL

SUPERINTENCIA FINANCIERA DE COLOMBIA (SFC): "La entidad es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y financiera y patrimonio propio".[26]

INFIS: Institutos de fomento y desarrollo Regional, por la cual se determina un régimen especial.

SGSI: para una entidad el diseño, implantación, mantenimiento contiguo de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

ISO 27001: La norma ISO 27001 es una norma internacional que ha sido emitida por la Organización Internacional de Normalización, en la que se describe cómo realizar la gestión de la seguridad de la información en una organización.[27]

SEGURIDAD INFORMATICA: seguridad informática es en sí mismo un concepto amplio y diverso que abarca numerosas derivadas. (...)[28] La seguridad se puede centrar en la prevención de ataques y situaciones de riesgo para los sistemas de una organización o hacerlo más en los mecanismos de mitigación de los efectos

[26] https://www.superfinanciera.gov.co/publicacion/20483

[27] La norma ISO 27001 es una norma internacional que ha sido emitida por la Organización Internacional de Normalización, en la que se describe cómo realizar la gestión de la seguridad de la información en una organización.

[28] ttp://www.iso27000.es/download/doc_sgsi_all.pdf

que un ataque pueda ocasionarle a una empresa o particular

POLITICAS DE SEGURIDAD: son controles que se utilizan para garantizar la intensidad, integridad, disponibilidad a la información de una entidad u organización.

MSPI: El “Instrumento de Evaluación MSPI” Es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente “Seguridad y Privacidad de la Información”.[29]

MAGERIT: es una metodología en la cual está regida bajo las normas ISO27001 en la cual nos proporciona control a los activos de una entidad, y minimiza Riesgos.

KALI LINUX: es un sistema de distribución o sistema operativo Linux con más de 300 herramientas que se utiliza para realizar auditorías, pruebas de instrucción y corregir posibles debilidades que contenga una infraestructura tecnológica.

METASPLOITABLE: es un sistema operativo que nos sirve para realizar pruebas de debilidad en el protocolo de red.

SERVIDORES: es una aplicación capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia

LEY HABES DATA 1581 DEL 2012: Ley para proteger los datos personales de una

[29] www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

persona, el derecho a la intimidad.

NMAP: es una herramienta que se utiliza para escanear puertos y encontrar debilidades en los protocolos de red.

ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

AMENAZAS: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

ANÁLISIS DE RIESGO: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

AUDITORÍA: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria.

AMENAZA: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

AMENAZA EXTERNA: Amenaza que se origina fuera de una organización.

AMENAZA INTERNA: Amenaza que se origina en una organización.

ARQUITECTURA DE SEGURIDAD: Una gran cantidad de reglas que retratan los beneficios de seguridad que debe brindar una entidad para abordar los problemas

de sus clientes, los componentes del sistema son importantes para actualizar dichas administraciones y los grados de ejecución que se requieren en los componentes para gestionar los peligros potenciales.

AUTENTICACIÓN: La garantía de que un intercambio de informática no sea falso. La confirmación en su mayor parte incluye la utilización de una clave secreta, una autenticación, un número de identificación individual u otros datos que se pueden utilizar para aprobar la personalidad o el perfil en una entidad.

12. DISEÑO METODOLOGICO

12.1 METODOLOGÍA DE INVESTIGACIÓN.

Investigación aplicada.

Investigación Aplicada: "Se trata de un tipo de investigación centrada en encontrar mecanismos o estrategias que permitan lograr un objetivo concreto."[30]

Dado el anterior conocimiento el SGSI se desarrollará mediante guías del min tic, circulares de la Superfinanciera Financiera de Colombia.

La metodología investigativa del proyecto aplicado se basara en el Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) con base los lineamientos y las comunicaciones emitidas por la superintendencia financiera de Colombia, según circular Externa 029 de 2014 para el Instituto Financiero para el desarrollo del Huila- INFIHUILA, permitirá que el diseño metodológico logre contar con la estrategia de seguridad de la información que requiere la institución, y generar canales, medios, seguridad y calidad en el manejo de la Información por lo tanto con el fin de alinear estrategias y lograr avances significativos se desarrollará en la siguiente estructura:

[30] https://psicologiaymente.com/miscelanea/tipos-de-investigacion

.

12.2 METODOLOGÍA DE DESARROLLO

Para desarrollar el sistema de Gestión de Seguridad de la Información “SGSI” se toma como desarrollo la **Investigación – acción:** Lomax (1990) define la investigación-acción como *“una intervención en la práctica profesional con la intención de ocasionar una mejora*”.[31] En la cual se tendrá en cuenta el diagnóstico de la institución que busca la mejora continua con implementación de normas y decretos de seguridad que se han desarrollado en el ámbito TIC para conservar la confiabilidad, integridad, y disponibilidad de la información, que busca sensibilizar a los funcionarios, contratistas frente al tema de la seguridad, y minimizar riesgos.

12.3 POBLACIÓN

El presente proyecto aplicado tiene como población a todos los funcionarios y contratistas, proveedores que estén relacionados con el Instituto Financiero Para el desarrollo del Huila -INFIHUILA.

12.4 Muestra

La muestra en la cual se enfocó el proyecto aplicado fue todos los procesos y sus controles que establece el instituto Financiero para el Desarrollo del Huila – INFIHUILA. Para la seguridad de la Información.

[31] Sara Rodríguez García… https://mestrado.prpg.ufg.br/up/97/o/IA._Madrid.pdf

A continuación se relaciona el equipo de sistemas en el Instituto Financiero para el Desarrollo del Huila -**INFIHUILA**:

Tabla 1: Equipo del área de Sistemas -**INFIHUILA**

Tabla 1 ***Integrantes del área de Sistema.***

Nombre y apellido	**Rol**	**Correo**	**Celular**
John Jairo Escobar	coordinador de Seguridad de la Información.	seguridad@infihuila.gov.co	87111168 ext. 113
Diani Lorena Borrero	Profesional de Apoyo	sistemas.tics@infihuila.gov.co	87111168 ext. 113

Fuente: Autor

12.5 Variables

- Gestión: será la aplicada por la Gerencia
- Seguridad: Que los controles implementados en los diferentes procesos cumplan su objetivo de garantizar su confiabilidad e integridad de la información.
- Continuidad: Que el proceso SGSI permita la continuidad de todos los procesos del Instituto.

13. RECOLECCION DE DATOS

13.1 Entrevistas Individuales y/o Colectivas

"*Las entrevistas se utilizan para recabar información en forma verbal*".[32] En la cual se seleccionará un determinado funcionarios u contratistas donde se efectúa intercambio de información cara a cara.

13.2 La Observación.

En esta técnica se observa a funcionarios y contratistas como efectúan sus labores, su integridad y confiabilidad de la información.

13.3 Cuestionario.

En esta técnica se desarrolla preguntas útiles con la cual se conocerá las opiniones y experiencias en los temas de seguridad y controles para salvaguardar las operaciones diarias.

13.4 Pruebas Piloto

Esta prueba se realiza con el fin de identificar vulnerabilidades, y verificar que los controles se estén cumpliendo, mediante técnica Hacking en donde se simulan

[32] https://www.monografias.com/trabajos12/recoldat/recoldat.shtml

diferentes ataques a la infraestructura del instituto Financiero para el Desarrollo del Huila - INFIHUILA.

13.5 Metodología a utilizar del SGSI

"La norma 27001 está diseñada para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información".[33] Por lo tanto se realiza el inventario de activos de información mediante la metodología MAGERET, en la cual se identificará los activos más críticos para que así mismo se minimicen los riesgos y fortalezca la infraestructura.

[33] ICONTEC. Compendio Seguridad de la Información. Técnicas de Seguridad. Editada en 2006-04-03. Colombia, Icontec, marzo de 2013, p. I. ISBN: 978-958-8585-37-6

14. RESULTADOS Y DISCUSION

El proyecto esta direccionado en tres fases con sus entregables de la siguiente manera:

Tabla 2 *Fase 1. de Levantamiento de Información.*

Tabla 2.

Identificación de vulnerabilidades y Gestión del riesgo	Diagnóstico del entorno método observación, entrevistas.
	Prueba e informes ejecutivos de ética a hacking.
	Recomendaciones.

Tabla 3 *Fase 2. Diseño del SGSI, Riesgos, costos*

	canales, medios, seguridad y calidad en el manejo de información para la infraestructura tecnológica del Instituto.
	Gestión de los controles según la norma ISO 27002, riesgos inherentes al

Diseño del Sistema de Gestión de Seguridad de la Información	proyecto -causa y efecto, valor del SGSI.
	Diseñar del sistema gestión seguridad de la información con bases al decreto 034 que exige la superintendencia financiera de Colombia SFC, costo de la implementación, y mejora continua.

Tabla 4 *Fase 3 Sensibilización*

Sensibilización y Asesorías	Revisión de la metodología aplicada para los activos de información, socialización.
	Revisión de las metodologías gestión de la Matriz Activos
	Implementación y Capacitación con respecto a las políticas de seguridad de la información. control de asistencia a la capacitación
	Sensibilizar y concientizar al usuario de la importancia de la seguridad de la

	información para continuo mejoramiento del INFIHUILA. control de asistencia
	Socialización del documento

15. CRONOGRAMA

Tabla 5 *Cronograma*

ACTIVIDAD	M 1	M 2	M 3	M 4	M 5	M 6	M 7	M 8	M 9	M 10	M 11	M 12
Entrega de propuesta de solución seguridad informática	x											
Formulación y planeación del proyecto		x	x	x								
Inicio del Proyecto				x	X	x						
Fase 1	Identificación de vulnerabilidades y gestión del Riesgo											
Diagnóstico del entorno método observación,												

entrevistas.												
Prueba e informes ejecutivos de ética a hacking.							X	x	X			
Recomendaciones.												
Fase 2.	Diseño del sistema de Gestión de seguridad de la información SGSI y Sensibilización											
canales, medios, seguridad y calidad en el manejo de información para la infraestructura tecnológica del Instituto.												
Gestión de los controles según la											x	

norma ISO 27002, riesgos inherentes al proyecto -causa y efecto, valor del SGSI.												
Diseñar del sistema gestión seguridad de la información con bases al decreto 034 que exige la superintendencia financiera de Colombia SFC, costo de la implement											x	

ación, y mejora continua												
Fase 3.												
Revisión de la metodología aplicada para los activos de información, socialización.												
Revisión de las metodologías gestión de la Matriz Activos												
Implementación y Capacitación con respecto a las políticas de												X

seguridad de la información. control de asistencia a la capacitación												
Sensibilizar y concientizar al usuario de la importancia de la seguridad de la información para continuo mejoramiento del INFIHUILA. control de asistencia												

Socialización del documento												

16. IDENTIFICACION DE VULNERABILIDADES

16.1 FASE 1. DIAGNOSTICO INICIAL DE LA INFRAESTRUCTURA TECNOLOGICA DEL INSTITUTO FINANCIERO PARA EL DESARROLLO DEL HUILA- INFIHUILA.

La realización de dicho diagnostico se toma como referencia diferentes tipos o métodos para explorar vulnerabilidades tanto en los procesos como en la infraestructura de soporta los activos y operaciones del instituto. Estas auditorias se realiza con algunos métodos y aplicaciones que son de utilidad a la hora de realizar un análisis a la infraestructura tecnológica del Instituto Financiero para el desarrollo del Huila- INFIHUILA.

Estos métodos o técnicas permitirán ver las debilidades y las diferentes vulnerabilidades con la cual se expone el instituto en la disponibilidad, integridad, accesibilidad a la información del instituto.

Objetivo.
Identificar vulnerabilidades en la infraestructura del Instituto Financiero para el desarrollo del Huila.

Establecer diagnóstico a nivel de procesos estratégicos, misionales y de apoyo de la entidad en relación con el cumplimiento de requerimientos legales, normativos y operativos en materia de infraestructura tecnológica.

18.1.1 Alcance

Esta prueba abarca alcance será todos los procesos del INFIHUILA, pruebas a la aplicación web, red y comunicaciones, sistemas de Información, base de Datos, sistemas operativos.

16.2 RECONOCIMIENTO DEL ENTORNO

El Instituto Financiero para el desarrollo del Huila – INFIHUILA, se ha presentado en dos ocasiones a la Superfinanciera, una en el ano 2014 y otra el ano 2019, donde acontecieron un diagnostico en la cual se debe mejorar en algunos aspectos como los que se muestra la figura No.3 "*Retos del Infihuila Vs Superfinanciera"* mencionan a continuación:

RETOS DE LA SUPERFINANCIERA

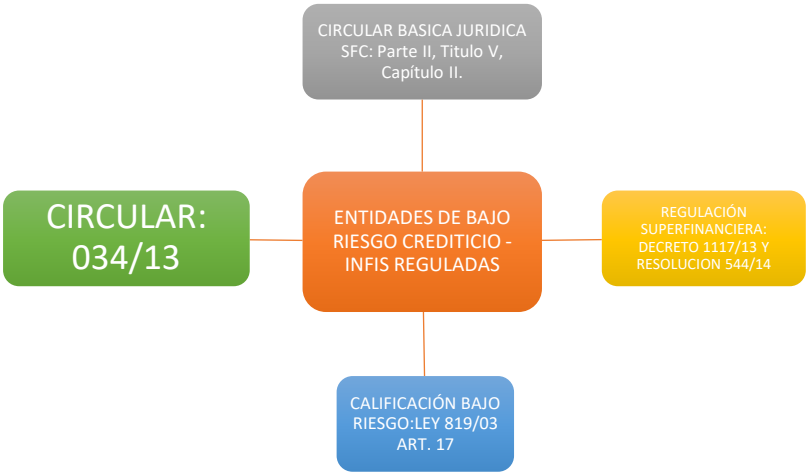


Figura 3 Retos del Infihuila Vs Financiera

La realización de este análisis se basa en las diferentes exigencias de la Superfinanciera de Colombia, sus requerimientos en los diferentes procesos, infraestructura que soporta las operaciones del instituto entre otras.

Es este el proceso donde los Retos se convierten en exigencias como lo indica en la figura No 4 (“*Requerimientos de la Superfinanciera”*) es el detalle de los diferentes requerimientos para que los Infis obtengan su certificación.

16.3 REQUERIMIENTOS DE LA SUPERFINANCIERA

Figura 4 Requerimientos de la Superfinanciera

Durante el desarrollo de las diferentes pruebas realizadas en esta fase del diagnóstico se aplicó el siguiente instrumento para tener una visión general del cumplimiento de los requerimientos exigidos por la superintendencia Financiera de Colombia SFC para la entidad en materia de infraestructura tecnológica:

Ficha Técnica: Escala de valoración mixta cualitativa-cuantitativa. Valoración asimétrica subjetiva con parámetros objetivos de medición. La calificación del cuestionario se explica a continuación:

1. No hay evidencia de cumplimiento (documentación), no hay actividad en desarrollo.
2. No hay evidencia de cumplimiento (documentación), o no hay actividad en desarrollo.
3. Cumple parcialmente las dos (documentación y/o actividad en desarrollo).
4. Hay evidencia de cumplimiento total a nivel de documentación sin evidencia del desarrollo o seguimiento; o hay evidencia del seguimiento y desarrollo sin evidencia documental.
5. Hay evidencia de cumplimiento total (documentación), cumple con el desarrollo esperado y se hace seguimiento.

Tabla 6 *Matriz de evaluación de requerimientos tecnológicos SFC*

ITEMS	Observación	Calificación				
		1	2	3	4	5
Gestionar la seguridad de la información, teniendo referencia el estándar ISO 27001	Observar Plan de Seguridad Informática. Se tiene el documento, pero no se tiene evidencia de seguimiento e implementación. No se trabaja con la ISO 27001 ni se tiene la certificación.		x			
Autenticación	Observar Plan de Seguridad informática. Está implementado en toda la infraestructura y el software				x	
Proveedores de redes y servicios de telecomunicaciones	Se tiene el servicio operando. Existe contrato documentado por un tercero. se tiene un proveedor Movistar cuenta con respaldo de otro operador. ETB					X

Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.	Soporte técnico, mantenimiento preventivo y correctivo, Manejo y conservación de la Información. Se tiene un seguimiento. Se tiene hoja de vida actualizada de los equipos de cómputo. Pendiente procedimientos de Seguridad.			X		
Dotar de seguridad la información confidencial de los dientes que se maneja en los equipos y redes de la entidad.	Se tiene Documento, pero no está ejecutando ni haciendo seguimiento. Observar Plan de Seguridad Informática.		x			
Velar porque la información enviada a los clientes esté libre de software malicioso.	Observar Plan de seguridad Informática. se cuenta con informe del antivirus qué realiza su respectivo mantenimiento.					X
Proteger las claves de acceso a los sistemas de información	Observar Plan de seguridad Informática. El Servidor cuenta con protección de información, cuenta con informe de seguimiento. Los computadores personales su seguridad depende de la persona			X		

Dotación a los terminales, equipos de cómputo y redes locales de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones	Se tiene instalada servicio de Directorio Activo el cual no permite que los usuarios instalen programas o dispositivos que capturen contraseña.					X
Ofrecer la posibilidad de manejar contraseñas diferentes para los instrumentos o canales, en caso de que éstos lo requieran y/o lo permitan.	Observar Plan de seguridad Informática. El Servidor cuenta con protección de información, no cuenta con informe de seguimiento. Los computadores personales su seguridad depende de la persona encargada, no se lleva seguimiento al personal.		x			
Establecer los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo sólo pueda ser realizado por personal debidamente autorizado	Se tiene implementación de la instalación del Servicio de directorio Activo. Solo lo puede realizar el personal del área de Sistemas					X
Tener en operación sólo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para el desarrollo de su actividad	Observar plan de Seguridad Informática. Se tiene documentado en las políticas y en la configuración de las aplicaciones.					X

Cuando a través de los distintos canales se pidan y se realicen donaciones, se debe generar y entregar un soporte incluyendo el valor de la donación y el nombre del beneficiario.	No se cuenta con procedimientos, pero si cuentan con una documentación para la realización de donaciones.			X		
Conservar todos los soportes y documentos donde se hayan establecido los compromisos, tanto de las entidades como de sus clientes y las condiciones bajo las cuales éstas prestan sus servicios.	Se tiene implementado un área de Riesgo donde se creó un documento de confiabilidad y privacidad de la información.					X
Llevar un registro de las consultas realizadas por los funcionarios de la entidad sobre la información confidencial de los clientes, que contenga al menos lo siguiente: identificación del funcionario que realizó la consulta, canal utilizado, identificación del equipo, fecha y hora.	No se tiene documentación e implementación de consultas realizadas por cada funcionario	X				
Dejar constancia del cumplimiento de la obligación de informar adecuadamente a los clientes respecto de las medidas de seguridad que deben tener en cuenta para la realización de operaciones por cada canal, así como los procedimientos para el bloqueo, inactivación, reactivación.	Ver solicitud cuenta usuario. Se hace seguimiento, pero no está documentado			X		

Grabar las llamadas realizadas por los clientes a los centros de atención telefónica cuando consulten o actualicen su información.	No se cuenta con grabaciones de llamadas realizadas a los clientes	X				
Los sistemas informáticos empleados para la prestación de servicios en las oficinas deben contar con soporte por parte del fabricante	Los sistemas informáticos cuentan con la estructura de arrendamiento leasing, la cual con soporte en las aplicaciones y sistema financiero por 3 años.					x
Contar con cámaras de video, las cuales deben cubrir al menos el acceso principal y las áreas de atención al público. Las imágenes deben ser conservadas por lo menos 8 meses o en el caso en que la margen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial.	Ver Plan de Seguridad Informática. Cuentan con cámaras de videos, las imágenes son conservadas por 45 días.			X		
Disponer de los mecanismos necesarios para evitar que personas no autorizadas atiendan a los clientes o usuarios en nombre de la entidad.	Observar Plan de Seguridad informática. Está implementado la autenticación en los computadores personales y el software cuenta con esta implementación.				x	

La información que viaja entre las oficinas y los sitios centrales de las entidades debe estar cifrada usando hardware de propósito específico, o software, o una combinación de los anteriores.	No se cuenta con la implementación y documentación de cifrado de información.	X				
Receptores de dinero en efectivo	La entidad no es receptora de dinero En efectivo	N/A				
Centro de atención telefónica (Cal Center, Contacto Center)	No se cuenta con Cal Center en la entidad	N/A				
Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.	No se cuenta con la implementación de los diferentes procedimientos de hardware o software al ingreso de dispositivos.	X				
Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura.	Se encuentra implementada algunos algoritmos y protocolos para una comunicación segura. Pero No se cuenta con la documentación	x				
Realizar como mínimo 2 veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de operaciones monetarias por este canal.	No cuenta con registro de prueba de vulnerabilidad, ni existe roles especificados ni personal contratado con estos temas.	x				

Implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (links) de su sitio web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.	No cuenta con procedimiento e implementación de modificación de enlaces de la página web.	x				
Contar con mecanismos para incrementar la seguridad de los portales, protegiéndolos de ataques de negación de servicio, inyección de código u objetos maliciosos, que afecten la seguridad de la operación o su conclusión exitosa.	Se cuenta con la implementación en el firewall, consola de Antivirus. Y documentación de Fortinet					x
Banca Móvil	No se cuenta con la implementación de la banca móvil por parte del proveedor.	x				

Al analizar los diferentes requerimientos que exige la SFC con el Instituto se describe como lo indica la figura 5 donde se aprecia de valoración mixta cualitativa y cuantitativa así:

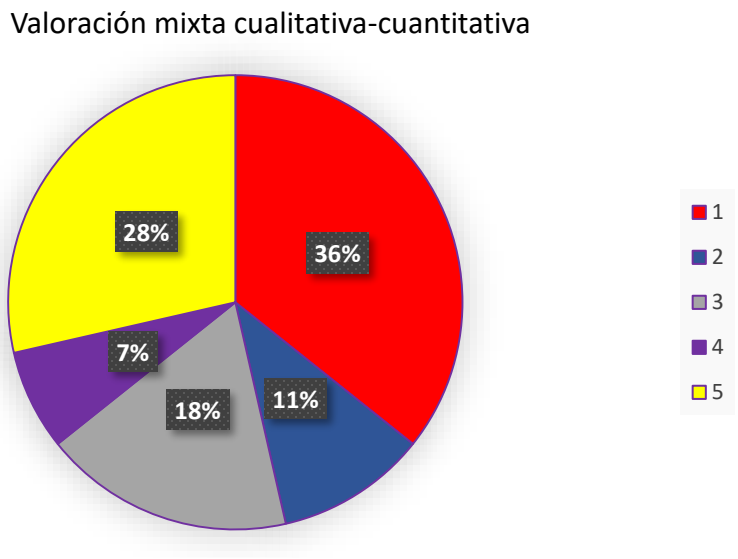


Figura 5 valoración mixta cualitativa-cuantitativa
Fuente Propia

la calificación de los requerimientos de la SFC en materia de Tecnología, para el caso del INFIHUILA tenemos el 36% en el nivel más bajo de calificación en el cual no hay evidencia de documentación con descripción del proceso ni hay evidencia de cumplimiento, ejecución y/o desarrollo.

un 11% con el segundo nivel más bajo de calificación en donde hay desarrollo documental parcial sin evidencia de desarrollo o seguimiento. Tomando estos dos niveles como los no aceptables para una entidad financiera o vigilada por la SFC vemos que en total tenemos un 47% de atributos en estado bajo de cumplimiento.

Al revisar los atributos en nivel tres tenemos un 18% con documentación, evidencia de desarrollo y seguimiento parcial. Esta categoría la denominaríamos aceptable y se requieren acciones para mejorar y da r cumplimiento de alto desempeño.

En las categorías más altas de cumplimiento del atributo tenemos solo el 7% en nivel cuatro y 28% en nivel 5 lo cual refleja el mejoramiento continuo de la infraestructura tecnológica según los requerimientos de SFC.

16.4 Diseño de la Infraestructura Tecnológica

El diseño tecnológico del Instituto cuenta con infraestructura robusta conformada por 4 servidores 3 de Leasing y 1 activo de la entidad en la que esta configura como el servicio de Directorio Activo, cuenta con servidor de Aplicaciones, servidor para alojamiento de la base de datos Virtual, y cuenta con otro servidor de copias, servidor de solo Backus de los equipos, base de datos e información general de las diferentes aplicaciones que se utilizan en el Institutito.

Aparte de esto cuenta con 32 equipos leasing marca HP, cortafuego Firewall Fortinet, y dos redes de comunicación alternas que trabajan en igualdad en caso de una llegue a fallar, como se interpreta con la siguiente figura:

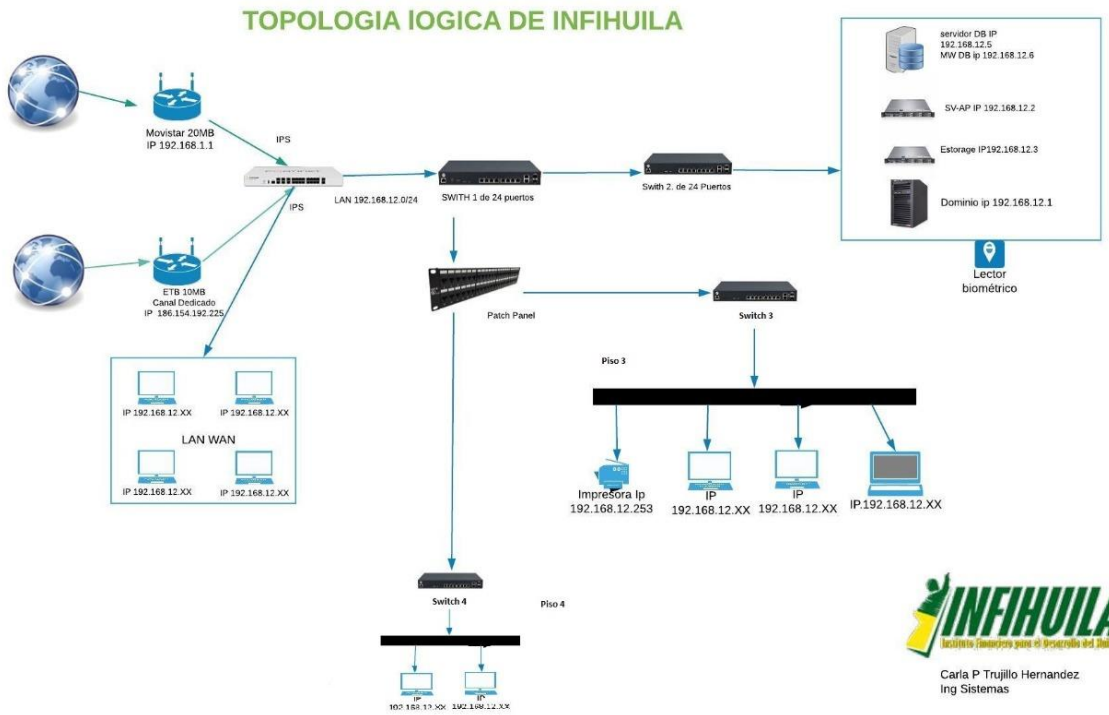


Figura 6 Topología de Infihuila

Hallazgos y Debilidades a nivel organizacional.

Se requiere que el sistema parametrice la Matriz de riesgo el cual se realiza y se consolida en Excel.

Se siguiere que el sistema tenga una alerta temprana para mitigación del riesgo, en cuanto a límites en contratación, personal de crédito, entre otros.

Hallazgos y Debilidades de la Infraestructura Tecnológica.

Realizando el análisis con entrevista, observación la institución cuenta con las siguientes vulnerabilidades:

A Nivel organización no se encuentra diseñada con los procesos tic alineados a seguridad y ciberseguridad.

Existe un nivel de rechazo y desconfianza ante el proveedor tecnológico.

A nivel Hardware, sus equipos son de arrendamiento leasing, en las cuales presentan muchas quejas y fallas en la operación de sus funciones.

cuenta con Data center regulado por la norma, en la cual sus observaciones son mínimas como es hecho de tener el biométrico en funcionamiento, cuenta con dos gabinetes identificados una para redes y el otro para servidores, control de temperatura, aire acondicionado en buen funcionamiento.

A nivel software: cuenta con sistema financiero estable e integro, pero aun así las fallas persisten en los resultados. Y en los demás entes de control sus informes lo presentan de forma manual, esto les genera desgaste en sus obligaciones.

El sistema de auditoria no registra al detalle todas las operaciones realizadas en el sistema.

En el módulo de activos se encuentran diferencias con el físico y el sistema.

Los formatos que maneja el área son Contaduría General "Chip", Exógena, Contraloría Departamental (Presupuesto y Gastos), que se encuentran integrados en el sistema, pero al momento de generarlos se presentan inconsistencias en cuanto saldos de cuentas.

Se requiere un software en el que se incluyan las actividades de cada proceso para hacer indicadores de gestión y tablero de indicadores de riesgos para realizar seguimiento.

No hay modulo para la gestión de manejo de riesgo para monitorear la brecha de liquidez límites para manejar los bancos, concentración y lo estipulado en los manuales SARL - SARM, se deben analizar los datos de forma manual para darle cumplimiento a los manuales, esta es una actividad.

A nivel de Redes: cuenta con un cableado estructurado categoría 6ª, puntos certificados y documentados. Pero el sistema de etiqueta y diseño los puntos no coinciden.

A nivel de Seguridad, el instituto no cuenta con un sistema de Gestión de Seguridad de la Información, las políticas están implementadas, documentadas, pero aún no son socializadas al resto de usuarios.

Se han desarrollado pruebas de estrés de dos niveles, una local y el otro nivel nacional donde la norma indica que el centro alterno debe estar mínimo a 500km esto ha tomado como referencia la ciudad de Bogotá donde se adelantó un simulacro con un servidor Cloud,

Aunque este proceso forma parte de los requisitos exigidos por la Superfinanciera de Colombia la circular 5 hace referencia a diferencias contingencias, en las cuales argumenta que la entidad debe contar con una base de datos alterna, que en debido momento no llegase a tener contacto con el proveedor principal tener una segunda

opción y que la productividad de operaciones sea constante, y esta situación aún sigue latente sin definir.

Otro tema que persiste es definición de roles y obligaciones se tiene contratada una persona para seguridad, pero no tiene obligaciones que se asimilen a estos temas en su mayoría.

Este método proporciona una gran cantidad de comando útiles para ***Prueba ética Hacking***

Una vez recopilada información a nivel de entorno mediante entrevistas, observaciones llegamos al nivel de la prueba de vulnerabilidades, prueba ética hacking a través diferentes métodos en este caso se utilizará la metodología CEH (Certified Ethical Hacker) con el método Nmap.

Nmap: es una herramienta de escaneo de redes que permite identificar qué servicios se están ejecutando en un dispositivo remoto, así como la identificación de equipos activos, sistemas operativos en el equipo remoto, existencia de filtros o firewalls, entre otros.[34]

Para elaborar las diferentes tentativas de Ética Hacking un proceso complicado se realizó un orden específico el análisis de identificación de vulnerabilidades y los diferentes daños que podría causar un atacante.

Para empezar, comenzamos escaneando la red con el siguiente comando.

[34] (Universidad Nacional autonoma de Mexico, s.f.)

- Nmap 192.168.XX.XX

Nota se mantiene en incógnita las direcciones IP ya que son de índole confidenciales para salvaguardar información.
tomar ventaja frente a las diferentes vulnerabilidades que pueda presentar en la infraestructura.

Como, por ejemplo:

- **Auth:** ejecuta todos sus *scripts* disponibles para autenticación
- **Default:** ejecuta los *scripts* básicos por defecto de la herramienta
- **Discovery:** recupera información del *target* o víctima
- **External:** *script* para utilizar recursos externos
- **Intrusive:** utiliza *scripts* que son considerados intrusivos para la víctima o *target*
- **Malware:** revisa si hay conexiones abiertas por códigos maliciosos o *backlogs* (puertas traseras)
- **Safe:** ejecuta *scripts* que no son intrusivos
- **Vuln:** descubre las vulnerabilidades más conocidas
- **All:** ejecuta absolutamente todos los *scripts* con extensión NSE disponibles.[35]

[35] (Pérez, 2015)

17. PRESENTACIÓN DE INFORME EJECUTIVO PRUEBA INTRUSION

Actividades

La ejecución de este nivel de prueba se llevaron a cabo diferentes pasos en los que se analiza, documenta e informa el estado de estructura tecnológica con sus nuevas tecnologías.

Este informe estará compuesto por:

Objetivo

Realizar un análisis con pruebas que tiene como fin la precepción, comprobación de la fortaleza o debilidad con la cuenta la infraestructura tecnológica del INFIHUILA. mediante la instrucción de métodos hacking y así fortalecer sus debilidades.

Operaciones realizadas

Se realizan las siguientes operaciones

Escaneo de puertos abiertos.
Escaneo de sistemas operativos.
Escaneo de host activos.

Ubicación

El sitio destinado para realizar las pruebas de penetración es de forma interna y externa.

Descripción

El proceso de la prueba de ética hacking se utilizará la herramienta Nmap en la cual a través de comandos y su objetivo, nos dará como resultado que tipos de puertos están abiertos, sistemas operativos entre otros.

Herramienta Utilizada
Nombre: Nmap
Fabricante: libre

Evidencias Mas Representativas

Continuando con la diligencia de la prueba se procedió a realizar el análisis en la cual se detallan a continuación.

1. En el análisis de la información se utilizó el comando

Escaneando la red interna.

- Nmap 192.168.12.0/24

Nota: las IP relacionadas se dejan con una XX para garantizar la confiabilidad de la entidad.

Reporta lo siguiente:

192.168.XX.XX

53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn

389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-pc-epmap
636/tcp open ldapssl
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
3389/tcp open ms-web-server
MAC Address: 00:0C:29: E9:51:4F

192.168.XX.XX

80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
2638/tcp open Sybase
3306/tcp open MySQL
3389/tcp open ms-web-server
5357/tcp open wsdapi
14000/tcp open scotty-ft
MAC Address: 70:10:6F:C8:84: 7ª
Microsoft Windows 2016

Escaneando Red externa.

PUERTOS ABIERTOS	**SISTEMA OPERATIVO**	**HOST**	**DOMINIO**	**IP**
135; 139;445; 2000; 5060:5357	Microsoft Windows 7 - 10 microsoft-ds	IN-CONTAB02	INFIHUILA-ID	**192.168. XX. XX**
	)	HP LaserJet printer http	INFIHUILA-ID	**192.168.XX.X X**
23;2000;5060	ZKSoftware ZEM560 access control device (Linux 2.6.24; MIPS		INFIHUILA-ID	**192.168.XX. XX 192.168.XX.X X**
	CISCO			**192.168.XX .XX**
23; 80;2000; 5060	HP MSM Controller or 1920-series switch			**192.168. XX. XX**
135; 139;445;2000; 3389; 5060:5357	Microsoft Windows 7 - 10 microsoft-ds	IN-CONTINTER-02	INFIHUILA-ID	**192.168. XX. XX**
135; 139;445;554;2000; 2869;2968;33	Microsoft Windows 7 - 10 microsoft-ds	GERENCIA-PC	WORKGROUP)	**192.168. XX. XX**

89; 5060:5357;10243;49152;49153;49154; 49155; 49156; 49157; 49159				
135; 139;445;2000; 5060;5357	Microsoft Windows 7 - 10 Microsoft-	IN-RIESGOS-02	INFIHUILA-ID	**192.168. XX. XX**
22;111;1521;2000;5060;5500	Oracle TNS listener 12.1.0.1.0	Oracle XML DB Enterprise Edición HTTP	INFIHUILA-ID	**192.168. XX. XX**
22;80;427; 443;902; 2000;5060;5989;8000;8100; 8300	VMware Autenticación Daemon 1.10	srv-virtual1.infihuila. local	INFIHUILA-ID	**192.168.XX.XX**
80/427/ 443/902/2000/ 5060/5989/8000/8100/8300		srv-virtual2.infihuila. local	INFIHUILA-ID	**192.168.XX.XX**
80/ 111/ 135/139/445/ 515/ 2000/2049/2301/2381/3260 /3389/5060 /49152/49153/	Microsoft Windows Server 2008 R2 - 2012	SRV-STORAGE	INFIHUILA-ID	**192.168.XX.XX**

49154/49155/ 49157/49176				
80/135/139 / 443/ 445/2638/ 3306/ 3389/5060/ 5357/14000	Windows Server 2008 R2 – 2012	Microsoft Windows Server 2008 R2	INFIHUILA-ID	**192.168.XX.XX**
53;464;636 ;2000;3269;50 60	SRV-DC	Active Directory	infihuila-id.local	**192.168.XX.XX**

ANALISIS DE VULNERABILIDADES

Para dicha prueba de instrucción se realiza con el método de Nmap ya que es una herramienta potente y gratuita nos proporciona herramientas y scripts para que se realicen diferentes auditorias.

Entre estas, se selecciona una más para detectar vulnerabilidades de la muestra de IP'S detectadas con puertos abiertos y se ejecuta el comando

Este comando permitirá analizar 1000 puertos abiertos, e intentara realizar su análisis con las vulnerabilidades más conocidas como son ataque DoS, o "*CSRF (Cross Site Request Forgery)"*.[36]

Las IP fueron la siguientes:

-Servidores

-Algunos equipos.

root@kali:~# nmap -f --script vuln **192.168.XX.XX** --Sistemas

Starting Nmap 7.70 (https://nmap.org) at 2019-11-28 12:11 EST

Pre-scan script results:

| broadcast-avahi-dos:

| Discovered hosts:

| 224.0.0.251

| After NULL UDP avahi packet DoS (CVE-2011-1002).

|_ Hosts are all up (not vulnerable).

Nmap scan report for 192.168.12.153

Host is up (0.0039s latency).

All 1000 scanned ports on 192.168.12.153 are filtered

MAC Address: E8: XX:XX:XX:XX:XX (Hewlett Packard)

root@kali:~# nmap -f --script vuln **192.168.XX.XX**

Starting Nmap 7.70 (https://nmap.org) at 2019-11-28 12:12 EST

Pre-scan script results:

| broadcast-avahi-dos:

| Discovered hosts:

| 224.0.0.251

---

[36] **Fuente especificada no válida.**

| After NULL UDP avahi packet DoS (CVE-2011-1002).

|_ Hosts are all up (not vulnerable).

Nmap scan report for **192.168.XX.XX →Dominio**

Host is up (0.0013s latency).

All 1000 scanned ports on **192.168.XX.XX** are filtered

MAC Address: 00: XX:XX:XX:XX:XX (VMware)

Nmap done: 1 IP address (1 host up) scanned in 56.75 seconds

root@kali:~# nmap -f --script vuln **192.168.XX.XX Servidor Aplicaciones**

Starting Nmap 7.70 (https://nmap.org) at 2019-11-28 12:13 EST

Pre-scan script results:

| broadcast-avahi-dos:

| Discovered hosts:

| 224.0.0.251

| After NULL UDP avahi packet DoS (CVE-2011-1002).

|_ Hosts are all up (not vulnerable).

Nmap scan report for 192.168.12.2

Host is up (0.0057s latency).

All 1000 scanned ports on **192.168.XX.XX** are filtered

MAC Address: 70: XX:XX:XX:XX:XX (Hewlett Packard Enterprise)

Nmap done: 1 IP address (1 host up) scanned in 56.80 seconds

root@kali:~# nmap -f --script vuln **192.168.XX.XX servidor de Copias**

Starting Nmap 7.70 (https://nmap.org) at 2019-11-28 12:14 EST

Pre-scan script results:

| broadcast-avahi-dos:

| Discovered hosts:

| 224.0.0.251

| After NULL UDP avahi packet DoS (CVE-2011-1002).

|_ Hosts are all up (not vulnerable).

Nmap scan report for **192.168.XX.XX**

Host is up (0.018s latency).

All 1000 scanned ports on 192.168.12.3 are filtered

MAC Address: 70: XX:XX:XX:XX:XX (Hewlett Packard Enterprise)

Nmap done: 1 IP address (1 host up) scanned in 56.76 seconds

root@kali:~# nmap -f --script vuln **192.168.XX.XX → Servidor base Datos**

Starting Nmap 7.70 (https://nmap.org) at 2019-11-28 12:15 EST

Pre-scan script results:

| broadcast-avahi-dos:

| Discovered hosts:

| 224.0.0.251

| After NULL UDP avahi packet DoS (CVE-2011-1002).

|_ Hosts are all up (not vulnerable).

Nmap scan report for 192.168.12.6

Host is up (0.0015s latency).

All 1000 scanned ports on 192.168.12.6 are filtered

MAC Address: 00:XX:XX:XX:XX:XX (VMware)

Nmap done: 1 IP address (1 host up) scanned in 56.75 seconds

Análisis de resultados

En el análisis de datos se encontraron 26 host o computadoras activas.

Dominio INDIHUILA-ID

Servidores 4

Sistemas operativos: Windows 7 actualizados a versión Windows 10, Linux

Impresoras

Base de Datos: Oracle

Se detecta que la infraestructura esta fortalecita en temas de seguridad, la tecnología, con sistema Fortegate, sus políticas, están bien definidas permiten el bloqueo de intrusos con defensa web, ID, que hacen que la red este más segura a la hora de enfrentarse a posibles ataques.

CONCLUSIONES

El término de la siguiente diligencia se llega a emitir lo siguiente:

Las pruebas realizadas son de gran Utilidad ya que estas permiten tener alertas tempranas para minimizar riesgos y fortalecer la infraestructura de amenazas futuras que puedan tentar contra la integridad, accesibilidad y confiabilidad de los activos importantes para el instituto.

RECOMENDACIONES

- Se recomienda realizar pruebas de intrusión de forma periódica.
- Monitorear aplicaciones para el buen funcionamiento.
- Capacitar y concientizar al usuario de los temas de seguridad.

Desde el componente Organizacional

Ajustar el Plan Estratégico de la Organización redefiniendo el rol del Proceso TIC y establecer líneas de política y ejes estratégicos claros y acorde a requerimientos actuales y de futuro.

Rediseñar el Proceso de Gestión Tecnológica y definir roles y responsabilidades no solo del área TIC sino de las dependencias que interactúan.

Desde el componente Infraestructura Tecnológica

Hardware

Se debe contar con equipos de contingencia como computadores, portátiles, impresoras y escáner.

Se debe contar con un contrato y presupuesto para las diferentes novedades que puedan suceder en temas de tecnología, como mantenimientos de impresoras, redes, servidores etc.

Software

Se debe contar o permitir la integración con un software de cuadro de Mando o Balance Score Card que permita a la gerencia y líderes de área contar con indicadores de todos los procesos de la entidad, brindando una visión clara del avance de las estrategias de la organización y facilitando la toma de decisiones a nivel gerencial.

Se debe contar o permitir la integración con un sistema de gestión documental que permita un control total en el ciclo de vida de los documentos que se producen o gestionan al interior de la entidad, de manera que la entidad acceder a los documentos de forma ágil para la ejecución de sus procesos diarios y con controles

de nivel de acceso que permita llegar un registro detallado de las acciones realizadas por los usuarios, además de conservar el patrimonio histórico documental del INFIHUILA.

Se recomienda llevar a cabo un proceso intensivo de apropiación del sistema, que todos los funcionarios contratistas tengan la capacidad de utilizarlo correctamente, esto se puede realizar mediante jornadas de capacitación.

18. FASE 2 DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para esta fase este nivel hace referenciar a la "*Parte I, Título II, Capítulo I "Canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros", de la Circular Básica Jurídica (Circular Externa 29 de 2014)"*[37] toda entidad que quiere ser vigilada debe definir como requerimiento mínimo los canales, medios, seguridad, y calidad en el manejo de la información del instituto Financiero para el Desarrollo del Huila - INFIHUILA.

18.1 CANALES DE PRESTACION DE SERVICIO.

Oficinas

Para mantener una buena comunicación la entidad debe saber cuáles son las canales apropiadas para brindar información de manera segura y eficaz al cliente.

El instituto maneja diversos canales comunicación entre estos tenemos los formales y los informales, los formales para transmitir información oficial están determinados la cuales son Comunicados, Circulares, ordenanzas, memorandos entre otras.

Las informales se tienen determinadas como conversaciones y rumores.

El Instituto Financiero para el Desarrollo del Huila – Infihuila cuenta con una oficina principal en la ciudad de Neiva con el servicio de:

[37] (Colombia s. F., s.f.)documento tomado directamente de la página oficial super financiera de Colombia.

horario de lunes a viernes de 7:30 a 12:00pm y de 2:30pm a 6:00pm en la cliente podrá a través de los diferentes canales mencionados anteriormente. Realizar lo siguiente:

- Realizar solicitudes de Crédito
- Consultar saldos de las obligaciones
- Consultar movimientos de las cuentas de depósito.
- Solicitar paz y salvo de los productos relacionados con el portafolio de servicios.
- Solicitar certificados Laborales
- Solicitar extractos bancarios.
- Solicitar asesorías en temas del institucionales entre otras.

los medios que se utilizan para transmitir la información de forma segura se tienen los siguientes:

Escritos: a través de comunicados, oficios, procedimientos, protocolos, noticias entre otras. Las cuales son de gran importancia ya que permanece la evidencia.
Orales: son las realizadas a través de comités, conferencias, capacitaciones etc.
Tecnológicos: tenemos la fusión de los dos anteriores Ítems, como son escritos digitales, .pdf, las imágenes para publicar con extensión .jpg. Y para ámbitos digitales las imágenes con extensión png, entre otras está definido el correo institucional, blogs del instituto.

Oficinas locales

El instituto financiero para el desarrollo del Huila -INFIHUILA tiene a su vez 3 sucursales u oficinas en los municipios Garzón, Pitalito y la plata la cual están son atendidas por 1 funcionario en cada una de ellas y están en la facultad de atender

los diferentes canales suscritos a la entidad como se relacionan anteriormente. Y en el mismo horario.

otros canales e instrumentos, mecanismos de prestación de servicios

Otro de los canales de servicio se tiene:
Línea se Servicio al ciudadano
El instituto financiero para el Desarrollo del Huila-INFIHUILA tiene destinado las siguientes líneas

- 8711168,- 8711168-8711169-8711234
- Cel: 314 2932941.

Canales de comunicación Virtual

- www.infihuila.gov.co

- Chat en Línea, comentarios

- Preguntas, quejas, reclamos y denuncias (PQRSD) formulario web.

-Contáctenos (https://www.infihuila.gov.co/contacto.html)

Correo Electrónico:

-Correo Institucional - contacto@infihuila.gov.co

-Notificaciones judiciales - notificacionesjudiciales@infihuila.gov.co

Otros mecanismos son:

AUDIENCIAS PUBLICAS

Diálogos en los cuales, se discutirán aspectos relacionados con la estructuración, ejecución o evaluación de políticas y programas a cargo de la entidad, y en especial cuando esté de por medio la afectación de derechos o intereses colectivos.

AUDICION PUBLICA DE RENDICION DE CUENTAS

Espacios para fortalecer los mecanismos de rendición de cuentas, promoviendo el diálogo continuo con los grupos de interés, e informando sobre los resultados de la gestión de un período.

RENDICION DE CUENTAS

El deber que tienen las autoridades de la administración pública de responder públicamente, ante las exigencias que haga la ciudadanía, por el manejo de los recursos, las decisiones y la gestión realizada en el ejercicio del poder que les ha sido delegado.

VEEDURIA CIUDADANA

Mecanismo democrático de representación que le permite a los ciudadanos o a las diferentes organizaciones comunitarias, ejercer vigilancia sobre la gestión pública, respecto a las autoridades, administrativas, políticas, judiciales, electorales, legislativas y órganos de control, así como de las entidades públicas o privadas[38]

uso de redes

[38] (INFIHUILA, s.f.)

- YouTube: Infihuila
- Twitter: @infihuila
- Facebook: infihuila

18.2 SEGURIDAD Y CALIDAD PARA LA REALIZACION DE OPERACIONES

Alcance

El instituto Financiero para el desarrollo del Huila -INFIHUILA tiene como alcance todos los procesos. desde Front donde llega el cliente hasta el resguardo de Información, de forma segura.

La entidad cuenta con un formato u oficio que le asegura el cliente que toda información adquirida es para un bien común. La entidad clasifica la información como confidencial en el caso que sea necesario y lo implementa con el procedimiento de etiquetación de activos de datos.

definiciones aplicables

Autenticación:

"*Conjunto de técnicas y procedimientos utilizados para verificar la identidad de un cliente, entidad o usuario, así como la facultad del cliente o usuario para realizar operaciones*".[39]

[39] Parte I-Titulo II – Capítulo I Circular externa 008 de 2009

EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila cuenta con procedimientos de ingresos al sistema financiero, computadores, acceso físico teniendo como referente la norma ISO 27002 la utilización de controles para el manejo de información.

EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila cuenta el servicio de directorio Activo para cada usuario con un perfil determinado, cuenta con servio de Antivirus en cada uno de sus equipos que es el que examina todo ingreso y descarga de internet este verifique si está libre de amenazas.

El instituto financiero trabaja con la tecnología Fortegate, que asegura que no haya intrusos en la red y cliente pueda estar seguro de que la transacción que se va a realizar sea de forma segura, que al igual que otras aplicaciones manesa sistema de autenticación.

EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila cuenta con el procedimiento de baja de un usuario cuando este ya no pertenece a la entidad con la técnica de eliminación que se hace desde el mismo software financiero terminando hasta le des habilitación de la cuenta de dominio.

EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila Cifrado fuerte implementado en el manual de políticas y con la técnica del servicio de directorio Activo entre otras.

EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila cuenta con el mecanismo de biometría que permite solo el acceso a personal autorizado tanto en el Data Center como el ingreso a las oficinas donde se maneja información sensible.

EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila cuenta con certificados de Firma por la entidad Certifirma es la que permite controlar la elaboración de información confidencial como son los bonos pensionales con el mecanismo del token.

EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila para aseguras sus operaciones cuenta con tokens de los diferentes bancos, ir fija, antivirus tanto del banco externo como del instituto para realizar transacciones electrónicas seguras.

Proveedores de redes y servicios de telecomunicaciones

EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila cuenta para el desarrollo de sus operaciones dos canales de Internet, uno contingencia del otro, un canal dedicado de 10MG y otro con Movistar de 20MG cada uno maneja sus sistemas de seguridad con sistema operativo y antivirus para minimizar riesgos, todo este servicio es suministrado por el proveedor de comunicaciones.

Criterios

seguridad de la información

- Confidencialidad: Hace referencia a la protección de información cuya divulgación no está autorizada.
- Integridad: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

- Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

Respecto de la calidad de la información

- Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.

- Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.

- Confiabilidad: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones

Teniendo en cuenta los siguientes criterios **EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila** cuenta con procedimientos y controles en los diferentes equipos y las diferentes aplicaciones (Software), estos equipos manejan sistemas operativos licenciados que son actualizados frecuentemente para minimizar amenazas esta seguridad permite cumplir exitosamente los criterios mencionados antes, para el cumplimiento de sus operaciones diarias.

EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila, para él envió de información cuenta con dominio propio infihuila.gov.co, correos instituciones, que se maneja a través de un tercero con seguridad en sus certificados y URL seguras.

EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila, cuenta con la política, procedimiento de claves seguras y con el mecanismo del servicio de

Directorio Activo en la que se implementa contraseñas robustas y el mantenimiento de ellas cada 45 días, y socialización de estas a los usuarios una vez que sean entregadas.

EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila, cuenta con consola de Antivirus donde se actualiza, informa y genera los diferentes informes que maquinas presentan vulnerabilidades o que están contaminadas, con alertas tempranas para minimizar amenazas.

EL INSTITUTO Financiero para el Desarrollo del Huila -Infihuila, cuenta en cada terminal o en cada host, seguridad en la instalación de programas o descargas maliciosas entre estas se complementa con el perfil, y la seguridad del firewall de la entidad.

Nivel 2.

También es de anotar que todo proyecto a implementarse es necesario evaluar los posibles riesgos y sobre todo en los riesgos inherentes que por su naturaleza no se pueden detectar de forma inmediata si no a la cadencia en que ellos avanzan, estos van surgiendo de forma inesperada.

Para este tipo de riesgos, se ha documentado cuales pueden ser y encontrarse en el diseño del SGSI especificando su causa y efecto.

Determinado esta etapa productiva se diseña y se gestiona los Controles teniendo como referencia la norma ISO27002, en la que nos informa con 14 capítulos, 18 dominios y 114 controles en donde debemos establecer los controles, como minimizar riesgos y fortalecer la seguridad de los activos de la entidad.

19. nivel 2: GESTION DEL RIESGOS INHERENTES CAUSA Y EFECTO.

riesgos inherentes al Proyecto del Sistema de Gestión de Seguridad de la Información del Instituto Financiero para el Desarrollo del Huila, se identifican 4 Riesgos.

Riesgos Inherentes del proyecto.

R1. Proyectos de inversión desarticulados con la plataforma estratégica

Efecto

- No viabilidad de los proyectos por parte de la entidad INFIHUILA.
- Retrasos en los tiempos de aprobación para su viabilizarían
- No cumplir con el plan estratégico de la entidad.

Causa

- Inexperiencia de la estructura o procesos de la entidad.
- Inexperiencia de las operaciones de la entidad y de los lineamientos de la entidad INFIHUILA.

R2. Informalidad en la realización de los planes estratégicos de la entidad.

Efecto

- Investigaciones disciplinarias
- Recortes presupuestales

Causa

- Incorrecto alcance en la ejecución de los proyectos.

- Inadecuado empalme en la entrega de información del proyecto.
- Mala imagen corporativa

R3. Interrupción competente inoportuno de los planes de inversión.

Efecto

- Investigaciones disciplinarias por parte de los organismos de control
- Afectación al presupuesto de inversión de la Entidad.

Causa

- Debilidad en la formalización del cierre del proyecto.
- Definición inadecuada de los entregables del proyecto.

R4. Falta de concientización y apropiación de los bienes o servicios generados por el Sistema de Gestión de Seguridad de la información.

Efecto

- Desgaste y reprocesos administrativos.
- investigaciones disciplinarias por parte de los organismos de control.
- Mala imagen corporativa
- Falta de socialización sobre los servicios alcanzados con la realización del proyecto.
- Falta de capacitación sobre la administración y manipulación de los servicios adquiridos con la realización del proyecto.
- No planear gestión del cambio y comunicaciones del proyecto.

20. Diseño del Sistema de Gestión de Seguridad de la Información SGSI Y SENSIBILIZACION.

Una vez determinados riesgos inherentes al diseño del SGSI, se determina los costos que implican SGSI (Sistema gestión de Seguridad de la Información).

El valor del diseño Sistema de Gestión de Seguridad de la Información SGSI de la entidad INFIHUILA este costo es un aproximado a los valores gestionados hoy en implementación, para que la seguridad de sus activos sea confiable hacia sus clientes y ante las entidades que lo vigilan.

Tabla 7 Diseño de Sistema de Seguridad de la información costo

	2019		2020	
	Iniciativa	**Valor**	**Iniciativa**	**Valor**
SGSI DE INFIHUILA	Renovación del servicio en la nube	$70.000.000	Implementación SGSI de Procesos // Preauditoria ISO 27001	$ 70.000.000
	Renovación certificados SSL	$ 35.000.000	Auditorias ISO 27001	$35.000.000
	Sensibilización Seguridad	$35.000.000	Solución de Cifrado	$ 20.000.000
	Cursos de Actualización Seguridad	$5.000.000	Ethical Hacking	$ 40.000.000
			Sensibilización Seguridad	$ 5.000.000
TOTAL X AÑOS	**$ 145.000.000**		**$ 170.000.000**	
TOTAL PERIODO 2019-2020				

La importancia de tener un Sistema de Gestión de Seguridad en el área de las TIC de la entidad INFIHUILA reside en numerosos puntos de vista tanto costos, como principalmente en ofrecer a la administración criterios de confiabilidad, integridad y accesibilidad a los activos de información del instituto.

Este Sistema de Gestión de Seguridad de la Información se debe actualizarse por lo menos cada año para el cumplimiento de los tres pilares de la seguridad como son Integridad, confiabilidad, disponibilidad de la información que su vez fortalecerá la infraestructura del Instituto y salvaguardando los activos más críticos de la entidad. es decir, el diseño del Sistema de Gestión de Seguridad de la Información SGSI propende de que el grupo obtenga el deber de coordinar, orientar la metodología y controlar que los líderes de cada área acepten las obligaciones utilitarias.

"Implementación comité de seguridad de la información, definiendo los participantes, las responsabilidades del comité, las funciones de cada participante, las funciones del consultor dentro del comité y la periodicidad de las reuniones ordinarias y extraordinarias". [40]

Para la construcción del comité de seguridad de la información es indispensable vincular a los jefes o directivos por departamento ya que la seguridad es responsable de todos en la cual se determinarán de la siguiente manera:

- *El jefe del área de informática o su delegado.*
- *El jefe del área de Planeación o su representante.*
- *El jefe del área Jurídica (según corresponda por distribución Orgánica de la entidad) o su delegado.*
- *El jefe encargado de los sistemas de Gestión de Calidad (según corresponda por distribución Orgánica de la entidad) o su delegado*

[40] Información suministrada de la guía de proyecto aplicado UNAD, como ejemplo al diseño del comité de seguridad de la información.

- *El jefe encargado de la Gestión Documental (según corresponda por distribución Orgánica de la entidad) o su delegado.*
- *El jefe encargado (según corresponda por distribución Orgánica de la entidad) de Control Interno o su delegado.*
- *El responsable de Seguridad de la información de la entidad.*[41]

El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

Objetivo del Comité de Seguridad de la Información.

El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.[42]

Funciones del comité. [43]

El Comité de Seguridad de la Información de la Nombre de la entidad tendrá dentro de sus funciones las siguientes:

41 https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

42 (MINTIC, s.f.)

43 (MINTIC, s.f.)

- Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
- Revisar los diagnósticos del estado de la seguridad de la información de
- Acompañar e impulsar el desarrollo de proyectos de seguridad.[44]
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de Nombre de la entidad.
- Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
- Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.

Las demás funciones inherentes a la naturaleza del Comité.

Una vez conformado el Comité de Seguridad de la Información, este podrá expedir su reglamento, en el cual fijará el alcance de cada una de las funciones operativas señalas en el presente informe.

[44] https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Secretaria Técnica: La Secretaría Técnica del Comité se definirá al interior del Comité y el secretario elegido será remplazado cada año (12) meses.

Funciones de la Secretaría Técnica. Las funciones de la Secretaría Técnica serán las siguientes:

- Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
- Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias
- Remitir oportunamente a los miembros la agenda de cada comité.
- Llevar la custodia y archivo de las actas y demás documentos soportes.
- Servir de interlocutor entre terceros y el Comité.
- Realizar seguimiento a los compromisos y tareas pendientes del Comité.
- Presentar los informes que requiera el Comité.
- Las demás que le sean asignadas por el Comité. [45]

Reuniones del Comité de Seguridad de la Información. El Comité de Seguridad de la Información – deberá reunirse (según periodicidad definida por la entidad), previa convocatoria del Secretario Técnico del Comité.

Sesiones Extraordinarias. Los miembros que conforman el Comité podrán ser citados a participar de sesiones extraordinarias de trabajo cuando sea necesario, de acuerdo con temas de riesgos, incidentes o afectaciones de continuidad dentro del Sistema de Gestión de Seguridad de la Información.

[45] (TIC, s.f.)

20.1 OBJETIVO SGSI

Implementar un sistema de gestión de seguridad para la entidad INFIHUILA en donde se protegerá todos los activos de información que la organización considere importante para garantizar su integridad, confiabilidad, y disponibilidad.

20.2 OBJETIVOS ESPECIFICOS SGSI

Estar al tanto y apropiarse se la Norma ISO 27001 en cuanto su metodología para aplicarse en la organización.

Cumplir un diagnóstico de todos los activos de la entidad y analizar sus riesgos.

Realizar un plan de tratamiento para salvaguardar los activos de la entidad mediante dominios y controles.

20.3 ALCALCE SGSI

Este análisis de contexto externo, interno abarca todos los procesos de la organización **INFIHUILA**, donde establece, implementa y opera en todos los activos de Información que la entidad considere importantes.

21. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL INFIHUILA.

La importancia de implementar las Políticas de Seguridad es el hecho de tomar acciones en un menor tiempo, fortalecer la infraestructura de una entidad, salvaguardar sus activos y minimizar riesgos.

Todo esto se puede realizar mediante un Manual de Políticas en cual su prioridad será la integridad, confidencialidad y disponibilidad de la información, mediante mejoras continuas a los proyectos implementados.

Siguiendo las pautas de la Norma ISO 27001:2013 se implementan las políticas de seguridad en la cual se tendrá a favor el control y su respectivo procedimiento. (**ver anexo manual de políticas**).

21.1 POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Este documento formaliza el deber de la administración, de administrar la seguridad de la información y muestra de forma escrita a los funcionarios y contratistas del instituto el resumen de las acciones con las que el Institutito Financiero para el desarrollo del Huila INFIHUILA establece normas para garantizar la integridad, confiabilidad y accesibilidad de los activos de la información de posibles riesgos, perdida y abuso de privilegios, hardware y otros activos de TI de la Entidad, que cambian y se desarrollan continuamente según el avance de la innovación y los requisitos previos de la entidad.

Este documento caracteriza las reglas que el Instituto Financiero para el desarrollo del Huila - INFIHUILA debe seguir en relación con la seguridad de la información. Estas reglas están escritas como políticas.[46]

21.2 OBJETIVO

Presentar y socializar en forma coherente los principios y la importancia de la política de seguridad de la información que deben conocer y cumplir todos los directivos, funcionarios, contratistas, y terceros que presten sus servicios o tengan algún tipo de relación con el Instituto Financiero Para el Desarrollo del Huila **INFIHUILA**

21.3 OBJETIVOS ESPECÍFICOS

- Promover la utilización de las mejores pruebas de seguridad sistemática en el trabajo, para que los clientes, usuarios, funcionarios se acoplen con la protección de datos y activos institucionales.

- Proponer los mecanismos de seguridad lógica, en el ambiente informático de modo que se contribuya con los componentes de seguridad sensibles en la condición de automatización para adicionar la confidencialidad, integridad y disponibilidad de la información.

[46] Políticas de seguridad de la información -Instituto Financiero para el Desarrollo del Huila - **INFIHUILA**

- Servir de guía para la conducta experta e individual de los funcionarios, contratistas del INFIHUILA, a fin de limitar los episodios de seguridad interna, por ejemplo, robo de datos o vandalismo.

- Promover los procedimientos prescritos de la seguridad física y lógica, mediante el uso de escenarios adecuadas que permitan el cuidado correcto de la información y el hardware supervisado por el área de seguridad, la utilización efectiva de los activos de tecnología de información.

- Regular la seguridad con partes legales y especializadas de seguridad de la información.

21.4 ALCANCE:

Las políticas aquí conocedoras deben ser de ejecución precisa para todas aquellas áreas, funcionarios, contratistas que utilicen equipos de cómputo y estén implicados continua o indirectamente con el uso de tecnologías de información y comunicaciones.

22. POLÍTICA PARA LA CONFIDENCIALIDAD DE LA INFORMACIÓN INTITUCIONAL Y TRATO CON TERCEROS.

Cada funcionario contratado por la entidad, para desempeñar sus propias obligaciones, aborda los datos institucionales en varias dimensiones (escrita, digital o verbales). Las instancias de este tipo de datos son notas, folletos, actas, circulares, bases de datos, informes, consultas a sistemas de datos.
Todos los datos privados a los que se acerca cada trabajador oficial o temporal en satisfacción de sus capacidades deben ser supervisados con el objetivo de que no se descubran a las personas que podrían utilizarlos para su propio beneficio, contra personas externas o la propia institución. Ningún trabajador oficial o temporal puede ajustar, borrar, encubrir o revelar datos para su propio beneficio o el de terceros.

En el estándar relacionado con esta estrategia, se hace referencia a las directrices y premisas legítimas que respaldan la regla del secreto de los datos

Dado lo anterior, esta política aplica al instituto Financiero para el Desarrollo del Huila - INFIHUILA según como se definió en el alcance, sus funcionarios, empelados en misión, terceros, aprendices, practicantes, proveedores y aliados estratégicos de la ciudadanía en general, teniendo en cuenta que los principios y políticas sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI y el Modelo de Seguridad y Privacidad de la Información, estarán determinadas por las siguientes proposiciones:

- Minimizar el riesgo en las funciones más importantes del instituto.
- Desempeñar los manuales de seguridad de la información.
- Mantener la confianza de sus asociados, clientes, socios, funcionarios, contratistas y aliados estratégicos.

- Apoyar la innovación tecnológica.
- Proteger los activos de información y 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, contratistas, terceros, aprendices, practicantes y clientes de **Instituto Financiero para el Desarrollo del Huila – INFIHUILA.**
- Garantizar la continuidad del negocio frente a incidentes.
- **El Instituto Financiero para el Desarrollo del Huila – INFIHUILA** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación, se establecen los principios de seguridad que soportan el SGSI del **Instituto Financiero para el Desarrollo del Huila – INFIHUILA**:

Los deberes con respecto a la seguridad de los datos serán específicos, intervenidas, distribuidos y reconocidos por cada uno de los trabajadores, proveedores, colegas o personas ajenas.

Instituto Financiero para el Desarrollo del Huila – INFIHUILA protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

Instituto Financiero para el Desarrollo del Huila – INFIHUILA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a

un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

Instituto Financiero para el Desarrollo del Huila – INFIHUILA protegerá su información de las amenazas originadas por parte del personal.

Instituto Financiero para el Desarrollo del Huila – INFIHUILA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos. [47]

Instituto Financiero para el Desarrollo del Huila – INFIHUILA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

Instituto Financiero para el Desarrollo del Huila – INFIHUILA garantiza control de acceso a la información, sistemas y recursos de red.

Instituto Financiero para el Desarrollo del Huila – INFIHUILA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

Instituto Financiero para el Desarrollo del Huila – INFIHUILA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

---

[47] Referencia al documento https://repository.unad.edu.co › bistraen › handle

Instituto Financiero para el Desarrollo del Huila – INFIHUILA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

Instituto Financiero para el Desarrollo del Huila – INFIHUILA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.[48]

Con base a las políticas de seguridad y privacidad de la información desarrolladas, se referencia a continuación la estructura de la norma ISO 27001 que expresan el cumplimiento de la norma en la **Instituto Financiero para el Desarrollo del Huila – INFIHUILA**:

[48] (ESPITIA)

Fuente: Activos de Información Saro Infihuila.

Figura 7 Dominios Noma ISO 27001.

NOTIFÍQUESE, COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

FIRMADO EN ORIGINAL.

LUIS ALFREDO ORTEGA MORENO

Gerente -INFIHUILA

Elaboro: Profesional Universitario de Informática.

Revisó: Comité SGSI - INFIHUILA

Aprobó: Comité SGSI - INFIHUILA

23. Listas de chequeo teniendo en cuenta la norma ISO/IEC 27002 en cada uno de los Dominios y Objetivos de control.

Teniendo como referencia la técnica u metodología de investigación se realiza la evaluación de cada control según la norma ISO 27002 en la que tiene como referencia 114 controles sobre 18 dominios en donde se analiza según los criterios observación, evidencia, entrevista, y la caracterización de cada proceso involucrado en el instituto Financiero para el Desarrollo del Huila INFIHUILA.

Se toma la evidencia del control, si aplica al Instituto Financiero para el Desarrollo del Huila y la recomendación que debería efectuar para el control para minimizar riesgos.

Tabla 8 Calificaciones o Nivel de Madurez

Se califica cada dominio de la ISO 27002 teniendo como base los valores del DAF y GEL en una escala del 1 al 5 (Siendo 1 debilidad y 5 fortaleza).		
Valoración	**efectividad**	**Cumplimiento** **Con respecto al control, es un control débil, cumple o excede las expectativas**
1	**No implantado**	No existen controles – Carencia completa de documentación y procesos
2	**50%**	Controles no estándar – La organización conoce los problemas y tiene intención de solucionarlos, algunos con enfoques propios, pero nada estandarizado
3	**90%**	El Requerimiento se Cumple en forma aceptable - Aunque existen los controles, no se comunican y/o difunden para crear consciencia y no se hace entrenamiento y seguimiento
4	**95%**	Controles Eficientes - Los controles se han documentado y estandarizado, se han seguido entrenamientos, sin embargo, la aplicación de estos en algunos casos es por cuenta propia del individuo.
5	**Administrado**	Optimizado – Es posible administrar los controles y medir el cumplimiento de estos para tomar medidas cuando no estén ejecutándose de forma debida.

SISTEMA DE GESTIÓN DE SEGURIDAD INFORMATICA						
CUADRO DE DOMINIOS Y CONTROLES SELECCIONADOS Y LISTA DE VERIFICACION						
MATRIZ DE VALORACIÓN ISO 27002						
CAPÍTULO 1 - Política de Seguridad Corporativa						
Procesos entrevistados/involucrados: Jurídica, Operaciones, Administración del sistema, Proyectos y convenios, mercadeo, Financiera, Contable, Dirección Administrativa, GTICS.						
	Ítem	**ISO Ref.**	**Control**	**Aplica (SI/NO)**	**Estado del cliente / Mecanismos de salvaguarda implementados**	**Valoración**	**Oportunidad de mejora y recomendación es**
	1.1	5	Políticas de Seguridad				
	1.1	5,1	Orientación de la dirección para la gestión de la seguridad de la información				
	1.1.1	5.1.1	Políticas para la seguridad de la información	Si	Existen políticas de seguridad Global de la información documentadas, pero falta socializarlas y que estas sean aprobadas y ejecutadas.	**2**	Aprobación, ejecución y socialización de la política
	1.1.2	5.1.2	Revisión de las políticas para la seguridad de la información	Si	No se tiene un plan periódico para la revisión, evaluación del cumplimiento de las políticas de la seguridad de	**2**	Se deberá dejar explícita la tarea periódica de revisión y evaluación en unas fechas formales.

					la información, aunque se cuenta con la política documentada.		
2	6	Organización de la Seguridad de la Información					
2.1	6,1	Organización Interna					
2.1.1	6.1.1	Roles y Responsabilidad de Seguridad de la Información	Si	Existe el compromiso y la voluntad por parte de la gerencia a nivel del área de Tecnología. Falta conciencia de seguridad de la información en los demás procesos, aunque se vienen adelantando campañas	**2**	Incrementar las campañas de densificación que permite tomar conciencia sobre el Sistema de Gestión de Seguridad de la Información
2.1.2	6.1.2	Contacto con autoridades	Si	No se tiene dentro del proceso de atención de incidentes el punto en concreto, las características que debe presentar el incidente y el protocolo a seguir para el contacto con las autoridades.	**1**	Realizar un procedimiento para control de incidentes.

	2.1.3	6.1.3	Contacto con grupos de interés especial	Si	El comité de seguridad no es miembro oficial de algún grupo especializado o de interés en seguridad de la información.	**2**	Inscribir a los miembros del comité de seguridad de la información en listas de correo especializadas e incrementar el contacto con los grupos de interés.
	2.1.4	6.1.4	Seguridad de la Información en la gestión de proyectos	Si	No son existen las funciones de la seguridad de la información en la evaluación y autorización de actividades en el procesamiento de datos o protección de la información, sin embargo existen procedimientos para realizar modificaciones o adiciones de software y hardware no aprobados ni socializados.	**2**	-Socializar y aprobar procedimientos. -realizar los esquemas de mantenimiento de documentos de auditorías de seguridad, como administración de Logs, revisión de bitácoras y monitoreo de incidentes en las áreas.
	2.1.5	6.1.5	Segregación de deberes	Si	Se realizan acuerdos específicos de confidencialidad tanto para la contratación como para la	**4**	Por ser una entidad financiera la organización, este punto tiene una especial madurez, incluyendo esquemas de estudios de seguridad y

					manipulación específica de datos o actividades en áreas de procesamiento de datos.		sanciones claramente especificadas
	2.2	6,2	Dispositivos móviles y teletrabajo				
	2.2.1	6.2.1	Política de dispositivos móviles	Si	No existe una política formal sobre el uso de computación móvil, de celulares, tables y demás dispositivos móviles.	**2**	Diseñar e implementar una política de control de computación móvil, acompañada del procedimiento adecuado al control a ciertos equipos.
	2.2.2	6.2.2	Teletrabajo	NO	No existe una política formal sobre actividades de teletrabajo.	**0**	Diseñar e implementar una política de Teletrabajo, acompañada del procedimiento adecuado de control que incluya las buenas prácticas permitidas y los mecanismos de control.
	3	7	Seguridad en los Recursos Humanos				
	3.1	7.1	Previo al Empleo				

	3.1.1	7.1.1	Selección. Verificación de antecedentes	Si	La Organización cumple con este control realizando el trámite de estos documentos, a través del área Jurídica en compañía con Talento humano-Contratación.	**3**	Mantener el control implementado y describir el procedimiento dentro del SGSI.
	3.1.2	7.1.2	Términos y condiciones del contrato	Si	se cumple en todos los procesos con el control, cuenta con el de confidencialidad.	**2**	Mantener el control implementado y describir el procedimiento dentro del SGSI
	3.2	7,2	Durante el empleo				
	3.2.1	7.2.1	Responsabilidades de la dirección	Si	Existen supervisores de los contratos, pero no existe un oficial de seguridad de la información.	**2**	La participación en seguridad de las directivas se realiza más que por su intención en el fortalecimiento de la seguridad por requerimiento y regulaciones. Esto puede mejorar con un plan de conciencia a nivel gerencial.

	3.2.2	7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Si	Se realizan muy pocas capacitaciones sobre esquemas y controles de seguridad. existe un plan formal de entrenamiento o conciencia en seguridad pero aún no se aprueba.	**3**	Aprobar y ejecutar el plan de concientización, el entrenamiento adecuado a los usuarios y la campaña completa de divulgación del SGSI
	3.2.3	7.2.3	Proceso disciplinario	Si	No es claro los descargos disciplinarios cuando se producen brechas de seguridad. Están documentados pero falta la socialización y aprobación de estos.	**1**	Capacitar y ejecutar procesos disciplinarios y descargos, e incluirlos dentro del manual de funciones y en el SGSI
	3.3	7.3	Terminación del contrato y cambio de empleo				
	3.3.1	7.3.1	Terminación o cambio de responsabilidades de empleo	Si	La INSTITUCION cumple con este control pero en algunos casos no hay procedimientos internos desde el punto de vista de seguridad de la información para dar de baja el usuario, sus permisos y roles.	**4**	Incluir el proceso en el SGSI cuando haya sido implementado en la terminación de contratos.

					La Organización cumple con este control, sin embargo no siempre se informa sobre los activos cuando una persona sale de su empleo.		
	4.1	8	Gestión de Activos				
	4.1	8,1	Responsabilidad de los Activos				
	4.1.1	8.1.1	Inventario de activos	Si	La Organización cumple satisfactoriamente con este control porque cuenta con una gestión del inventario manual (para hardware y software) y la identificación de los activos de información desde el punto de vista de seguridad de la información.	3	Centralizar el inventario de todos los activos en un listado maestro, enmarcado en un procedimiento y asignado a su responsable por su mantenimiento, todo desde un mismo software.

	4.1.2	8.1.2	Propiedad de los activos	Si	Cada proceso conoce los activos de información que tiene a su cargo pero no tiene plenamente identificadas las propiedades de cada activo., confidencial, publico o reservado y no conoce las consecuencias de una falla en la confidencialidad, Disponibilidad e integridad a las cuales podría estar sometida en algún momento la información.	**5**	Capacitar y sensibilizarlos de las responsabilidades sobre los activos de información.
	4.1.3	8.1.3	Uso aceptable de los activos	Si	Existe una política que indica que se proveen los medios necesarios para asegurar que un usuario preserve y proteja los activos de información de una manera confiable, con el fin de darle un buen uso a dichos recursos, sin embargo, a falta de auditorías internas en seguridad, no se	**3**	-Realizar procesos de auditoría en términos de cumplimiento operativo. -Aprobar y ejecutar la política de uso aceptable de los activos.

					conoce que tanto es el nivel de cumplimiento de esta política y si hay alguna violación de esta.		
	4.1.4	8.1.4	Devolución de los activos	SI	El instituto no cuenta con la socialización de un procedimiento y/o formato para que Los activos sean devueltos.	**0**	Se debe implementar y socializar el formato y el proceso de devolución de activos.
	4.2	8,2	Clasificación de la Información				
	4.2.1	8.2.1	Clasificación de la información	Si	No se tienen claramente Como etiquetar la información. Cada proceso conoce la pertinencia de la información pero carece de un procedimiento que le ayude a clasificar la información y le asigne un nivel de pertinencia (privado, publico interno, publico externo, etc.).	**2**	-Se debe capacitar y socializar el procedimiento de etiquetado de información e incluirlo en el SGSI.

	4.2.2	8.2.2	Etiquetado de la información	Si	Existe el procedimiento de etiquetado de los activos tanto en medios electrónicos como físicos que reflejen los niveles de clasificación de la información.	**2**	El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
	4.2.3	8.2.3	Manejo de activos de información	si	Existe el procedimiento pero aún falta aprobación y ejecución.	**2**	Ejecutar y aprobar el procedimiento de manejo de activos.
	4.3	8,3	Manejo de Medios				
	4.3.1	8.3.1	Gestión de medios removibles	Si	existe una política estricta sobre el uso de medios removibles dentro de la organización pero aún no se ha socializado ni aprobado.	**1**	Aprobar y ejecutar la política.
	4.3.2	8.3.2	Disposición de los medios	Si	La organización cuenta con elementos de destrucción documental, y realiza la disposición segura de medios cuando	**3**	Es necesario continuar con el proceso con revisiones periódicas.

					es requerido por parte de soporte interno.		
	4.3.3	8.3.3	Transferencia de medios físicos	Si	No se conoce una práctica formal de protección para los medios en movimiento.	**1**	En los casos en que sea necesario transportar información, debe exigirse el cumplimiento de una política de protección para esta información. La política y procedimientos deben ser estrictas e incluidas en el SGSI
	5	9	Control de Acceso				
	5.1	9,1	Requerimientos del Negocio para el Control de Acceso				

	5.1	9.1.1	Política de Control de Acceso	SI	Existe una política de control de acceso en la política de seguridad de la información.	**2**	Implementar, aprobar y ejecutar todas las acciones técnicas y mejoras que se puedan dar para optimizar el control de acceso (ejemplo: nuevas tecnologías biométricas).
	5.2	9.1.2	Acceso a redes y a servicios de red	SI	Actualmente existe una política formalmente definida para el uso adecuado de los servicios de red, pero no se ejecuta de manera óptima por parte de los usuarios (internet) debido a que la alta gerencia permite el uso de ciertos sitios web que podrían representar amenazas a la seguridad de la información.	**2**	Mantener y fortalecer la política de uso de los servicios de red que especifique la intención, autorización y control de este.
	5.2	9.2	Gestión de acceso a usuarios				

	5.2.1	9.2.1	Registro y cancelación del registro de usuarios	Si	Se realiza un proceso de registro de usuarios para cada individuo con perfiles y permisos asignados según justifique el caso. No se realiza un seguimiento periódico y formal a los usuarios en desuso del sistema. Se revisan usuarios bajo requerimiento.	**3**	Mantener la política de control de acceso de usuarios, realizar un seguimiento cronológico a usuarios creados con el fin de verificar su validación en los sistemas de información.
	5.2.2	9.2.2	Suministro de acceso de usuarios	SI	La organización cumple con un control fuerte para las contraseñas, sin embargo es responsabilidad del usuario final mantenerlas seguras.	**3**	Seguir concientizando a los usuarios finales en el uso de las contraseñas seguras. Para que sea más efectivo el control.
	5.2.2	9.2.3	Gestión de derechos de acceso privilegiado	SI	La Organización cumple satisfactoriamente con este control, tiene controles y documentación del proceso de	**4**	Mantener el control de administración de privilegios, documentarlo alinearlo con el SGSI.

					asignación de perfiles a los usuarios.		
	5.2.3	9.2.4	Gestión de información de autenticación secreta de usuarios	SI	Se tienen directivas sobre el uso y administración de contraseñas.	**4**	Socializar SGSI y la política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas.
	5.2.4	9.2.5	Revisión de los derechos de acceso a usuarios		No se realiza la tarea periódicamente con el detalle requerido para identificar inconvenientes con los perfiles.	**1**	Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
	5.2.4	9.2.6	Retiro o ajuste de los derechos de acceso	SI	Se debe exigir a los usuarios que cumplan las prácticas de la institución para el uso de información de autenticación privilegiado.	**0**	Se debe implementar un procedimiento u formato que una vez finalizada su labor o contrato el usuario con privilegios sean cancelados o en su defecto bloqueados.
	5.3	9,3	Responsabilidades de los usuarios				

	5.3.1	9.3.1	Uso de información de autenticación secreta	SI	La Institución, mediante recordatorios, promueve el buen uso de las contraseñas, recomendando no escribirla y no usar una contraseña en más de 1 sistema al tiempo.	**4**	Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema.
	5.4	9.4	Control de acceso a sistemas y aplicaciones				
	5.4.1	9.4.1	Restricción de acceso a la información	SI	Se tienen restricciones a los diferentes sistemas de información, se cuenta con acceso a la Base de Datos de toda la información del instituto, a esta se puede ingresar por medio de aplicación o por medio de herramientas que permiten ingresar	**2**	Socializar el procedimiento, y que este sea aprobado de acceso a la información.

					directamente a la información.		
	5.4.2	9.4.2	Procedimiento de ingreso seguro	SI	La institución cuenta con métodos de autenticación segura otorgada por los protocolos usados para autenticar. Existe un procedimiento y política	**4**	Aprobar y sensibilizar a los usuarios del ingreso seguro.
	5.4.3	9.4.3	Sistema de gestión de contraseñas	SI	El instituto cumple satisfactoriamente con este control. Está documentada la Políticas	**4**	Aprobar, sensibilizar y Mantener el esquema implementado de la política.
	5.4.4	9.4.4	Uso de programas utilitarios privilegiados	SI	la restricción existe debido a que los usuarios trabajan a través de terminales.	**4**	Los usuarios están conectados a través de terminales lo que permite llevar un mejor control.

	5.4.5	9.4.5	Control de acceso a códigos fuente de programas	SI	El instituto cuenta con la política, Se restringe el acceso a códigos fuente de programas. Solo usuarios con privilegios pueden ingresar a los códigos fuente de los programas.	**4**	Solo Los usuarios del sistema de información están conectados a través de terminales lo que permite llevar un mejor control.
	6.1	10.1	Controles Criptográficos				
	6.1.1	10.1.1	Política sobre el uso de controles criptográficos	Si	La institución no emplea controles criptográficos para almacenar la información. Solo se utiliza en las transacciones	**1**	Los esquemas criptográficos deben ser obligatorios para el manejo y transporte de información utilizando la clasificación de información. Este esquema debe implementarse y ser aprobada en la política contenida en el SGSI

					electrónicas y certificados de bonos pensionales.		
	6.1.2	10.1.2	Gestión de llaves	SI	No hay una política formal en el área para la administración de llaves de cifrado debido a que no se tienen controles criptográficos.	0	Una vez implementados los controles cifrado, es necesario definir e implementar una política y procedimiento de administración metodológica de cifrado.
	7.1	11	Seguridad física y del entorno				
	7.1	11.1	Áreas seguras				
	7.1.1	11.1.1	Perímetro de Seguridad Física	Si	La institución cumple parcialmente con este control, en el primer piso del	**3**	Implementar más controles biométricos a las áreas críticas para fortalecer el perímetro de seguridad.

					edificio hay vigilancia, y en tercer piso la entrada es través de biometría. Está pendiente el control biométrico en otras áreas		
	7.1.2	11.1.2	Controles de acceso físicos	Si	La Institución cumple parcialmente con algunos controles, existe control biométrico al ingreso del instituto y control en centro de cómputo. También existe la política y	3	-Aprobar e implementar más controles en las áreas críticas. -- implementar un esquema para luego ser monitoreado por el responsable.

					procedimiento		
	7.1.3	11.1.3	Seguridad de oficinas, recintos e instalaciones	Si	Parcialmente las áreas dentro de las instalaciones se encuentran controladas y monitoreadas con cámaras de seguridad. se mantienen cerradas las puertas de las oficinas.	**3**	Incluir, aprobar la política en el SGSI la descripción de las precauciones de seguridad en oficinas. Algunas áreas son visibles desde el exterior.
	7.1.4	11.1.4	Protección contra amenazas externas y ambientales	Si	Actualmente el SGST ha realizado esquemas, según lo indica la norma para las	**4**	Documentar todos los controles de protección contra amenazas externas

					diferentes áreas para garantizar que no se generen afectaciones por parte de amenazas externas o ambientales. Por parte del edificio se tienen controles generales contra incendios.		
	7.1.5	11.1.5	Trabajo en áreas seguras	SI	En la actualidad no existen áreas restringidas en el instituto. Se tiene,	**2**	Implementar controles de acompañamiento y registro de todos los usuarios que ingresan a áreas que manejan información sensible.

					en el centro de datos del instituto, unos controles y en el tercer piso.		
	7.1.6	11.1.6	Áreas de despacho y carga	NO	No se conocen sitios de cargue y descargue	**0**	la entidad no lo requiere
	7.2	11,2	Equipos				
	7.2.1	11.2.1	Ubicación y protección de los equipos	Si	Los equipos tecnológicos se ubican en lugares seguros, libre del polvo buscando mantener el menor nivel de exposición a terceros o visitantes.	**3**	Debe aprobar la política y ejecutarse dentro del SGSI que requiera la protección y ubicación de los equipos tecnológicos en áreas protegidas.

	7.2.2	11.2.2	Servicios de suministro	Si	La institución cumple satisfactoriamente con este control, usando las medidas de respaldo del edificio, en donde se tiene una UPS con un Banco de baterías de energía que puede alimentar a los equipos y servidores del INFIHUILA para aproximadamente 1 hora lo suficiente como para apagarse de forma	4	Se debe mantener el esquema de UPS e implementar una planta eléctrica en óptimas condiciones minimizar riesgos en el funcionamiento de servicio.

					controlada.		
	7.2.3	11.2.3	Seguridad en el cableado	Si	La Organización cumple satisfactoriamente con este control, todo su cableado es certificado, marcado, protegido y separado.	**5**	Mantener el esquema y monitorear cables obsoletos.
	7.2.4	11.2.4	Mantenimiento de equipos	Si	Existe un procedimiento, y un plan de mantenimiento de equipos, se controla con la consola de	**5**	Se debe mantener el cronograma de mantenimientos constantes sobre los equipos tecnológicos.

					Antivirus q frecuentemente da aviso de sus vulnerabilidades. En los cuales se han llevado a cabo de forma correcta.		
	7.2.5	11.2.5	Retiro de activos	Si	El instituto no cumple estrictamente el protocolo para la salida y entrada de activos y no hay evidencia de esta.	**3**	Incentivar el estricto uso del protocolo de entrada y salida de activos. Implementar formato, procedimiento y su respectiva aprobación.

	7.2.5	11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI	Se tienen documentados un procedimiento pero no se cumple sin embargo estos controles difícilmente son llevados a cabo el 100% de las veces debido a que se los empleados pueden sacar activos tecnológicos y de información por su cuenta.	**3**	El SGSI debe dictaminar las políticas de uso de equipos de cómputo fuera de las instalaciones de la organización que permitan a directivos y a los líderes de los procesos, conocer los requerimientos de seguridad para el uso de estos elementos.

	7.2.6	11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.		Se documenta la política pero no aún no se ejecuta, se controla con el antivirus de cada equipo que al conectarse el detecta el análisis de forma automática. No se tiene un procedimiento para el borrado seguro de la información y reutilización de tecnología.	**3**	Se debe diseñar implementar y aprobar un procedimiento para el borrado seguro de la información y socializarlos con los funcionarios y contratistas. Y reutilización de equipos mediante una política fuerte dentro del SGSI que no discrimine ningún caso.
	7.2.7	11.2.8	Equipos de usuario desatendido	SI	existe política para los usuarios deben asegurarse de	**3**	Actualmente se encuentra implantada una política de bloqueo en los equipos de forma automática en el tiempo establecido por la entidad.

					que a los equipos desatendidos se les da protección apropiada. Pendiente aprobación de esta		
	7.2.7	11.2.9	Política de escritorio y pantalla limpios	SI	Existe política documentada. Pero aún no ha sido aprobada, ejecuta, socializada y monitoreada	2	-Socializar aprobar y monitorear la política -- capacitaciones de concientización y entrenamiento encaminados al tema
		12	Seguridad de operaciones				
	8.1	12.1	Procedimientos operacionales y responsabilidades				
	8.1.1	12.1.1	Procedimientos de operación documentados	Si	Se mantienen manuales operativos sobre los procesos	**4**	Socializar los procedimientos y los diferentes formatos para que este alineado o incluido en el SGSI

					fundamentales del área, que indiquen el qué hacer y cómo hacerlo al momento de llevar a cabo alguna actividad.		
	8.1.2	12.1.2	Gestión de cambios	Si	Se encuentran en los procedimientos y formatos registros de control de cambios para cualquier actualización en los sistemas	**3**	Se debe aprobar y ejecutar el procedimiento de registros de control de cambios deben incluir los elementos de seguridad necesarios, la protección y revisión de estos y su inclusión en el SGSI

					de información sin embargo existe un procedimiento formal para la gestión del cambio que debe aprobarse, hasta ahora sólo se basa en peticiones de los usuarios.			
	8.1.3	12.1.3	Gestión de capacidad	Si	Existe un procedimiento para gestión de capacidad pero no se ha implementado, ni	**2**		La información debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere que se apruebe, diseñe un

					aprobado, ni socializado.		formato para el control y socialice dicho procedimiento.
	8.1.4	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	SI	Se cuentan con ambientes de Producción y pruebas que aún no están separados.	**3**	Se debe aprobar, ejecutar e implementar la separación de ambientes de pruebas con controles para asegurar la confiabilidad, integridad y disponibilidad de la información.
	8.2	12.2	Protección contra códigos maliciosos				

	8.2.1	12.2.1	Controles contra códigos maliciosos	SI	Actualmente la institución tiene consola de antivirus de información de todos los equipos instalados en la institución, licenciados que previenen la ejecución del código malicioso, tanto en servidores como en estaciones de trabajo.	**4**	Socializar y aprobar el procedimiento y formato diseñados de revisión a todas las estaciones de trabajo.
	8.3	12.3	Copias de Respaldo		Si		
	8.3.1	12.3.1	Respaldo de la información		La institución cumple satisfactoriamente	**4**	Conservar esta política y sociabilizarla al grupo de usuarios.

					con este control y se tiene una política de Backus documentada, pendiente extenderla a las demás las estaciones de trabajo.		
	8.4	12.4	Registro y Seguimiento				
	8.4.1	12.4.1	Registro de eventos	Si	La institución no cumple en su totalidad con este control. Aunque se tienen los registros y las configuraciones de auditoría, estos	**2**	Elaborar procedimiento y formato para conservar y revisar periódicamente los registros acerca de las actividades de los usuarios, fallas, y eventos de la seguridad de la información.

					no se revisan de manera formal y periódica.		
	8.4.2	12.4.2	Protección de la información de registro	Si	La institución posee una política pendiente por socializar, aprobar y ejecutar.	**1**	Aprobación de la política, ejecución y monitoreo continuo.
	8.4.3	12.4.3	Registros del administrador y del operador	Si	La institución no cumple con los registros de actividades del administrador y el operador de Sistemas, no existe un responsable.	**3**	Se debe delegar un responsable para que realice el monitoreo de dichas actividades, ejecutando la política y su procedimiento.

	8.4.4	12.4.4	Sincronización de relojes	SI	Se tienen sincronizados los servidores y equipos de algunos clientes.	4	Se debe mantener el procedimiento de sincronización de todos los Sistemas y Aplicaciones, con un sistema unificado para toda la plataforma tecnológica de la organización.
	8.5	12.5	Control de software operacional			Si	
	8.5.1	12.5.1	instalación de software en los sistemas operativos	si	Existe la política y el procedimiento para controlar instalación de software en los sistemas operativos.	**4**	Aprobar política y procedimientos para seguir el esquema implementado de revisión de sistemas y de puesta en producción.
	8,6	12,6	Gestión de vulnerabilidad técnica			Si	
	8.6.1	12.6.1	Gestión de las vulnerabilidades técnicas	SI	La institución cuenta con antivirus que maneja las diferentes estaciones de	**4**	Dada la oportunidad de mejora es recomendable realizar el paso a paso con su respectivo procedimiento o manual que incorpore este monitoreo, y así mismo definir los tiempos.

					Trabajo en la cual oportunamente está informando de las vulnerabilidades de los equipos ya sea sistema operativo o alguna aplicación especial.		
	8.6.2	12.6.2	Restricciones sobre la instalación de software	SI	La institución tiene implementado el servicio de Directorio Activo la cual cohíbe al usuario instalar sin autorización.	**4**	Aunque existe la restricción es indispensable aprobar la política y socializarla.
	8.7	12.7	Consideraciones relacionadas con la auditoría interna				

	8.7.1	12.7.1	Controles de auditorías de sistemas de información	SI	Las auditorías no se realizan sobre los registros y sistemas de información, aunque tienen un comité que define unos procesos de auditoría.	**2**	Documentar e implementar dentro del SGSI, los casos y controles para tener en cuenta para las actividades de auditoría sobre sistemas en producción.
		13	. Seguridad de las comunicaciones				
	9.1	13.1	Gestión de la seguridad de las redes	Si			
	9.1.1	13.1.1	Controles de redes	Si	El instituto cuenta con diferentes herramientas para controlar la red, pero a pesar de contar	**2**	Se debe utilizar una estrategia para la arquitectura de seguridad en la red LAN (desde el punto de vista de correlación de eventos y monitoreo de seguridad), para ubicar y configurar correctamente todos los elementos de seguridad y

					con los elementos necesarios para el monitoreo de la red, no se realizan monitoreo constante sobre tráfico, conexiones o revisión de anomalías.		monitoreo en la red. Esto debe estar acompañado de una política de seguridad en el SGSI.
		13.1.2	Seguridad de los Servicios de Red	SI	El instituto tiene documentada políticas y prácticas adoptadas para monitorear la red, La organización cumple con este control mediante un	**3**	Aprobar la política, socializarla Generar un adecuado control sobre todos los servicios de red e implementar un sistema de detección intrusos, prevención y responder a amenazas en tiempo real

					firewall, control de DNS, Web que protege y restringe el acceso a la infraestructura aplicaciones.		
	9.13	13.1.3	Separación en las redes	SI	En el instituto no existe la segmentación de redes.	**0**	Implementar la segmentación, documentarla y realizar el plano de cableado estructurado actualizado.
	9.2	13.2	Transferencia de información				
	9.2.1	13.2.1	Políticas y procedimientos de transferencia de información	Si	Los lineamientos con respecto a intercambio de información son	**1**	Implementar una metodología para realizar un intercambio de información seguro. Se recomienda el uso de (boxcriptor) para encriptar el contenido que se publica en Dropbox.

					incluidos a nivel de contrataciones y de acuerdos con entes reguladores, a través de acuerdos de confidencialidad. El instituto cuenta con la política y efectúa el control con un formato de confiabilidad que es otorgado a cada contratista, funcionario, aprendiz, practicantes etc. a la hora de firmar		

					el contrato.		
	9.2.2	13.2.2	Acuerdos sobre transferencia de información	Si	Además de los acuerdos de confidencialidad, no se hacen controles adicionales sobre el intercambio de información.	**2**	El manejo de información y su intercambio con terceros debería incluir acuerdos sobre su transporte y almacenamientos seguros al tratar y manipular la información segura (por ejemplo comprimir y cifrar la información)

	9.2.3	13.2.3	Mensajería Electrónica	Si	El correo electrónico es el medio principal de comunicación de la Institución. También se utiliza como repositorio de registros, actas, y otro tipo de constancias auditables. No se cuenta con encriptación de mensajería.	**2**	Existe la política y el protocolo a seguir con el correo electrónico pero aun Se debe mantener el diseño de seguridad sobre el correo a nivel de contingencias, antivirus, antispam y revisar periódicamente la efectividad de todos los controles, adicionalmente se requiere encriptación, vía PGP o S/MIME.
	9.2.4	13.2.4	Acuerdos de confidencialidad o de no divulgación	SI	Se realizan acuerdos de confidencialidad específicos para la labor con terceros que	**3**	Incluir la política de seguridad en los acuerdos y contratos con terceros en su ámbito de aplicación.

					implican la manipulación de información y el ingreso a áreas, sin embargo, se da a conocer a algunos terceros sobre la política de seguridad pero no se hace firmar un documento que deje plena constancia de que el tercero conoce dichas políticas y acepta cumplirlas dentro de su ámbito de aplicación.		

	10	14	Adquisición, desarrollo y mantenimiento de sistemas				
	10.1	14..1	Procesamiento correcto en aplicaciones				
	10.1.1.	14.1.1	Análisis y especificación de requisitos de Seguridad de la información	Si	La entidad realiza estudio de mercado con especificaciones y requisitos que orienta al responsable en los temas de aplicaciones seguras.	4	Se debe realizar el proceso paso a paso y así mismo documentarlo.

	10.1.2	14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Si	El instituto cuenta con servicios seguros, a través de distintas herramientas, para controlar software malicioso o dañino.	**4**	Realizar de Forma Periódica revisión de estas herramientas, actualizaciones etc. y realizar el proceso y documentarlo.
	10.1.3	14.1.3	Protección de transacciones de los servicios de las aplicaciones	SI	La institución cuenta con tokens para realizar las distintas transacciones electrónicas de Forma segura, aparte de esto el banco maneja su seguridad a través de	**4**	Conociendo la anterior información se recomienda realizar el proceso de adquisición de herramientas de seguridad con un manual y su respectivo procedimiento y formatos.

					otras herramientas que son otorgadas a la institución para manejo de transacciones electrónicas.		
	10.2	14.2	Seguridad en los procesos de desarrollo y soporte				
	10.2.1	14.2.1	Política de desarrollo seguro	Si	Aunque no es un instituto que desarrolla software cuenta con uno pequeño, al cual existe política documentada pendiente aprobación.	**4**	Monitorear con Frecuencia la política, una vez sea aprobada.
	10.2.2	14.2.2	Procedimientos de control de cambios de sistemas	Si	La Institución cuenta con el procedim	**2**	Aprobar, socializar y ejecutar procedimiento

					iento pero aún no se evidencia aprobación e implementación y socialización		
	10.2.3	14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Si	La Institución cumple parcialmente con este control, sin embargo no hay un documento formal para aprobar cambios en los sistemas operativos.	**3**	Realizar formato de control de cambios (RACI) para los diferentes sistemas, aplicaciones u herramientas operativos en el del instituto.
	10.2.8	14.2.8	Pruebas de Seguridad de sistemas	Si	Durante la implementación se realizan las diferentes pruebas para que	3	Conociendo lo anterior el área tics debe implementar flujos de pruebas y casos de usos para las pruebas de seguridad y aceptación de los sistemas. Así mismo se solicita al proveedor unas pruebas de estas.

					estas puedan activarse en el Instituto. Este control se evidencia con las diferentes actas. Pero no se evidencia casos de uso		
	10.2.9	14.2.9	Prueba de aceptación de sistemas		La institución no tiene un procedimiento formal para la aceptación de sistemas de tal forma que se le exija a los proveedores cumplir ciertos lineamientos de segurida	**1**	De debe realizar un procedimiento de establecimiento de requerimientos para la aceptación de nuevos sistemas o modificaciones sobre los existentes.

					d antes de poner un sistema en producción.			
	10.3	14.3	Datos de Prueba					
	10.3.1	14.3.1	Protección de datos de prueba	SI	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente	**3**	Se evidencia que el Infihuila tiene protegidos los datos de prueba con usuarios de autenticación con privilegios, se debe realizar un procedimiento acorde a la protección de datos de prueba se	
	11	15	Relaciones con los proveedores					
	11.1	15.1	Seguridad de la información en las relaciones con los proveedores					
	11.1.1	15.1.1	Política de Seguridad de la información para las relaciones con proveedores	SI	Los requisitos de seguridad de la información para mitigar los riesgos asociadas con el acceso de proveedores a los activos de la organización	**2**	Aprobar y socializar la política.	

					se deben acordar con estos y se deben documentar.		
	11.1.2	15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	SI	El instituto cuenta con cláusulas para concientizar a los proveedores. pero no se evidenció documentación. s pendiente aprobar el documento. Socializarlo y aplicarlo	**3**	Elaborar un documento o instructivo, aprobarlo y socializarlo para conserva la confiabilidad, integridad y accesibilidad de los activos de información a los que estos tienen acceso.

	11.1.3	15.1.3	Cadena de suministro de tecnología de información y comunicación.	SI	El instituto cuenta con cláusula de riesgos de seguridad de la información, pendiente aprobación	**2**	Pendiente por aprobar documentación e implementarla con los clientes y/u proveedores.
	11.2	15.2	Gestión de la prestación de servicios de proveedores				
	11.2.1	15.2.1	Seguimiento y revisión de los servicios de los proveedores	SI	El instituto realiza seguimiento revisar con regularidad la prestación de servicios de los proveedores. Mediante un formato cronograma de actividades, se evidencia formato supervisión de obligaciones	**3**	Se realiza un seguimiento mensualmente frente a la supervisión de los contratos, en donde se revisa el cumplimiento del objeto contractual y determinar el nivel de cumplimiento del contrato.

	11.2.2	15.2.2	Gestión de cambios en los servicios de los proveedores	SI	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.	**0**	Elaborar un formato que se diligencia frente al cumplimiento del proveedor, así mismo se realiza la respectiva evaluación y se solicita si es necesario cambios frente a los servicios.
	12	16	Gestión de incidentes de seguridad de la información				
	12.1	16.1	Gestión de incidentes y mejoras en la seguridad de la información				

	12.1.1	16.1.1	Responsabilidades y procedimientos	Si	El instituto cuenta un documento pero que aún no está divulgado sobre las responsabilidades de cada rol en un incidente de seguridad de la información.	**1**	aprobar, divulgar y socializar formalmente el proceso implementado dentro del marco del SGSI.
	12.1.2	16.1.2	Reporte de eventos de Seguridad de la información.	Si	El instituto cuenta con un formato donde se reporta los diferentes eventos de seguridad, pero no se ha socializado con los funcionarios y demás contratistas de la entidad por lo tanto no tiene	**3**	Se debe socializar dicho documento sus procedimientos y los diferentes eventos, crear capacitaciones de concientización y entrenamiento, identificar claramente los incidentes relacionados con la seguridad de la información y su reporte.

					conciencia de los mismos.		
	12.1.3	16.1.3	Reporte de debilidades de seguridad de la información		Se identifican las debilidades teóricas concernientes a la seguridad en todos los aspectos (análisis de riesgos de seguridad de la información interno) se evidencia un formato, y una matriz de los riesgos reportados.	**5**	Se debe realizar seguimiento, realizar acciones de mejora y monitorear trimestral mente.
	12.1.4	16.1.4	Evaluación de eventos de Seguridad de la información y		Los eventos de seguridad de la información se deben evaluar y se debe decidir	**0**	se debe elaborar, implementar, aprobar y ejecutar un procedimient o asociado a

			decisiones sobre ellos		si se van a clasificar como incidentes de seguridad de la información. No se evidencia dicha evaluación y respuesta.		incidentes de seguridad de la información y socializar dicha información.
	12.1.5	16.1.5	Respuesta a incidentes de seguridad de la información	Si		**0**	
	12.1.6	16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Si	No se realizan estudios (por ejemplo: análisis forenses) de los incidentes de seguridad. Algunos intentos de intrusión son monitoreados.	0	Además de tipificar esta labor como parte de las actividades de un oficial de seguridad, definir el procedimiento adecuado en el SGSI y realizar la revisión a todos los reportes de incidentes e incluirlos en el plan de mejoramiento.

	12.1.7	16.1.7	Recolección de evidencia	SI	No se tiene la conciencia de la gravedad de un incidente de seguridad (a nivel de usuarios finales) lo que hace lento el proceso de recolección de evidencia si se llegare a presentar.	**0**	Diseñar e implementar el procedimiento detallado de recolección de evidencia que permita de forma efectiva obtener toda la información necesaria y concientizar a los usuarios del impacto que puede tener un incidente y las demoras que representaría en su trabajo para la toma de evidencias.
	13	17	Aspectos de Seguridad de la información de la gestión de continuid				
	13.1	17.1	Continuidad de Seguridad de la información				
	13.1.1	17.1.1	Planificación de la continuidad de la seguridad de la información	Si	La entidad cuenta con un plan, para mantener la	**3**	Tener diseñado un cronograma de prueba de pen tes para el monitoreo de la infraestructura, los tiempos de respuesta y

					continuidad del negocio para garantizar que las operaciones críticas del instituto no paren. Contratada por un tercero.		actualizar cada año este documento.
	13.1.2	17.1.2	Implementación de la continuidad de la seguridad de la información	Si	El instituto cuenta a través de una firma la implementación de sitios alternos según los planes de continuidad del negocio en todos los procesos críticos.	3	Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria.
			Verificación, revisión y evaluación de la continuidad de la	SI	No se realizan revisiones a los planes de continuidad del negocio. Se tiene un plan pero al no ejecutarse	3	Debe Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a

	13.1.3	17.1.3	seguridad de la información		carecen de elementos y experiencia para su actualización.		prueba o en simulacro.
	13.2	17.2	Redundancia				
	13.2.1	17.2.1	Disponibilidad de instalaciones de procesamiento de información	SI	El instituto cuenta con un procesamiento datos Cloud, contratado por un tercero.	4	Debe socializar la disponibilidad de estas instalaciones con la organización con temas de concientizar al usuario para dichos eventos en caso de presentar alguna novedad.
	14	18	Cumplimiento				
	14.1	18.1	Cumplimiento de los requisitos legales y contractuales.				
	14.1.1	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Si	El Instituto cumple satisfactoriamente con este control, se cuenta con los controles establecidos para la función pública y con las exigencias de	**4**	Extender la investigación de legislaciones aplicables a los temas de seguridad de la información.

					los entes externos como la contraloría y la DIAN.		
	14.1.2	18.1.2	Derechos de propiedad intelectual	Si	La Organización cumple satisfactoriamente con este control, tiene pleno respeto por el licenciamiento del software en todos sus sistemas. Se tiene implementado una auditorias de control donde se realiza un reporte anual acerca de licenciamiento de Software, este es realizado por Control Interno y Revisoría.	**4**	Debe implementar un formato en las TICS para llevar el control junto con la representación implementado por control interno. Aprobar la política de cumplimiento sobre la propiedad intelectual.

	14.1.3	18.1.3	Protección de registros	Si	Los registros del Instituto tienen salvaguarda y se aplican una serie de medidas como la retención y clasificación por tipos, sin embargo no se tiene aprobada la política para el control de medios de almacenamiento removibles.	**3**	Establecer procedimientos, aprobar la política, socializar temas de seguridad para los registros Institucionales de clasificación confidencial.
	14.1.4	18.1.4	Privacidad y protección de información de datos personales	Si	La institución cumple satisfactoriamente con este control, tiene una política de protección de datos personales.	**4**	Socializar y aprobar la política con. Implementar esta política en sitio web, sección PQRSD cuando los usuarios se registren.
	14.1.5	18.1.5	Reglamentación de controles criptográficos		El instituto cuenta con la política de controles criptográficos, solo está la criptografía en certificados y transaccione	**2**	se debe implementar controles Criptográficos en cumplimiento de todos los acuerdos, decretos, resoluciones legales.

					s electrónicas.		
	14.2	18.2	Revisiones de Seguridad de la información				
	14.2.1	18.2.1	Revisión independiente de la seguridad de la información	Si	Existen políticas de seguridad de la información documentadas, pero falta sociabilizarlas y crear conciencia mediante programas formales y Reinducciones.	**2**	Aprobar y ejecutar las políticas de seguridad de la información documentadas, y sociabilizarlas para crear conciencia mediante programas formales.

	14.2.2	18.2.2	Cumplimiento con las políticas y normas de Seguridad	Si	Actualmente el alcance de la política cubre globalmente la seguridad de la información, la Institución de seguridad de la información pero aún no se ha socializado ni aprobado.	**2**	Debe implementarse la política, aprobarse y socializarse crear conciencia a los funcionarios y contratista en todos los temas de seguridad.
	14.2.3	18.2.3	Revisión del cumplimiento técnico	Si	El instituto no cuenta con el control de revisión periódicamente para verificar si las políticas se están cumpliendo ya que falta aprobación y designar un responsable	**0**	Se debe implementar y delegar un responsable para revisión periódica de las políticas aprobadas.

Tabla 9 Matriz de Valoración ISO27002

24. MEDICION EN EL NIVEL DE MADUREZ DE CADA DOMINO

Se identificaron los diferentes controles que el Institutito Financiero para el Desarrollo del Huila, tiene por cada Dominio según lo contemplado en la Norma ISO 27002 en donde se orienta el proceso de analizar y evaluar 14 capítulos, contemplados con 18 Dominios y 114 controles los que se toman como referencia a los implementados por el Instituto. Dichos controles se toman como muestra el nivel de Madurez en cada uno como lo ilustra en la siguientes gráficos y tablas.

Tabla 10 Calificaciones

Cada uno de los requerimientos de la hoja de los DOMINIOS ha sido calificado en una escala del 1 al 5 (Siendo 1 debilidad y 5 fortaleza).

Calificación	Efectividad	Cumplimiento Con respecto al control, es un control débil, cumple o excede las expectativas	CNM-INFIHUILA
0	**0%**	No está definido ningún tipo de control	12
1	**10%**	No existen controles efectivos – Deficiencias considerables con respecto a lo esperado para el requerimiento	8
2	**50%**	Controles Básicos – Deficiencias menores con respecto a lo esperado para el requerimiento	30

3	**90%**	El Requerimiento se Cumple en forma Efectiva	36
4	**95%**	Controles Comprehensivos	23
5	**100%**	Optimizado – Implementación que mejora el estándar	2

Fuente Autor.

Tabla 11 Nivel de Madurez por Dominio

Dominio	Porcentaje Cumplimiento
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50%
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	36%
SEGURIDAD DE LOS RECURSOS HUMANOS	64%
GESTIÓN DE ACTIVOS	56%
CONTROL DE ACCESO	74%
CRIPTOGRAFÍA	25%
SEGURIDAD FÍSICA Y DEL ENTORNO	71%
SEGURIDAD DE LAS OPERACIONES	78%
SEGURIDAD DE LAS COMUNICACIONES	34%
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	71%
RELACIONES CON LOS PROVEEDORES	75%

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	21%
ASPECTOS DE LA SEGURIDAD DE LA INFORMACION DE LA GESTION DE LA CONTINUIDAD DEL NEGOCIO	90%
CUMPLIMIENTO	71%

Nivel de Cumplimiento de los controles

Tabla 12 Resumen Cumplimiento

Controles Aprobados	**100**
Controles No aprobados	**3**
Controles no aplicados	**11**

Figura 8 Cumplimiento.

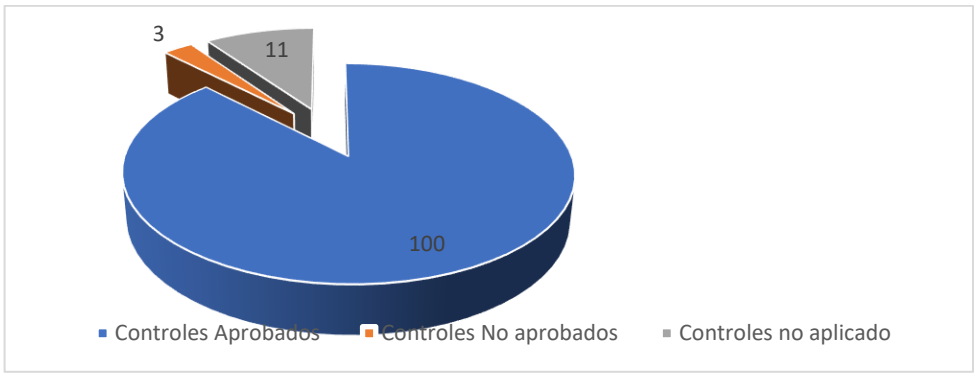
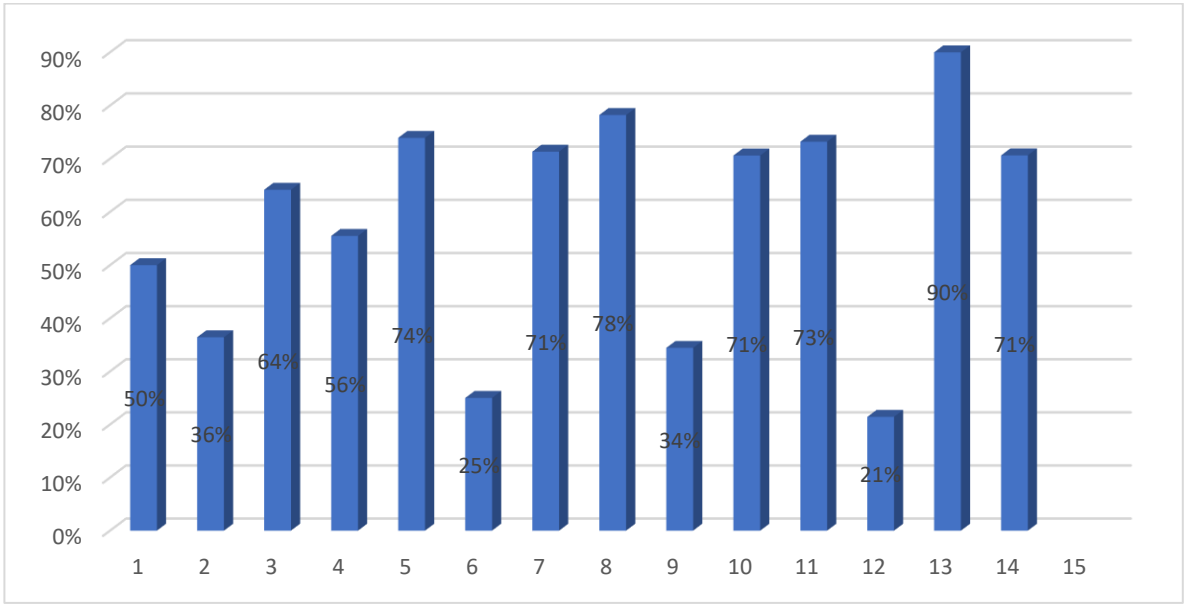


Figura 9 Nivel de Madurez como referencia al SGSI



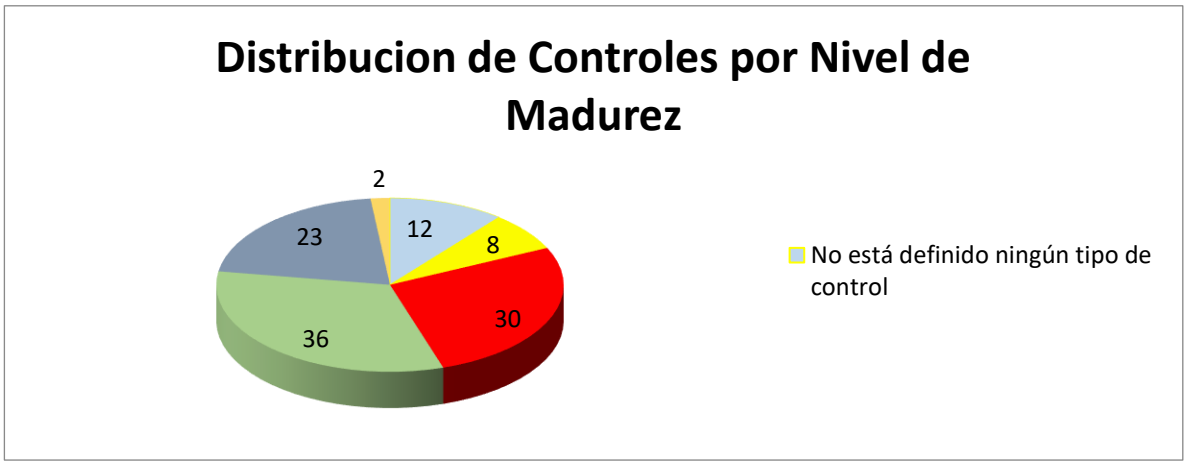
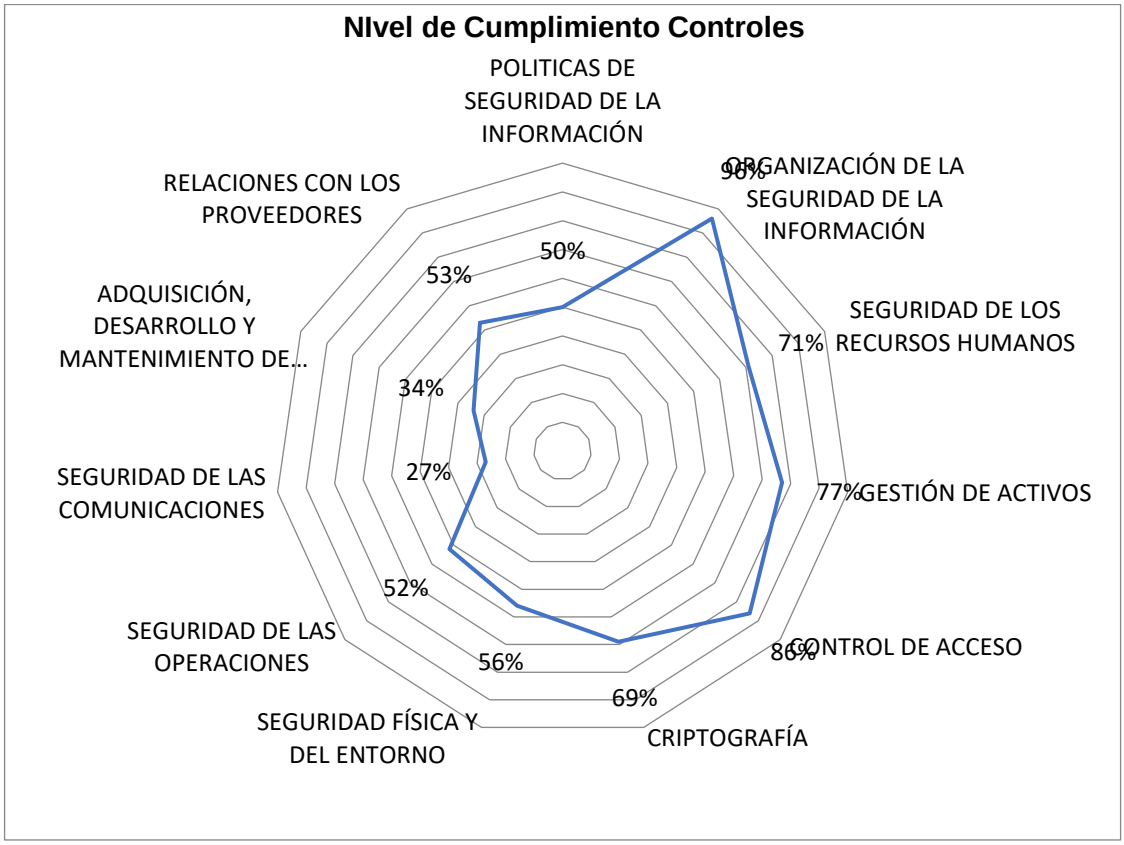


Figura 10 Controles por nivel según su distribución

Figura 11 Nivel de cumplimiento de controles como referencia SGSI



25. **E**NTREGABLE PARA EL INSTITUTO FINANCIERO PARA EL DESARROLLO DEL HUILA INFIHUILA.

El Análisis de gestión de riesgos en la organización **INFIHUILA** parte de la metodología Magerit, que se adapta a la organización. Con la cual se establece el marco para la evaluación de riesgos la cual contiene lo siguiente:

a. Objetivo
b. Alcance
c. Contexto legal
d. Enfoque metodológico
e. Tratamiento También establezca:

Tabla 13 Gestión de Riesgo organización Infihuila

OBJETIVO	Realizar la identificación, análisis y evaluación de los activos y riesgos de seguridad de la información.
ALCANCE	Aplica para los activos de la Empresa INFIHUILA
Nombre de la Empresa:	**Instituto Financiero Para el desarrollo del Huila**
Sitio web:	www.infihuila.gov.co
CONTEXTO LEGAL	NTC ISO/IEC 27001 - NTC ISO/IEC 27005 - NTC ISO/IEC 31000
ENFOQUE METODOLOGICO	El enfoque de gestión de riesgos a aplicar está basado en la metodología **MAGERIT**
TRATAMIENTO	Se tratarán los riesgos cuyos niveles sean:
	[INDIQUE EL NIVEL A TRATAR] **INACEPTABLE**

	Se aceptarán los riesgos cuyo resultado después de la valoración de riesgos sean:
	[INDIQUE EL NIVEL A ACEPTAR] **ADMISIBLE** (3 – 43) **MODERADO** (44 – 104) x
	Niveles de aceptación del riesgo (1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I))
	Una vez aplicados los controles se acepta un riesgo de residual en niveles APRECIABLE o **IMPORTANTE**
	Criticidad residual (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 crítico(C))

Para esta actividad se concentra en los diferentes activos que produce la entidad en cada uno de sus procesos y se toma como referencia la caracterización la cual permite conocer que activos de información producen y que son vitales para la entidad.

a. Clasificación y valoración de los activos de información

La presente tabla clasifica que tipo de información es, si el activo del que sale de un proceso es de clasificación datos, instalación, servicio, software o hardware y así poder realizar su valoración.

Los procesos implicados en el desarrollo de la entidad fueron:

Tabla 14 funcionarios entrevistados del INFIHUILA

ENTREVISTADO	CARGO	RESPONSABILIDADES	PROCESO
Ramiro Rengifo	Profesional Universitario	_contratación, adquisición de bienes y servicios, Nomina, SSGT	De Apoyo
James Parra	Profesional Universitario	Contabilidad, presupuesto, balances, certificados de disponibilidad. etc.	De Apoyo
Ruby Conde	Profesional especializado	Crédito, planeación, indicadores, cartera.	Misional y estratégico.
Mireya Murcia	Auxiliar administrativo	Oficios de Gerencia, Gestión de Archivo, caja menor	De apoyo
William Cedeño	Profesional Universitario	-Convenios, proyectos, administración de fondos especiales.	Misional
Idelber Pabón	Profesional especializado	Control Interno, auditorias	
Arileny Suarez	Auxiliar administrativo	-auxiliar de tesorería, oficios, archivos, verificación de cuentas por pagar.	Misional
Leonardo Martínez	Profesional Universitario	Transferencias bancarias, notas débito, colocación, pagos, ventanilla única, apertura de cuentas y cierre.	Misional
Luis Alfredo Ortega	Gerente	Todo lo referente a la tecnología, Backus, redes, data center, centro alterno, iCloud	Estratégico

Tabla 15 Clasificación y valoración de los activos INFIHUILA

No.	DATOS DEL ACTIVO DE INFORMACION			TIPO									
	Nombre del activo de información	Proceso propietario del activo	Responsable	[D] DATOS	[K] CLAVES CRIPTOGRAFICAS	[S] SERVICIOS	[SW] SOFTWARE	[HW] EQUIPAMENTO	[COM] REDES DE	[Media] SOPORTE DE	[AUX] EQUIPAMENTO AUXILIAR	[L] INSTALACIONES	[P] PERSONAL
1	Bono Pensionales	talento humano	RAMIRO RENGIFO							x			
2	certificados Seguridad Social	talento humano	RAMIRO RENGIFO							x			
3	Comprobantes de Nomina	talento humano	RAMIRO RENGIFO							x			
4	Actas de bienestar	talento humano	RAMIRO RENGIFO							X			
5	Resoluciones	talento humano	RAMIRO RENGIFO							X			
6	Formatos SGST	talento humano	RAMIRO RENGIFO							X			

7	contratos	talento humano	RAMIRO RENGIFO							X			
8	Contraloría INFORMES	talento humano	RAMIRO RENGIFO							X			
9	certificados Cesantías	talento humano	RAMIRO RENGIFO							X			
10	Archivo digital con información contable de la empresa.	Contabilidad	JAMES PARRA DURAN							X			
11	Archivos digitales con información de clientes de la empresa.	Crédito y Cartera	RUBY CONDE							X			
12	Archivo digital con información corporativa. (Actas, Resoluciones, Informes, Procesos de	Gerencia-secretaria gerencia	MIREYA MURCIA							X			

	Administración)												
13	Archivos físicos con información corporativa.	secretaria gerencia	MIREYA MURCIA							X			
14	Archivos físicos de clientes de la empresa.	Gestión Documental	MIREYA MURCIA							X			
15	Archivos físicos de respaldo de la contabilidad. (Libros contables)	contabilidad - gestión documental	JAMES PARRA DURAN							X			
16	Página web	Tecnología	CONTRATISTA APOYO			X							
	PSE	Tecnología	CONTRATISTA APOYO			x							
8	Correo corporativo.	Tecnología	CONTRATISTA APOYO			X							
9	licencia software financiero	Tecnología	CONTRATISTA APOYO		X								
10	Software documental	Tecnología	CONTRATISTA APOYO				X						

12	Auditoria y seguimiento a políticas informáticas	Tecnología	CONTRATISTA APOYO							X			
13	Software de correo corporativo. Outlook	Tecnología	CONTRATISTA APOYO			X							
14	Sistema operativo de los equipos de cómputo - Windows 10	Tecnología	CONTRATISTA APOYO				X						
	soporte a usuarios HD	Tecnología	CONTRATISTA APOYO			x							
15	Suite Office 365	Tecnología	CONTRATISTA APOYO				X						
16	Software antivirus - Kaspersky	Tecnología	CONTRATISTA APOYO				X						
17	Navegador Chrome - Mozilla	Tecnología	CONTRATISTA APOYO				X						

	servidor Base de Datos Oracle			x									
18	Modulo SIINET	Tecnología	CONTRATISTA APOYO				X						
	Modulo IAS	Tecnología	CONTRATISTA APOYO				X						
19	Windows Server 2016-dominio-Directorio Activo	Tecnología	CONTRATISTA APOYO				X						
20	Licencia Oracle	Tecnología	CONTRATISTA APOYO		X								
21	Switches	Tecnología	CONTRATISTA APOYO					x					
22	Computadores.	Tecnología	CONTRATISTA APOYO					x					
23	Impresora/ Scanner.	Tecnología	CONTRATISTA APOYO					x					
24	Huellero biométrico	tecnología	CONTRATISTA APOYO					x					
25	Cámaras de Seguridad	tecnología	CONTRATISTA APOYO					x					

26	Servidor Local Backus	tecnología	CONTRATISTA APOYO					x					
27	Servidor Local Aplicaciones	tecnología	CONTRATISTA APOYO					x					
28	Servidor Local Base de datos	tecnología	CONTRATISTA APOYO					x					
29	UPS	tecnología	CONTRATISTA APOYO					x					
30	Firewall Fortinet	tecnología	CONTRATISTA APOYO					x					
31	Banco de Baterías	tecnología	CONTRATISTA APOYO					x					
32	Celulares corporativos.	tecnología	CONTRATISTA APOYO						x				
33	Red LAN	tecnología	CONTRATISTA APOYO						x				
33	Conexión a internet.	tecnología	CONTRATISTA APOYO						x				
34	Teléfono fijo.	tecnología	CONTRATISTA APOYO						x				
35	VPN.	tecnología	CONTRATISTA APOYO						x				

36	GERENTE	Gerencia-secretaria gerencia	LUIS ALFREDO ORTEGA										X
37	PROFESIONAL ESPECIALIZADO - Control interno	Procesos de Control	IDELBER PABON										X
38	PROFESIONAL UNIVERSITARIO - Tesorería	Tesorería - Inversiones-colocación	LEONARDO MARTINEZ										X
39	PROFESIONAL UNIVERSITARIO - Cartera	Cartera	RUBY CONDE										X
40	PROFESIONAL UNIVERSITARIO - Contratación	gestión de Talento humano y adquisición de bienes y servicios	RAMIRO ENGIFO										X

41	PROFESIONAL UNIVERSITARIO - Apoyo de sistemas	gestión de la tecnología e informática	CONTRATISTA APOYO										X
42	PROFESIONAL UNIVERSITARIO - Convenios	Gestión de Mercadeo	WILLIAM CEDEÑO										X
43	AUXILIAR ADMINISTRATIVO - secretaria, archivo	gestión documental	MIREYA MURCIA										X
44	AUXILIAR ADMINISTRATIVO - servicios generales	Gestión Documental	ARILENY SUAREZ										X
45	PROFESIONAL UNIVERSITARIO - contabilidad	Gestión contabilidad y presupuesto	JAMES PARRA DURAN										X
46	PROFESIONAL	Gestión Jurídica	CONTRATISTA APOYO										X

	UNIVERSITARIO - Apoyo de Jurídica												
47	PROFESIONAL UNIVERSITARIO - Apoyo Financiero	Administración de Fondos especiales	CONTRATISTA APOYO										X
48	PROFESIONAL UNIVERSITARIO - Apoyo planeación - calidad	Planeación y direccionamiento estratégico	CONTRATISTA APOYO										X
49	PROFESIONAL UNIVERSITARIO - Revisoría	Procesos de Control	CONTRATISTA APOYO										X
50	PROFESIONAL UNIVERSITARIO - Riesgos	Gestión del Riesgo	CONTRATISTA APOYO										X
51	PROFESIONAL	gestión de	RAMIRO RENGIFO										X

	UNIVERSITARIO - Talento Humano	Talento humano y adquisición de bienes y servicios											
52	PROFESIONAL UNIVERSITARIO - asesores	Gestión de Mercadeo	WILLIAM CEDEÑO										X
53	Caja de seguridad.	Teoría	LEONARDO MARTINEZ										X
54	Carpetas - cajas	Archivo	MIREYA MURCIA								X		
55	Acetas.	todos los procesos	RAMIRO RENGIFO								X		
56	USB.	contabilidad - gestión documental	RAMIRO RENGIFO							X			
57	CD.	todos los procesos	RAMIRO RENGIFO							X			
58	Acetas para información contable.	contabilidad	JAMES PARRA DURAN							X			

59	Acetas para información de pólizas.	contratación	RAMIRO RENGIFO							X				
60	Acetas con información empresarial.	Gerencia-secretaria gerencia	MIREYA MURCIA							X				
61	Agenda.	Gerencia-secretaria gerencia	MIREYA MURCIA							X				
63	Cl. 10 # 5-05 piso 3 EDIFICIO KOKORIKO, Neiva, Huila	talento humano	RAMIRO RENGIFO										X	
64	centro de Datos	tecnología	CONTRATISTA APOYO										X	

A continuación, se evalúa los diferentes activos de información según su dimensión, proceso de donde proviene el activo, y su responsable, teniendo en cuenta los tres pilares de la seguridad Informática que son Integridad, Confiabilidad y accesibilidad de la Información.

Tabla 16 Datos de los Activo INFIHUILA

No.	DATOS DEL ACTIVO DE INFORMACION			DIMENSION				
	Nombre del activo de información	Proceso propietario del activo	Responsable	Dimensión Autenticidad (B / M /A /	Dimensión Trazabilidad (B / M /A /	Dimensión Confidencialidad (B / M /A / MA/ MB)	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)
1	Bono Pensionales	talento humano	RAMIRO RENGIFO	MA	MA	MA	MA	MA
2	certificados Seguridad Social	talento humano	RAMIRO RENGIFO	A	M	M	A	A
3	Comprobantes de Nomina	talento humano	RAMIRO RENGIFO	MA	M	A	A	A
4	Actas de bienestar	talento humano	RAMIRO RENGIFO	MA	M	M	M	M
5	Resoluciones	talento humano	RAMIRO RENGIFO	A	MA	A	A	M
6	Formatos SGST	talento humano	RAMIRO RENGIFO	A	MA	MA	MA	MA

7	contratos	talento humano	RAMIRO RENGIFO	MA	A	MA	MA	MA
8	Contraloría INFORMES	talento humano	RAMIRO RENGIFO	MA	A	MA	MA	A
9	certificados Cesantías	talento humano	RAMIRO RENGIFO	A	A	A	A	A
10	Archivo digital con información contable de la empresa.	Contabilidad	JAMES PARRA DURAN	MA	A	MA	MA	A
11	Archivos digitales con información de clientes de la empresa.	Crédito y Cartera	RUBY CONDE	MA	A	A	A	A
12	Archivo digital con información corporativa. (Actas, Resoluciones, Informes, Procesos de Administración)	Gerencia-secretaria gerencia	MIREYA MURCIA	MA	A	A	A	A
13	Archivos físicos con	secretaria gerencia	MIREYA MURCIA	A	A	A	A	A

	información corporativa.							
14	Archivos físicos de clientes de la empresa.	Gestión Documental	MIREYA MURCIA	MA	A	MA	MA	A
15	Archivos físicos de respaldo de la contabilidad. (Libros contables)	contabilidad - gestión documental	JAMES PARRA DURAN	MA	A	MA	MA	A
16	Página web	tecnología	CONTRATISTA APOYO	A	A	A	A	A
	PSE	tecnología	CONTRATISTA APOYO	A	A	A	A	A
8	Correo corporativo.	tecnología	CONTRATISTA APOYO	A	M	A	A	A
9	licencia software financiero	tecnología	CONTRATISTA APOYO	A	A	A	A	A
10	Software documental	tecnología	CONTRATISTA APOYO	MA	A	A	MA	A
12	Auditoria y seguimiento a políticas informáticas	tecnología	CONTRATISTA APOYO	A	A	A	A	A
13	Software de correo	tecnología	CONTRATISTA APOYO	A	M	A	A	A

	corporativo. Outlook							
14	Sistema operativo de los equipos de cómputo - Windows 10	tecnología	CONTRATISTA APOYO	A	A	A	A	A
	soporte a usuarios HD	tecnología	CONTRATISTA APOYO	MA	A	A	A	A
15	Suite Office 365	tecnología	CONTRATISTA APOYO	A	A	A	A	A
16	Software antivirus - Kaspersky	tecnología	CONTRATISTA APOYO	A	M	A	A	A
17	Navegador Chrome - Mozilla	tecnología	CONTRATISTA APOYO	MA	A	B	B	B
	servidor Base de Datos Oracle			MA	A	MA	MA	MA
18	Modulo SIINET	tecnología	CONTRATISTA APOYO	MA	MA	A	MA	MA
	Modulo IAS	tecnología	CONTRATISTA APOYO	MA	MA	MA	MA	MA
19	Windows Server 2016-dominio-Directorio Activo	tecnología	CONTRATISTA APOYO	A	M	A	A	MA

20	Licencia Oracle	tecnología	CONTRATISTA APOYO	MA	A	M	MA	MA
21	Switches	tecnología	CONTRATISTA APOYO	MA	A	B	B	A
22	Computadores.	tecnología	CONTRATISTA APOYO	MA	A	A	A	A
23	Impresora/Scanner.	tecnología	CONTRATISTA APOYO	B	MA	B	A	A
24	Huellero biométrico	tecnología	CONTRATISTA APOYO	MA	A	MA	A	A
25	Cámaras de Seguridad	tecnología	CONTRATISTA APOYO	A	A	A	A	A
26	Servidor Local Backus	tecnología	CONTRATISTA APOYO	MA	MA	MA	MA	A
27	Servidor Local Aplicaciones	tecnología	CONTRATISTA APOYO	MA	MA	MA	MA	MA
28	Servidor Local Base de datos	tecnología	CONTRATISTA APOYO	MA	MA	MA	MA	MA
29	UPS	tecnología	CONTRATISTA APOYO	B	A	B	B	A
30	Firewall Fortinet	tecnología	CONTRATISTA APOYO	A	A	A	A	A
31	Banco de Baterías	tecnología	CONTRATISTA APOYO	B	A	B	B	A
32	Celulares corporativos.	tecnología	CONTRATISTA APOYO	B	M	M	M	A

33	Red LAN	tecnología	CONTRATISTA APOYO	A	A	A	A	A
33	Conexión a internet.	tecnología	CONTRATISTA APOYO	B	A	A	B	A
34	Teléfono fijo.	tecnología	CONTRATISTA APOYO	B	A	A	B	A
35	VPN.	tecnología	CONTRATISTA APOYO	A	A	A	A	A
36	GERENTE	Gerencia-secretaria gerencia	LUIS ALFREDO ORTEGA	A	A	A	A	A
37	PROFESIONAL ESPECIALIZADO - Control interno	Procesos de Control	IDELBER PABON	A	A	A	A	A
38	PROFESIONAL UNIVERSITARIO - Tesorería	Tesorería-Inversiones-colocación	LEONARDO MARTINEZ	MA	A	MA	MA	A
39	PROFESIONAL UNIVERSITARIO - Cartera	cartera	RUBY CONDE	A	A	A	A	A
40	PROFESIONAL UNIVERSITA	gestión de Talento humano y adquisición	RAMIRO ENGIFO	MA	A	A	A	MA

	RIO - Contratación	de bienes y servicios						
41	PROFESIONAL UNIVERSITARIO - Apoyo de sistemas	gestión de la tecnología e informática	CONTRATISTA APOYO	A	A	A	A	A
42	PROFESIONAL UNIVERSITARIO - Convenios	Gestión de Mercadeo	WILLIAM CEDEÑO	MA	MA	MA	MA	MA
43	AUXILIAR ADMINISTRATIVO - secretaria, archivo	gestión documental	MIREYA MURCIA	A	A	A	A	A
44	AUXILIAR ADMINISTRATIVO - servicios generales	Gestión Documental	ARILENY SUAREZ	MB	M	M	A	M
45	PROFESIONAL UNIVERSITARIO - contabilidad	Gestión contabilidad y presupuesto	JAMES PARRA DURAN	MA	MA	A	MA	A

46	PROFESIONAL UNIVERSITARIO - Apoyo de Jurídica	Gestión Jurídica	CONTRATISTA APOYO	A	A	A	A	A
47	PROFESIONAL UNIVERSITARIO - Apoyo Financiero	Administración de Fondos especiales	CONTRATISTA APOYO	MA	A	MA	MA	MA
48	PROFESIONAL UNIVERSITARIO - Apoyo planeación - calidad	Planeación y direccionamiento estratégico	CONTRATISTA APOYO	M	M	A	A	A
49	PROFESIONAL UNIVERSITARIO - Revisoría	Procesos de Control	CONTRATISTA APOYO	MA	A	MA	MA	A
50	PROFESIONAL UNIVERSITARIO - Riesgos	Gestión del Riesgo	CONTRATISTA APOYO	A	A	A	A	A
51	PROFESIONAL UNIVERSITA	gestión de Talento humano y adquisición	RAMIRO RENGIFO	MA	M	MA	MA	MA

	RIO - Talento Humano	de bienes y servicios						
52	PROFESIONAL UNIVERSITARIO - asesores	Gestión de Mercadeo	WILLIAM CEDEÑO	M	M	A	A	M
53	Caja de seguridad.	tesorería	LEONARDO MARTINEZ	MA	MA	A	MA	A
54	Carpetas - cajas	Archivo	MIREYA MURCIA	M	A	A	A	A
55	Acetas.	todos los procesos	RAMIRO RENGIFO	B	A	A	A	A
56	USB.	contabilidad - gestión documental	RAMIRO RENGIFO	A	MA	MA	A	M
57	CD.	todos los procesos	RAMIRO RENGIFO	M	M	M	M	MA
58	Acetas para información contable.	contabilidad	JAMES PARRA DURAN	A	A	A	A	A
59	Acetas para información de pólizas.	contratación	RAMIRO RENGIFO	A	A	A	A	A
60	Acetas con información empresarial.	Gerencia-secretaria gerencia	MIREYA MURCIA	A	A	A	A	A

61	Agenda.	Gerencia-secretaria gerencia	MIREYA MURCIA	B	M	M	M	M
63	Cl. 10 # 5-05 piso 3 EDIFICIO KOKORIKO, Neiva, Huila	talento humano	RAMIRO RENGIFO	A	M	M	M	M
64	centro de Datos	tecnología	CONTRATISTA APOYO	MA	MA	MA	MA	MA

Tabla 17 Evaluación de Riesgos de los activos INFIHUILA

METODOLOGÍA PARA LA VALORACIÓN DEL RIESGO EN LOS ACTIVOS DE INFORMACIÓN MAGERIT

Valoración del Riesgo.

PROBABILIDAD DEL RIESGO

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	**Prácticamente seguro**	5
	A	**Probable**	4
	M	**Posible**	3
	B	**Poco probable**	2
	MB	**muy raro**	1

IMPACTO DEL RIESGO

	Nomenclatura	Categoría	Valoración
Impacto	MA	**Muy Alto**	5
	A	**Alto**	4
	M	**Medio**	3
	B	**Bajo**	2
	MB	**Muy Bajo**	1

Figura 12 Valoración del riesgo INFIHUILA

		Insignificante	Menor	Moderado	Mayor	Catastrófico
IMPACTO	MUY ALTA	, R72, R67, R65, R63, R61, R59, R57, R47, R46, R45, R37, R36, R33, R31, R20, R18, R16, R11, R10, R4	, R69, R48, R40, R39, R35, R34, R6	, R56, R55, R52, R51, R50, R49, R44, R43, R41, R29, R28, R26, R23, R22, R8	, R54, R42, R27, R25, R24, R3, R2, R1	, R5
	ALTA					
	MEDIA					
	BAJA					
	MUY BAJA					
RIESGO		MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA

a. Evaluación de los activos frente a sus atributos

Tabla 18 Evaluación de los activos frente a sus atributos

No.	DATOS DEL ACTIVO DE INFORMACION			ATRIBUTOS/Importancia del Activo								
	Nombre del activo de información	Proceso propietario del activo	Responsable	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes o	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:		
										Leve	Importante	Grave

1	Bono Pensionales	talento humano	RAMIRO RENGIFO	s	s	s	s	S	S		X	
2	certificados Seguridad Social	talento humano	RAMIRO RENGIFO	s	s	s	S	S	S		X	
3	Comprobantes de Nomina	talento humano	RAMIRO RENGIFO	N	s	S	N	S	N		X	
4	Actas de bienestar	talento humano	RAMIRO RENGIFO	N	s	S	N	N	N	X		
5	Resoluciones	talento humano	RAMIRO RENGIFO	N	s	N	S	N	N		X	
6	Formatos SGST	talento humano	RAMIRO RENGIFO	N	s	S	N	S	N		X	
7	contratos	talento humano	RAMIRO RENGIFO	S	s	S	S	S	S			X
8	Contraloría INFORMES	talento humano	RAMIRO RENGIFO	S	s	S	S	S	S			X
9	certificados Cesantías	talento humano	RAMIRO RENGIFO	N	s	S	S	N	N			X
10	Archivo digital con información contable de la empresa.	Contabilidad	JAMES PARRA DURAN	S	s	S	S	S	S			X

11	Archivos digitales con información de clientes de la empresa.	Crédito y Cartera	RUBY CONDE	S	s	S	S	S	S		X	
12	Archivo digital con información corporativa. (Actas, Resoluciones, Informes, Procesos de Administración)	Gerencia-secretaria gerencia	MIREYA MURCIA	S	s	S	S	S	S			X
13	Archivos físicos con información corporativa.	secretaria gerencia	MIREYA MURCIA	S	s	S	S	S	S			X

14	Archivos físicos de clientes de la empresa.	Gestión Documental	MIREYA MURCIA	S	S	S	S	S	S			X
15	Archivos físicos de respaldo de la contabilidad. (Libros contables)	contabilidad - gestión documental	JAMES PARRA DURAN	S	s	S	S	S	S			X
16	Página web	Tecnología	CONTRATISTA APOYO	N	N	S	S	N	S	X		
	PSE	Tecnología	CONTRATISTA APOYO	S	s	S	S	S	S			X
8	Correo corporativo.	Tecnología	CONTRATISTA APOYO	N	N	S	S	S	S			X
9	licencia software financiero	Tecnología	CONTRATISTA APOYO	N	S	S	N	S	S			X
10	Software documental	Tecnología	CONTRATISTA APOYO	S	S	S	S	S	S			X
12	Auditoria y seguimiento a políticas	Tecnología	CONTRATISTA APOYO	S	s	S	S	S	S		X	

	informáticas											
13	Software de correo corporativo. Outlook	Tecnología	CONTRATISTA APOYO	S	s	S	S	S	S		X	
14	Sistema operativo de los equipos de cómputo - Windows 10	Tecnología	CONTRATISTA APOYO	N	s	S	S	S	S			X
	soporte a usuarios HD	Tecnología	CONTRATISTA APOYO	N	s	S	S	S	S			X
15	Suite Office 365	Tecnología	CONTRATISTA APOYO	N	N	S	S	S	S			X
16	Software antivirus - Kaspersky	Tecnología	CONTRATISTA APOYO	N	s	S	S	S	S			X
17	Navegador Chrome - Mozilla	Tecnología	CONTRATISTA APOYO	N	N	S	S	S	S		X	
	servidor Base de Datos Oracle			S	s	S	S	S	S			X

18	Modulo SIINET	Tecnología	CONTRATISTA APOYO	S	s	S	S	S	S		X	
	Modulo IAS	Tecnología	CONTRATISTA APOYO	S	s	S	S	S	S			X
19	Windows Server 2016-dominio-Directorio Activo	Tecnología	CONTRATISTA APOYO	N	s	S	S	S	S			X
20	Licencia Oracle	tecnología	CONTRATISTA APOYO	N	s	S	S	S	S			x
21	Switches	tecnología	CONTRATISTA APOYO	N	N	S	S	S	S			x
22	Computadores.	tecnología	CONTRATISTA APOYO	N	N	S	S	S	S			x
23	Impresora/ Scanner.	tecnología	CONTRATISTA APOYO	N	N	S	S	S	S		X	
24	Huellero biométrico	tecnología	CONTRATISTA APOYO	N	S	S	S	S	S			X
25	Cámaras de Seguridad	Tecnología	CONTRATISTA APOYO	N	s	S	S	S	S			X
26	Servidor Local Backus	Tecnología	CONTRATISTA APOYO	S	s	S	S	S	S			X
27	Servidor Local	Tecnología	CONTRATISTA APOYO	S	s	S	S	S	S			X

	Aplicaciones											
28	Servidor Local Base de datos	Tecnología	CONTRATISTA APOYO	S	s	S	S	S	S			X
29	UPS	Tecnología	CONTRATISTA APOYO	N	s	S	S	S	S			X
30	Firewall Fortinet	Tecnología	CONTRATISTA APOYO	N	s	S	S	S	S			X
31	Banco de Baterías	Tecnología	CONTRATISTA APOYO	N	N	S	S	S	S			X
32	Celulares corporativos.	Tecnología	CONTRATISTA APOYO	N	s	S	S	S	S	X		
33	Red LAN	Tecnología	CONTRATISTA APOYO	N	s	S	S	S	S			X
33	Conexión a internet.	Tecnología	CONTRATISTA APOYO	N	s	S	S	S	S			X
34	Teléfono fijo.	Tecnología	CONTRATISTA APOYO	N	N	S	S	S	S	X		
35	VPN.	Tecnología	CONTRATISTA APOYO	S	s	S	S	S	S		X	
36	GERENTE	Gerencia-secretaria gerencia	LUIS ALFREDO ORTEGA	S	s	S	S	S	S			X
37	PROFESIONAL ESPECIALIZADO -	Procesos de Control	IDELBER PABON	S	s	S	S	S	S			X

	Control interno											
38	PROFESIONAL UNIVERSITARIO - Tesorería	Tesorería - Inversiones-colocación	LEONARDO MARTINEZ	S	s	S	S	S	S			X
39	PROFESIONAL UNIVERSITARIO - Cartera	cartera	RUBY CONDE	S	s	S	S	S	S			X
40	PROFESIONAL UNIVERSITARIO - Contratación	gestión de Talento humano y adquisición de bienes y servicios	RAMIRO ENGIFO	S	s	S	S	S	S		X	
41	PROFESIONAL UNIVERSITARIO - Apoyo de sistemas	gestión de la Tecnología e informática	CONTRATISTA APOYO	S	s	S	S	S	S			X
42	PROFESIONAL	Gestión de	WILLIAM CEDEÑO	S	s	S	S	S	S		X	

	UNIVERSITARIO - Convenios	Mercadeo											
43	AUXILIAR ADMINISTRATIVO - secretaria, archivo	gestión documental	MIREYA MURCIA	S	s	S	S	S	S		X		
44	AUXILIAR ADMINISTRATIVO - servicios generales	Gestión Documental	ARILENY SUAREZ	N	N	S	N	N	S		X		
45	PROFESIONAL UNIVERSITARIO – contabilidad	Gestión contabilidad y presupuesto	JAMES PARRA DURAN	S	s	S	S	S	S			X	
46	PROFESIONAL UNIVERSITARIO - Apoyo de Jurídica	Gestión Jurídica	CONTRATISTA APOYO	S	s	S	S	S	S			X	
47	PROFESIONAL UNIVERSITARIO -	Administración de Fondos	CONTRATISTA APOYO	S	s	S	S	S	S			X	

	Apoyo Financiero	especiales										
48	PROFESIONAL UNIVERSITARIO - Apoyo planeación – calidad	Planeación y direccionamiento estratégico	CONTRATISTA APOYO	S	s	S	S	S	S			X
49	PROFESIONAL UNIVERSITARIO – Revisoría	Procesos de Control	CONTRATISTA APOYO	S	s	S	S	S	S			X
50	PROFESIONAL UNIVERSITARIO – Riesgos	Gestión del Riesgo	CONTRATISTA APOYO	S	s	S	S	S	S			X
51	PROFESIONAL UNIVERSITARIO - Talento Humano	gestión de Talento humano y adquisición de bienes y servicios	RAMIRO RENGIFO	S	s	S	S	S	S			X
52	PROFESIONAL	Gestión de	WILLIAM CEDEÑO	S	s	S	S	S	S		X	

	UNIVERSITARIO – asesores	Mercadeo											
53	Caja de seguridad.	teoría	LEONARDO MARTINEZ	S	s	S	S	S	S			X	
54	Carpetas - cajas	Archivo	MIREYA MURCIA	S	s	S	S	S	S			X	
55	Acetas.	todos los procesos	RAMIRO RENGIFO	S	s	S	S	S	S			X	
56	USB.	contabilidad - gestión documental	RAMIRO RENGIFO	S	s	S	S	S	S		X		
57	CD.	todos los procesos	RAMIRO RENGIFO	N	N	S	S	S	S		X		
58	Acetas para información contable.	contabilidad	JAMES PARRA DURAN	S	s	S	S	S	S		X		
59	Acetas para información de pólizas.	contratación	RAMIRO RENGIFO	S	s	S	S	S	S		X		
60	Acetas con información	Gerencia-secretaria gerencia	MIREYA MURCIA	S	s	S	S	S	S		X		

	empresarial.											
61	Agenda.	Gerencia-secretaria gerencia	MIREYA MURCIA	S	s	S	S	S	S		X	
63	Cl. 10 # 5-05 piso 3 EDIFICIO INFIHUILA, Neiva, Huila	talento humano	RAMIRO RENGIFO	S	s	S	S	S	S			X
64	centro de Datos	tecnología	CONTRATISTA APOYO	S	s	S	S	S	S			X

b. Ubicación de los Activos

Tabla 19 Ubicación de los Activos

No.	DATOS DEL ACTIVO DE INFORMACION			UBICACIÓN	
	Nombre del activo de información	Proceso propietario del activo	Responsable	Físico	Electrónico
1	Bono Pensionales	talento humano	RAMIRO RENGIFO		PLATAFORMA CERTICAMARA
2	certificados Seguridad Social	talento humano	RAMIRO RENGIFO		SOFWARE IAS
3	Comprobantes de Nomina	talento humano	RAMIRO RENGIFO		SOFWARE IAS
4	Actas de bienestar	talento humano	RAMIRO RENGIFO	ACETAS	
5	Resoluciones	talento humano	RAMIRO RENGIFO	ACETAS	
6	Formatos SGST	talento humano	RAMIRO RENGIFO		SERVIDOR BAKAUP
7	contratos	talento humano	RAMIRO RENGIFO	ARCHIVO	SERVIDOR BAKAUP

8	Contraloría INFORMES	talento humano	RAMIRO RENGIFO	SERVIDOR BASE DE DATOS	
9	certificados Cesantías	talento humano	RAMIRO RENGIFO	SERVIDOR BASE DE DATOS	
10	Archivo digital con información contable de la empresa.	Contabilidad	JAMES PARRA DURAN		
11	Archivos digitales con información de clientes de la empresa.	Crédito y Cartera	RUBY CONDE		SERVIDOR BAKAUP
12	Archivo digital con información corporativa. (Actas, Resoluciones, Informes, Procesos de Administración)	Gerencia-secretaria gerencia	MIREYA MURCIA		SERVIDOR BAKAUP
13	Archivos físicos con	secretaria gerencia	MIREYA MURCIA	ARCHIVO CENTRAL	

	información corporativa.				
14	Archivos físicos de clientes de la empresa.	Gestión Documental	MIREYA MURCIA	ARCHIVO CENTRAL	
15	Archivos físicos de respaldo de la contabilidad. (Libros contables)	contabilidad - gestión documental	JAMES PARRA DURAN		
16	Página web	tecnología	CONTRATISTA APOYO		SERVIDOR HOSTING
	PSE	tecnología	CONTRATISTA APOYO		PAGINA WEB BANCO
8	Correo corporativo.	tecnología	CONTRATISTA APOYO		SERVIDOR HOSTING
9	licencia software financiero	tecnología	CONTRATISTA APOYO		PENDIENTE
10	Software documental	tecnología	CONTRATISTA APOYO		SERVIDOR-AP
12	Auditoria y seguimiento a políticas informáticas	tecnología	CONTRATISTA APOYO		SERVIDOR BAKUP

13	Software de correo corporativo. Outlook	tecnología	CONTRATISTA APOYO		HOSTING
14	Sistema operativo de los equipos de cómputo - Windows 10	tecnología	CONTRATISTA APOYO	EQUIPOS DE COMPUTO	
	soporte a usuarios HD	tecnología	CONTRATISTA APOYO		WEB
15	Suite Office 365	tecnología	CONTRATISTA APOYO		WEB
16	Software antivirus – Kaspersky	tecnología	CONTRATISTA APOYO		SERVIDOR DE APLICACIONES
17	Navegador Chrome - Mozilla	tecnología	CONTRATISTA APOYO		COMPUTADORES DE COMPUTO
	servidor Base de Datos Oracle			DATA-CENTER	
18	Modulo SIINET	tecnología	CONTRATISTA APOYO		SERVIDOR DE APLICACIONES

	Modulo IAS	tecnología	CONTRATISTA APOYO		SERVIDOR APLICACONES
19	Windows Server 2016-dominio-Directorio Activo	tecnología	CONTRATISTA APOYO		SERVIDOR DE DOMINIO
20	Licencia Oracle	tecnología	CONTRATISTA APOYO		
21	Switches	tecnología	CONTRATISTA APOYO	DATA-CENTER	
22	Computadores.	tecnología	CONTRATISTA APOYO	ESTACIONES DE TRABAJO	
23	Impresora/Scanner.	tecnología	CONTRATISTA APOYO	ESTACIONES DE TRABAJO	
24	Huellero biométrico	tecnología	CONTRATISTA APOYO	DATA-CENTER, TERCER PISO	
25	Cámaras de Seguridad	tecnología	CONTRATISTA APOYO	EN DIFERENTES AREAS DE TRABAJO.	
26	Servidor Local Backus	tecnología	CONTRATISTA APOYO	DATA CENTER	

27	Servidor Local Aplicaciones	tecnología	CONTRATISTA APOYO	DATA CENTER	
28	Servidor Local Base de datos	tecnología	CONTRATISTA APOYO	DATA CENTER	
29	UPS	tecnología	CONTRATISTA APOYO	DATA CENTAR	
30	Firewall Fortinet	tecnología	CONTRATISTA APOYO	DATA CENTER	
31	Banco de Baterías	tecnología	CONTRATISTA APOYO	DATA CENTAR	
32	Celulares corporativos.	tecnología	CONTRATISTA APOYO	SERCRETARIA-GERENCIA	
33	Red LAN	tecnología	CONTRATISTA APOYO	EDIFICIO 3-4 PISO	
33	Conexión a internet.	tecnología	CONTRATISTA APOYO	DATA CENTER	
34	Teléfono fijo.	tecnología	CONTRATISTA APOYO	ESTACIONES DE TRABAJO	
35	VPN.	tecnología	CONTRATISTA APOYO		FIREWALL
36	GERENTE	Gerencia-secretaria gerencia	LUIS ALFREDO ORTEGA	GERENCIA	
37	PROFESIONAL	Procesos de Control	IDELBER PABON	CONTROL-INTERNO	

	ESPECIALIZADO - Control interno				
38	PROFESIONAL UNIVERSITARIO - Tesorería	Tesorería-Inversiones-colocación	LEONARDO MARTINEZ	TESORERIA	
39	PROFESIONAL UNIVERSITARIO – Cartera	cartera	RUBY CONDE	AREA DE CARTERA	
40	PROFESIONAL UNIVERSITARIO - Contratación	gestión de Talento humano y adquisición de bienes y servicios	RAMIRO ENGIFO	AREA TALENTO HUMANO	
41	PROFESIONAL UNIVERSITARIO - Apoyo de sistemas	gestión de la tecnología e informática	CONTRATISTA APOYO	AREA DE SISTEMAS	
42	PROFESIONAL UNIVERSITARIO - Convenios	Gestión de Mercadeo	WILLIAM CEDEÑO	AREA DE CONVENIOS	

43	AUXILIAR ADMINISTRATIVO - secretaria, archivo	gestión documental	MIREYA MURCIA	AREA GERENCIA-SECRETARIA	
44	AUXILIAR ADMINISTRATIVO - servicios generales	Gestión Documental	ARILENY SUAREZ	AREA ADMINISTRATIVA	
45	PROFESIONAL UNIVERSITARIO - contabilidad	Gestión contabilidad y presupuesto	JAMES PARRA DURAN	AREA CONTABILIDAD	
46	PROFESIONAL UNIVERSITARIO - Apoyo de Jurídica	Gestión Jurídica	CONTRATISTA APOYO	AREA JURIDICA	
47	PROFESIONAL UNIVERSITARIO - Apoyo Financiero	Administración de Fondos especiales	CONTRATISTA APOYO	AREA FINANCIERA	
48	PROFESIONAL UNIVERSITARIO - Apoyo	Planeación y direccionam	CONTRATISTA APOYO	AREA PLANEACION	

	planeación – calidad	iento estratégico			
49	PROFESIONAL UNIVERSITARIO - Revisoría	Procesos de Control	CONTRATISTA APOYO	AREA REVISRORIA	
50	PROFESIONAL UNIVERSITARIO – Riesgos	Gestión del Riesgo	CONTRATISTA APOYO	AREA RIESGO	
51	PROFESIONAL UNIVERSITARIO - Talento Humano	gestión de Talento humano y adquisición de bienes y servicios	RAMIRO RENGIFO	AREA TALENTO HUMANO	
52	PROFESIONAL UNIVERSITARIO - asesores	Gestión de Mercadeo	WILLIAM CEDEÑO	AREA ASESORES	
53	Caja de seguridad.	teoría	LEONARDO MARTINEZ	AREA TESORERIA	
54	Carpetas - cajas	Archivo	MIREYA MURCIA	ARCHIVO CENTRAL	

55	Acetas.	todos los procesos	RAMIRO RENGIFO	ESTACIONES DE TRABAJO	
56	USB.	contabilidad - gestión documental	RAMIRO RENGIFO	FUNCIONARIOS DEL INSTITUTO	
57	CD.	todos los procesos	RAMIRO RENGIFO	FUNCIONARIOS DEL INSTITUTO	
58	Acetas para información contable.	contabilidad	JAMES PARRA DURAN	AREAS DE TRABAJO	
59	Acetas para información de pólizas.	contratación	RAMIRO RENGIFO	CONTRATACION	
60	Acetas con información empresarial.	Gerencia-secretaria gerencia	MIREYA MURCIA	CONTRATACION-ARCHIVO	AREA JURIDICA
61	Agenda.	Gerencia-secretaria gerencia	MIREYA MURCIA	SECRETARIA GERENCIA	
63	Cl. 10 # 5-05 piso 3 EDIFICIO KOKORIKO, Neiva, Huila	talento humano	RAMIRO RENGIFO	CENTRO-NEIVA	
64	centro de Datos	Tecnología	CONTRATISTA APOYO	4 PISO.	

d. Valoración cuantitativa de la evaluación de riesgos de los activos:

Tabla 20 **Valoración de los Activos**

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
Bono Pensionales	CRITICO	25	25	25	25	25	25
certificados Seguridad Social	IMPORTANTE	20	15	15	20	20	18
Comprobantes de Nomina	IMPORTANTE	25	15	20	20	20	20
Actas de bienestar	IMPORTANTE	25	15	15	15	15	17
Resoluciones	IMPORTANTE	20	25	20	20	15	20
Formatos SGST	CRITICO	20	25	25	25	25	24
contratos	CRITICO	25	20	25	25	25	24
Contraloría INFORMES	CRITICO	25	20	25	25	20	23
certificados Cesantías	IMPORTANTE	20	20	20	20	20	20

Archivo digital con información contable de la empresa.	CRITICO	25	20	25	25	20	23
Archivos digitales con información de clientes de la empresa.	CRITICO	25	20	20	20	20	21
Archivo digital con información corporativa. (Actas, Resoluciones, Informes, Procesos de Administración)	CRITICO	25	20	20	20	20	21
Archivos físicos con información corporativa.	IMPORTANTE	20	20	20	20	20	20
Archivos físicos de clientes de la empresa.	CRITICO	25	20	25	25	20	23
Archivos físicos de respaldo de la contabilidad. (Libros contables)	CRITICO	25	20	25	25	20	23
Página web	IMPORTANTE	20	20	20	20	20	20
PSE	IMPORTANTE	20	20	20	20	20	20
Correo corporativo.	IMPORTANTE	20	15	20	20	20	19

licencia software financiero	IMPORTANTE	20	20	20	20	20	20
Software documental	CRITICO	25	20	20	25	20	22
Auditoria y seguimiento a políticas informáticas	IMPORTANTE	20	20	20	20	20	20
Software de correo corporativo. Outlook	IMPORTANTE	20	15	20	20	20	19
Sistema operativo de los equipos de cómputo - Windows 10	IMPORTANTE	20	20	20	20	20	20
soporte a usuarios HD	CRITICO	25	20	20	20	20	21
Suite Office 365	IMPORTANTE	20	20	20	20	20	20
Software antivirus - Kaspersky	IMPORTANTE	20	15	20	20	20	19
Navegador Chrome - Mozilla	APRECIABLE	25	20	9	9	9	14
servidor Base de Datos Oracle	CRITICO	25	20	25	25	25	24
Modulo SIINET	CRITICO	25	25	20	25	25	24

Modulo IAS	CRITICO	25	25	25	25	25	25
Windows Server 2016-dominio-Directorio Activo	IMPORTANTE	20	15	20	20	25	20
Licencia Oracle	CRITICO	25	20	15	25	25	22
Switches	IMPORTANTE	25	20	9	9	20	17
Computadores.	CRITICO	25	20	20	20	20	21
Impresora/Scanner.	IMPORTANTE	9	25	9	20	20	17
Huellero biométrico	CRITICO	25	20	25	20	20	22
Cámaras de Seguridad	IMPORTANTE	20	20	20	20	20	20
Servidor Local Backus	CRITICO	25	25	25	25	20	24
Servidor Local Aplicaciones	CRITICO	25	25	25	25	25	25
Servidor Local Base de datos	CRITICO	25	25	25	25	25	25
UPS	APRECIABLE	9	20	9	9	20	13

Firewall Fortinet	IMPORTANTE	20	20	20	20	20	20
Banco de Baterías	APRECIABLE	9	20	9	9	20	13
Celulares corporativos.	APRECIABLE	9	15	15	15	20	15
Red LAN	IMPORTANTE	20	20	20	20	20	20
Conexión a internet.	IMPORTANTE	9	20	20	9	20	16
Teléfono fijo.	IMPORTANTE	9	20	20	9	20	16
VPN.	IMPORTANTE	20	20	20	20	20	20
GERENTE	IMPORTANTE	20	20	20	20	20	20
PROFESIONAL ESPECIALIZADO - Control interno	IMPORTANTE	20	20	20	20	20	20

PROFESIONAL UNIVERSITARIO – Tesorería	CRITICO	25	20	25	25	20	23
PROFESIONAL UNIVERSITARIO – Cartera	IMPORTANTE	20	20	20	20	20	20
PROFESIONAL UNIVERSITARIO – Contratación	CRITICO	25	20	20	20	25	22
PROFESIONAL UNIVERSITARIO - Apoyo de sistemas	IMPORTANTE	20	20	20	20	20	20
PROFESIONAL UNIVERSITARIO – Convenios	CRITICO	25	25	25	25	25	25
AUXILIAR ADMINISTRATIVO - secretaria, archivo	IMPORTANTE	20	20	20	20	20	20
AUXILIAR ADMINISTRATIVO - servicios generales	APRECIABLE	4	15	15	20	15	14
PROFESIONAL UNIVERSITARIO – contabilidad	CRITICO	25	25	20	25	20	23
PROFESIONAL UNIVERSITARIO - Apoyo de Jurídica	IMPORTANTE	20	20	20	20	20	20

PROFESIONAL UNIVERSITARIO - Apoyo Financiero	CRITICO	25	20	25	25	25	24
PROFESIONAL UNIVERSITARIO - Apoyo planeación – calidad	IMPORTANTE	15	15	20	20	20	18
PROFESIONAL UNIVERSITARIO – Revisoría	CRITICO	25	20	25	25	20	23
PROFESIONAL UNIVERSITARIO – Riesgos	IMPORTANTE	20	20	20	20	20	20
PROFESIONAL UNIVERSITARIO - Talento Humano	CRITICO	25	15	25	25	25	23
PROFESIONAL UNIVERSITARIO – asesores	IMPORTANTE	15	15	20	20	15	17
Caja de seguridad.	CRITICO	25	25	20	25	20	23
Carpetas -cajas	IMPORTANTE	15	20	20	20	20	19
Acetas.	IMPORTANTE	9	20	20	20	20	18
USB.	CRITICO	20	25	25	20	15	21

CD.	IMPORTANTE	15	15	15	15	25	17
Acetas para información contable.	IMPORTANTE	20	20	20	20	20	20
Acetas para información de pólizas.	IMPORTANTE	20	20	20	20	20	20
Acetas con información empresarial.	IMPORTANTE	20	20	20	20	20	20
Agenda.	APRECIABLE	9	15	15	15	15	14
Cl. 10 # 5-05 piso 3 EDIFICIO KOKORIKO, Neiva, Huila	IMPORTANTE	20	15	15	15	15	16
centro de Datos	CRITICO	25	25	25	25	25	25

Una vez realizado el levantamiento de Activos según como lo indica la ISO27001:2013, se le da un valor cuantitativo, valorando los activos más críticos de la entidad en la cual se considera los más importantes, así mismo monitoreando su impacto, y fortaleciendo la infraestructura de un posible riesgo.

Una vez realizado dicho proceso se determinan las amenazas y posibles vulnerabilidades de la siguiente manera:

c. Determinación de Amenazas y vulnerabilidades

Tabla 21 Determinación de Amenazas y vulnerabilidades

No. De Amenazas y [illegible]	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades
1	Bono Pensionales	25	[E1] Errores de los usuarios	Información errónea
2	certificados Seguridad Social	18	[A15] Modificación deliberada de la información	bloqueo
3	Comprobantes de Nomina	20	[E18] Destrucción de información	robo de información
4	Actas de bienestar	17	[E18] Destrucción de información	beneficio a un tercero, perdida de información
5	Resoluciones	20	[E1] Errores de los usuarios	inactividad de procesos
6	Formatos SGST	24	[A15] Modificación deliberada de la información	Datos alterados
7	contratos	24	[A15] Modificación deliberada de la información	daño corporativo, imagen

8	Contraloría INFORMES	23	[A5] Suplantación de la identidad del usuario	robo de información
9	certificados Cesantías	20	[A15] Modificación deliberada de la información	retraso en las operaciones, funciones.
10	Archivo digital con información contable de la empresa.	23	[A25] Robo	robo de información
11	Archivos digitales con información de clientes de la empresa.	21	[E14] Escapes de información	información errónea
12	Archivo digital con información corporativa. (Actas, Resoluciones, Informes, Procesos de Administración)	21	[A15] Modificación deliberada de la información	retraso de procesos
13	Archivos físicos con información corporativa.	20	[E14] Escapes de información	manipulación de información para su propio beneficio
14	Archivos físicos de clientes de la empresa.	23	[A15] Modificación deliberada de la información	manipulación de información para su propio beneficio
15	Archivos físicos de respaldo de la contabilidad. (Libros contables)	23	[A7] Uso no previsto	retraso de procesos

16	Página web	20	[E24] Caída del sistema por agotamiento de recursos	retrasos de procesos
17	PSE	20	[E14] Escapes de información	Usuarios insatisfechos
18	Correo corporativo.	19	[E1] Errores de los usuarios	información poco confiable
19	licencia software financiero	20	[E8] Difusión de software dañino	foro de información
20	Software documental	22	[E20] Vulnerabilidades de los programas (software)	robo de información
21	Auditoria y seguimiento a políticas informáticas	20	[E14] Escapes de información	historial de la entidad
22	Software de correo corporativo. Outlook	19	[E19] Fugas de información	manipulación de información para su propio beneficio
23	Sistema operativo de los equipos de cómputo - Windows 10	20	[E4] Errores de configuración	usuario insatisfecho
24	soporte a usuarios HD	21	[A24] Denegación de servicio	retrasos de procesos
25	Suite Office 365	20	[E24] Caída del sistema por agotamiento de recursos	integridad de los datos

26	Software antivirus - Kaspersky	19	[A26] Ataque destructivo	información poco confiable
27	Navegador Chrome - Mozilla	14	[A26] Ataque destructivo	robo de información
28	servidor Base de Datos Oracle	24	[A18] Destrucción de información	robo de información
29	Modulo SIINET	24	[A6] Abuso de privilegios de acceso	retrasos de procesos
30	Modulo IAS	25	[E14] Escapes de información	información poco confiable
31	Windows Server 2016-dominio-Directorio Activo	20	[E4] Errores de configuración	información poco confiable
32	Licencia Oracle	22	[E20] Vulnerabilidades de los programas (software)	información poco confiable
33	Switches	17	[E4] Errores de configuración	información poco confiable
34	Computadores.	21	[A5] Suplantación de la identidad del usuario	manipulación de información para su propio beneficio
35	Impresora/Scanner.	17	[E14] Escapes de información	retraso de procesos
36	Huellero biométrico	22	[E4] Errores de configuración	foro de informaron
37	Cámaras de Seguridad	20	[A24] Denegación de servicio	manipulación de información para

				su propio beneficio
38	Servidor Local Backus	24	[E18] Destrucción de información	retrasos de procesos
39	Servidor Local Aplicaciones	25	[E3] Errores de monitorización (log)	Usuarios insatisfechos
40	Servidor Local Base de datos	25	[E18] Destrucción de información	Usuarios insatisfechos
41	UPS	13	[E24] Caída del sistema por agotamiento de recursos	robo de información
42	Firewall Fortinet	20	[E19] Fugas de información	manipulación accidental información para su propio beneficio
43	Banco de Baterías	13	[I6] Corte del suministro eléctrico	retrasos accidental procesos
44	Celulares corporativos.	15	[I8] Fallo de servicios de comunicaciones	retrasos de procesos
45	Red LAN	20	[I8] Fallo de servicios de comunicaciones	daño corporativo, margen

46	Conexión a internet.	16	[I8] Fallo de servicios de comunicaciones	información poco confiable
22	Teléfono fijo.	16	[I8] Fallo de servicios de comunicaciones	Información poco confiable
23	VPN.	20	[I8] Fallo de servicios de comunicaciones	roro de información
24	GERENTE	20	[A6] Abuso de privilegios de acceso	Información utilizada para beneficiar un tercero
25	PROFESIONAL ESPECIALIZADO - Control interno	20	[E19] Fugas de información	claves débiles
26	PROFESIONAL UNIVERSITARIO - Tesorería	23	[A19] Divulgación de información	el no cambio de claves
27	PROFESIONAL UNIVERSITARIO - Cartera	20	[A15] Modificación deliberada de la información	muchas conexiones
28	PROFESIONAL UNIVERSITARIO - Contratación	22	[A15] Modificación deliberada de la información	beneficio s un tercero
29	PROFESIONAL UNIVERSITARIO - Apoyo de sistemas	20	[E2] Errores del administrador	beneficio I un tercero

30	PROFESIONAL UNIVERSITARIO - Convenios	25	[E14] Escapes de información	manipulación de información para su propio beneficio
31	AUXILIAR ADMINISTRATIVO - secretaria, archivo	20	[A30] Ingeniería social (picaresca)	información poco confiable
32	AUXILIAR ADMINISTRATIVO - servicios generales	14	[A30] Ingeniería social (picaresca)	información poco confiable
33	PROFESIONAL UNIVERSITARIO - contabilidad	23	[E15] Alteración accidental de la información	información poco confiable
34	PROFESIONAL UNIVERSITARIO - Apoyo de Jurídica	20	[E18] Destrucción de información	robo de información
35	PROFESIONAL UNIVERSITARIO - Apoyo Financiero	24	[A30] Ingeniería social (picaresca)	robo de información
36	PROFESIONAL UNIVERSITARIO - Apoyo planeación - calidad	18	[E15] Alteración accidental de la información	represión de tareas
37	PROFESIONAL UNIVERSITARIO - Revisoría	23	[A15] Modificación deliberada de la información	represión de tareas
38	PROFESIONAL UNIVERSITARIO - Riesgos	20	[A18] Destrucción de información	represión de tareas

39	PROFESIONAL UNIVERSITARIO - Talento Humano	23	[A30] Ingeniería social (picaresca)	represión de tareas
40	PROFESIONAL UNIVERSITARIO - asesores	17	[E14] Escapes de información	represión de tareas
41	Caja de seguridad.	23	[A25] Robo	represión de tareas
42	Carpetas -cajas	19	[A18] Destrucción de información	represión de tareas
43	Acetas.	18	[A18] Destrucción de información	represión de tareas
44	USB.	21	[A25] Robo	represión de tareas
45	CD.	17	[A25] Robo	represión de tareas
46	Acetas para información contable.	20	[A15] Modificación deliberada de la información	represión de tareas
47	Acetas para información de pólizas.	20	[A15] Modificación deliberada de la información	represión de tareas
23	Acetas con información empresarial.	20	[A15] Modificación deliberada de la información	represión de tareas
24	Agenda.	14	[E14] Escapes de información	represión de tareas

25	Cl. 10 # 5-05 piso 3 EDIFICIO KOKORIKO, Neiva, Huila	16	[N*] Desastres naturales	represión de tareas
26	centro de Datos	25	[I2] Daños por agua	represión de tareas

d. Propuesta para la gestión del riesgo (Plan de tratamiento de riesgos)

Una vez analizado las amenazas y vulnerabilidades se procede al tratamiento de riesgo con su posible control

Tabla 22 Tratamiento de Riesgos

No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Plan de Tratamiento de Riesgos Sugeridos
1	Comprobantes de Nomina	20	usuario con autenticación.
2	Actas de bienestar	17	digitalización de archivo con copias

3	Resoluciones	20	digitalización de archivo con copias
4	Formatos SGST	24	Copia de los formatos servidor de copias
5	certificados Cesantías	20	autenticación con criptografía
6	Página web	20	usuario con autenticación. Privilegios de administrador
7	Correo corporativo.	19	Antivirus, protocolo de certificación
8	licencia software financiero	20	certificados con números de Licencia y fecha de vencimiento
9	Sistema operativo de los equipos de cómputo - Windows 10	20	actualización de los sistemas operativos.
10	soporte a usuarios HD	21	políticas de seguridad, servicio de soporte activo, usuario con privilegios
11	Módulos SIINET	24	personal idóneo, soporte activo.
12	Suite Office 365	20	actualización de licencias, presupuesto

13	Software antivirus – Kaspersky	19	monitoreo de procesos
14	Navegador Chrome – Mozilla	14	actualización de los navegadores.
15	Windows Server 2016-dominio-Directorio Activo	20	monitoreo continuo de capacidad, procedimiento, formato.
16	Licencia Oracle	22	licencias Activas x usuario y actualizaciones de seguridad.
17	Switches	17	aumento de velocidad de canal
18	Computadores.	21	capacitación de usuarios, mantenimientos preventivos-cronograma
19	Impresora/Scanner.	17	capacitación de usuarios, mantenimientos preventivos-cronograma
20	Huellero biométrico	22	usuarios con privilegios, autorizados.
21	Cámaras de Seguridad	20	procedimiento, monitoreo de

			cámaras. - planta eléctrica
22	UPS	13	configuración de políticas y alertas temprano
23	Firewall Fortinet	20	Monitero tráfico de red
24	Banco de Baterías	13	servidores de prueba
25	Celulares corporativos.	15	Auditorias contables
26	Red LAN	20	licenciamiento y actualizaciones
27	Conexión a internet.	16	configuración de seguridad de la base de datos
28	Teléfono fijo.	16	configuración de parches de seguridad
29	AUXILIAR ADMINISTRATIVO - servicios generales	14	configuración de parches de seguridad
30	CD.	17	Contratar personal experto
31	Bono Pensionales	25	Contratar personal experto
32	certificados Seguridad Social	18	Contratar personal experto
33	contratos	24	Contratar personal experto

34	Contraloría INFORMES	23	cronograma de actividades
35	Archivo digital con información contable de la empresa.	23	capacitación del usuario
36	Archivos digitales con información de clientes de la empresa.	21	capacitación del usuario
37	Archivo digital con información corporativa. (Actas, Resoluciones, Informes, Procesos de Administración)	21	capacitación del usuario
38	Archivos físicos con información corporativa.	20	capacitación del usuario
39	Archivos físicos de clientes de la empresa.	23	mantenimiento de equipos
40	Archivos físicos de respaldo de la contabilidad. (Libros contables)	23	capacitación del usuario
41	PSE	20	Digitalización de documentos con copia en la nube
42	Software documental - SIINET	22	Digitalización de documentos con copia en la nube

43	Auditoria y seguimiento a políticas informáticas	20	configuración de seguridad, contraseñas, y sistema de cifrado
44	Software de correo corporativo. Outlook	19	políticas de seguridad
45	Base de Datos SIINET	25	políticas de seguridad
46	servidor Base de Datos Oracle	24	políticas de seguridad
47	Modulo SIINET	24	Digitalización de documentos con copia en la nube
48	Modulo IAS	25	políticas de seguridad
49	Servidor Local Backus	24	políticas de seguridad
50	Servidor Local Aplicaciones	25	políticas de seguridad
51	Servidor Local Base de datos	25	políticas de seguridad
52	VPN.	20	políticas de seguridad
53	GERENTE	20	configuración de políticas de seguridad
54	PROFESIONAL ESPECIALIZADO - Control interno	20	políticas de seguridad

55	PROFESIONAL UNIVERSITARIO - Tesorería	23	monitoreo de red de test de velocidad
56	PROFESIONAL UNIVERSITARIO - Cartera	20	cronograma de mantenimientos
57	PROFESIONAL UNIVERSITARIO - Contratación	22	actualización de aplicativo
58	PROFESIONAL UNIVERSITARIO - Apoyo de sistemas	20	equipos de contingencia
59	PROFESIONAL UNIVERSITARIO - Convenios	25	certificación de puntos cableado
60	AUXILIAR ADMINISTRATIVO - secretaria, archivo	20	centro alterno
61	PROFESIONAL UNIVERSITARIO - contabilidad	23	herramientas de contingencia
62	PROFESIONAL UNIVERSITARIO - Apoyo de Jurídica	20	herramientas de contingencia
63	PROFESIONAL UNIVERSITARIO - Apoyo Financiero	24	herramientas de contingencia
64	PROFESIONAL UNIVERSITARIO -	18	herramientas de contingencia

	Apoyo planeación - calidad		
65	PROFESIONAL UNIVERSITARIO - Revisoría	23	herramientas de contingencia
66	PROFESIONAL UNIVERSITARIO - Riesgos	20	herramientas de contingencia
67	PROFESIONAL UNIVERSITARIO - Talento Humano	23	herramientas de contingencia
68	PROFESIONAL UNIVERSITARIO - asesores	17	herramientas de contingencia
69	Caja de seguridad.	23	herramientas de contingencia
70	Carpetas -cajas	19	herramientas de contingencia
71	Acetas.	18	herramientas de contingencia
72	USB.	21	herramientas de contingencia
73	Acetas para información contable.	20	herramientas de contingencia
74	Acetas para información de pólizas.	20	herramientas de contingencia
75	Acetas con información empresarial.	20	herramientas de contingencia

76	Agenda.	14	herramientas de contingencia
77	Cl. 10 # 5-05 piso 3 EDIFICIO INFIHUILA, Neiva, Huila	16	herramientas de contingencia
78	centro de Datos	25	centro alterno - contingencia
79	MECANEIVA-HISTORIAL DE ARCHIVO	25	digitalización de archivos y resguardado en la nube
80	centro de Datos-Alterno Local	25	centro alterno iCloud

26. RESUMEN EJECUTIVO

El resultado final de la valoración del riesgo al que está expuesto cada activo depende de la suma de la probabilidad VS el impacto de la tabla anterior. El cálculo se basa en todo lo recogido durante las entrevistas y el cómputo de la pestaña "Inventario y Valoración de Activos" contra la tabla de valoración del riesgo. Obteniendo el siguiente resumen:

CLASIFICACION DE ACTIVOS

Tabla 23 clasificación de los Activos

Clasificación general y Número de activos	
Tipo de activo	**Cantidad**
Tipo Dato	2
Tipo Aplicación	9
Tipo Personal	18
Tipo Instalación	4
Tipo Servicio	5
Tipo Tecnología	11
Tipo Redes Comunicación	5
Tipo soporte Información	22
Tipo Equipamiento auxiliar	2
Tipo Criptografía	2
	80

CLASIFICACION SEGÚN SU IMPACTO A LA SEGURIDAD

Tabla 24 clasificación según su impacto a la seguridad

Clasificación según impacto a la seguridad	
Leve	4
Importante	23
Grave	53

CLASIFICACION DE ACTIVOS SEGÚN SU VALOR

Tabla 25 clasificación según su valor

Número de activos de clientes o terceros que deben protegerse	51
Activos de información que deben ser restringidos a un número limitado de empleados	69
Número de activos de información que deben ser restringidos a personas externas	79
Activos de información que pueden ser alterados o comprometidos para fraudes o corrupción	75
Número de activos de información que son muy críticos para las operaciones internas	75
Número de activos de información que son muy críticos para el servicio hacia terceros	75

RESUMEN DE VALORACION DE LOS ACTIVOS EN ESCALA

Tabla 26 Resumen de la Valoración de Activos en escala

Nombre	Riesgo	Confidencialidad	Integridad	Disponibilidad	Valor
Comprobantes de Nomina	ALTO	6	6	6	6
Resoluciones	ALTO	6	6	5	6
certificados Cesantías	ALTO	6	6	6	6
Página web	ALTO	6	6	6	6
Correo corporativo.	ALTO	6	6	6	6
licencia software financiero	ALTO	6	6	6	6
Sistema operativo de los equipos de cómputo - Windows 10	ALTO	6	6	6	6
soporte a usuarios HD	ALTO	6	6	6	6
Módulos SIINET	ALTO	6	6	6	6
Suite Office 365	ALTO	6	6	6	6
Navegador Chrome - Mozilla	ALTO	6	6	9	7
Switches	ALTO	6	6	6	6
Impresora/Scanner.	ALTO	9	6	6	7
Huellero biométrico	ALTO	6	6	6	6
UPS	ALTO	6	6	6	6
Celulares corporativos.	ALTO	6	6	6	6
AUXILIAR ADMINISTRATIVO - servicios generales	ALTO	5	5	9	6
Bono Pensionales	ALTO	5	6	6	6
Archivo digital con información contable de la empresa.	ALTO	6	6	6	6
Archivos digitales con información de clientes de la empresa.	ALTO	6	6	6	6
Archivo digital con información corporativa. (Actas, Resoluciones, Informes, Procesos de Administración)	ALTO	6	6	6	6
Archivos físicos de respaldo de la contabilidad. (Libros contables)	ALTO	6	6	6	6
PSE	ALTO	6	9	6	7
Software documental – SIINET	ALTO	6	6	6	6
Auditoria y seguimiento a políticas informáticas	ALTO	6	6	6	6
Servidor Local Aplicaciones	ALTO	6	6	6	6

Servidor Local Base de datos	ALTO	6	6	6	6
VPN.	ALTO	6	6	6	6
PROFESIONAL ESPECIALIZADO - Control interno	ALTO	6	6	6	6
PROFESIONAL UNIVERSITARIO - Tesorería	ALTO	6	6	9	7
PROFESIONAL UNIVERSITARIO - Cartera	ALTO	6	6	6	6
PROFESIONAL UNIVERSITARIO - Apoyo de sistemas	ALTO	6	6	6	6
PROFESIONAL UNIVERSITARIO - Convenios	ALTO	6	9	6	7
AUXILIAR ADMINISTRATIVO - secretaria, archivo	ALTO	6	6	6	6
PROFESIONAL UNIVERSITARIO - Apoyo de Jurídica	ALTO	6	6	6	6
PROFESIONAL UNIVERSITARIO - Apoyo planeación – calidad	ALTO	6	6	6	6
PROFESIONAL UNIVERSITARIO - Riesgos	ALTO	6	6	5	6
PROFESIONAL UNIVERSITARIO - Talento Humano	ALTO	6	9	6	7
PROFESIONAL UNIVERSITARIO - asesores	ALTO	6	6	6	6
Caja de seguridad.	ALTO	6	6	6	6
Carpetas -cajas	ALTO	9	6	5	7
Acetas.	ALTO	6	6	6	6
USB.	ALTO	6	6	6	6
Acetas para información contable.	ALTO	6	6	6	6

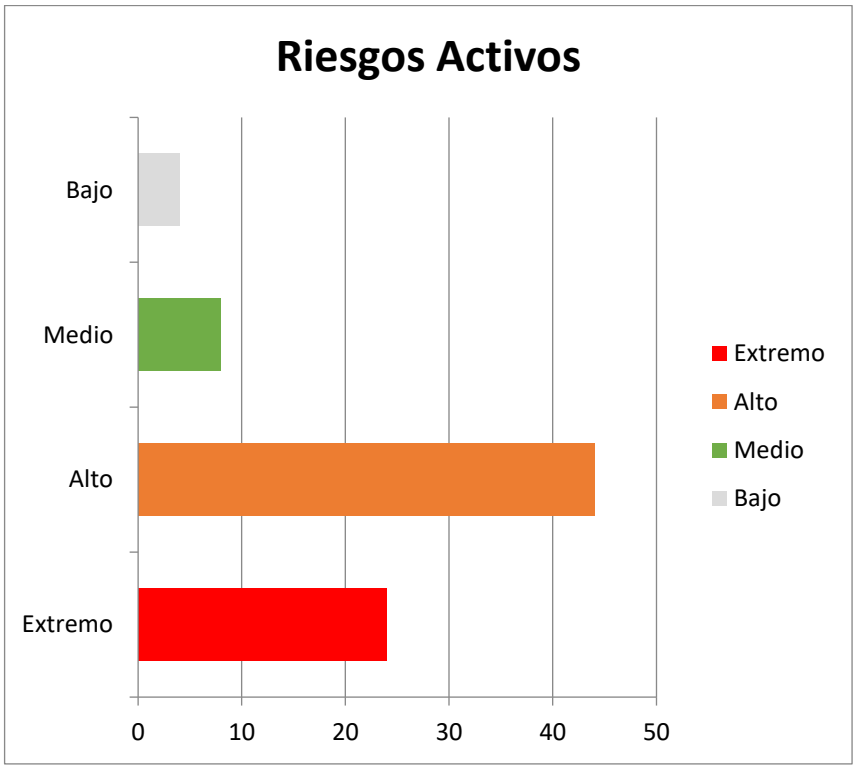
RESUMEN DEL NIVEL DE RIESGOS DE LOS ACTIVOS

Tabla 27 Nivel de Riesgos de los Activos.

Resumen de nivel de riesgo en los activos	
Extremo	24
Alto	44
Medio	8
Bajo	4

En la figura No.13 “Riesgos Activos” identifica de forma gráfica los diferentes activos que han sido clasificados como los de mayor probabilidad de impacto de inversión en la entidad, y los con probabilidad de impacto bajo en la entidad. Como lo especifica la tabla No 27 “*Nivel de Riesgos de los Activos”.*

Figura 13 Riesgos Activos



,

27. FASE 3 .INTEGRACIÓN DEL PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Objetivos**:**

Informar, estar al tanto, a los funcionarios y contratistas la aprobación de las políticas de seguridad de la información.

Optimar el nivel de conocimiento en los diferentes temas de seguridad y difundir la novedad de sucesos y/u eventualidades.

Generar cultura al interior del Instituto Financiero Para el desarrollo del Huila en todo lo referente a Seguridad de la Información.

ESTRATEGIAS INFORMACION DE LA POLITICAS DE SEGURIDAD

Los procedimientos propuestos por el Instituto Financiero para el Desarrollo de Huila - INFIHUILA, intentan avanzar en los temas de Seguridad de la Información y están alineados a la misión de la entidad.

Es fundamental crear una cultura jerárquica dentro del Instituto Financiero para el Desarrollo de Huila - INFIHUILA a pesar de los problemas de seguridad de los datos, por esta razón se sugieren ejercicios confiables que apoyen la comprensión de lo que significa la seguridad de la información y los resultados potenciales incluso con negligencia, generalmente responsable, en el caso de malas direcciones de la información**.**

DEFINICIONES

Sensibilización:

es un procedimiento cuyo objetivo fundamental es afectar la conducta de una población o fortalecer con grandes prácticas un tema específico

Entrenamiento

proceso utilizado para mostrar habilidades, permite que un individuo ejecuta capacidades explícitas relegando su posición.

Política

divulgaciones de alto nivel que expresan los objetivos a cumplir de la entidad con respecto a un tema específico.

Brecha

El espacio o curso que se va a ir entre un estado presente y un estado deseado

ingeniería social: “Tipo de ataque de seguridad en la cual un individuo manipula al otro con el fin de obtener información que puede ser utilizada para acceder a un

sistema no autorizado, sustraer dinero o incluso suplantar la identidad de la víctima”[49]

Para el plan de sensibilización se realizar una campaña la cual tendrá los siguientes temas a tratar:

Sensibilización:

Para esta fase es necesario abarcar varios temas en los cuales su principal objetivo es impactar y reforzar con buenas prácticas.
Un ejemplo práctico: sería la de las contraseñas seguras, consecuencias, y que hacer si esta es olvidada por alguna razón.

Para esta sesión se genera conciencia en los funcionarios y contratistas de la entidad de que la seguridad es un tema de buenas prácticas y de todos.

Entrenamiento:

Formar, a los funcionarios y contratistas del instituto Financiero para el desarrollo del Huila – INFIHUILA, el uso de las buenas prácticas y divulgación de los deberes a través de las diferentes políticas de seguridad de la Información.

Educación a los funcionarios y Contratistas.

cuando se hayan terminado las etapas anteriores, se avanzará la propensión en los funcionarios y contratistas preparados para estar a la vanguardia de los problemas

[49] (Mintic, s.f.) Complete Guide To CISM Certificación, Pág. 191

identificados con la seguridad de los datos y las mejores prácticas; lo que permitirá contribuir de manera efectiva con los enfoques de valor, la mejora incesante y la administración satisfactoria de la seguridad de la información.

Legislación

El instituto Financiero para el desarrollo del Huila capacitará a todos los funcionarios y contratistas en temas de legalidad, leyes que se deben tener en cuenta para tomar una buena decisión.

Inventario de música, videos y borrado de contenidos ilegales:

se realizará auditorias espontaneas a todos los PC del Instituto, para verificación de software ilegal, sin licencia, videos, música que no sean propias del instituto

Borrado de información personal:

Formar a los funcionarios y contratitas a la cultura de suprimir, borrado seguro de la información confidencial que no es apropiada para la entidad. (información personal).

Navegación segura por internet:

Formar a los funcionarios y contratistas al no ingreso de Facebook, Twitter, MSN entre otros en horarios laborares, o incluso cuando están atendiendo clientes, reuniones, conferencias, ingreso de páginas seguras, descargas seguras. Con el fin de que hagan buen uso del internet.

Uso del correo electrónico:

El instituto financiero para el desarrollo del Huila capacitara la política de correo electrónico, socializar el protocolo y los posibles riesgos de abrir un correo inseguro.

El instituto Financiero para el Desarrollo del Huila – INFIHUILA desarrollara una campaña que lleva por nombre INFI-SEGURO-, la cual tiene como objetivo la sensibilización de todos los funcionarios y contratistas en los temas de seguridad de la información orientado hacia la norma ISO 27001 e implementación del Sistema de Gestión de Seguridad de la Información.

El desarrollo de esta campaña se realizará con una pequeña lista de actividades:

- diseño de una imagen para la campaña.
- diseño de pendones
- Diseño de salvapantallas
- Un slogan para la campaña
- Diseño de 2 fondos de pantalla en temas de seguridad
- Creación y entrega de recordatorios alusivos a la seguridad de la información
- Interacción con los funcionarios y contratistas mediante juego y retroalimentando la seguridad de la información.
- Se presenta diferentes photo booth con temas de seguridad, para cada puesto de trabajo, con el objetivo concientizar y familiarizar al usuario de la seguridad informática.
- Se diseñará 10 mensajes alusivos a la seguridad de información, de las cuales se proporcionará a través de los diferentes canales del instituto con objetivo de que todos los funcionarios, contratistas, proveedores y clientes crean conciencia moral, racional y emocional dentro y fuera de la entidad.

FASES DE EJECUCION

El instituto Financiero Para el desarrollo del Huila. INFIHUILA realizara la campaña de la siguiente manera:

Una sensibilizando a los funcionarios y contratistas con pequeñas actividades como son obras cortas de teatro, en donde se formará en los temas más rutinarios en el auditorio del instituto con la utilidad de reunir a todos los usuarios y monitorear que sitios de trabajo quedaron vulnerables a una amenaza. Esta actividad tendrá un tiempo de 1 hora en la mañana.

La segunda campaña de Divulgación se realizará actividades de juegos, concursos en donde todos los funcionarios, contratistas podrán participar y ganar recordatorios. Esta actividad tendrá como determinación el conocimiento, que tanto saben de seguridad, y como ellos actúan antes los diferentes incidentes. Con este tema se recogerá una muestra y una medición de que personas están atentas ante una amenaza, se empleará formación en temas de políticas de seguridad el instituto y se formará un perfil o score con el que lo definirá con mayor puntaje para el premio especial.

FASE TRANSFERENCIA DE CONOCIMIENTO

Como integridad el instituto Financiero para el Desarrollo del Huila contemplará una capacitación con un asesor experto en temas de seguridad donde transmitirá los conocimientos de seguridad de la información, activos, computadores seguros entre otros.

La capacitación estará dirigida a todos los funcionarios y contratistas del instituto Financiero para el Desarrollo del Huila -INFIHUILA ("Administración De Contraseñas Uso Y Manejo De Inventario Malware y sus diferentes tipos Software Permitido/Prohibido En La Entidad Políticas Organizacionales Relacionadas Con Seguridad De La Información Uso De Dispositivos De La Entidad Fuera De Las Instalaciones Uso De Correo Electrónico E Identificación De Correos Sospechosos Seguridad En El Puesto De Trabajo Uso Apropiado De Internet Temas de control de acceso a los sistemas (privilegios, separación de roles) Política De Escritorio Limpio Ingeniería Social Sanciones Por Incumplimiento De Las Políticas Gestión De Incidentes (Como reportar, que puedo reportar").[50]

FASE DEL CIERRE

El instituto Financiero para el Desarrollo del Huila, en el cumplimiento de dichas campañas acompañada de diferentes actividades tendrá como evidencia listado de asistencia.

DETALLE DE LAS ACTIVIDDES

OBRAS PEQUEÑAS

Concepto: difundir mensajes en temas de seguridad de la información a través del dramatizado.

[50] (MInTic, s.f.)

Datos de la Dramatización:

Lugar: Auditorio del Infihuila
Fecha: 22 de noviembre 2019
Hora: 8:30 am

Presentación del Dramatizado 20 minutos aprox.

2. Punto juego TRIVIA

Concepto: se informará de temas visto anteriormente midiendo su conocimiento en seguridad de la información.

Lugar: Auditorio del Infihuila
Fecha: 22 de noviembre 2019
Hora: 9:00 am

Concurso en el cual el funcionario u contratista participa y el que tenga mayor score gana premio algunas de estas actividades son:

- Preguntas asociadas en temas de seguridad.
- Principales políticas de seguridad
- Se empleará los canales de comunicación del Instituto Financiero Para el Desarrollo del Huila.
- Se presentará la tabla con mejores puntajes. Y el mejor puntaje se le obsequiara un premio.

CAPACITACION A FUNCIONARIOS Y CONTRATISTAS DEL INFIHUILA

ASESOR:
Consultor de Informática de la alcaldía de Neiva

Lugar: Auditorio del Infihuila
Fecha: 25 de noviembre 2019
Hora: 8:00 am

Temáticas de la capacitación

- Administración De Contraseñas
- Uso Y Manejo De Inventario
- Malware y sus diferentes tipos Software Permitido/Prohibido En La Entidad
- Políticas Organizacionales Relacionadas Con Seguridad De La Información
- Uso De Dispositivos en La Entidad y Fuera De Las Instalaciones
- Uso De Correo Electrónico E Identificación De Correos Sospechosos

REGISTROS

- Toma de fotografía
- Listado de asistencia.

28. GLOSARIO DE TERMINOS

Activo de información: lo que es muy importante y que contiene datos cruciales de la organización que deben ser protegidos.

Riesgo: es el motivo potencial del daño a un recurso de datos.

Análisis de riesgos: utilización sistemática de datos accesibles para reconocer peligros y medir peligros. Causa: Razón por la que se produce el peligro.

Controles: son aquellos instrumentos que se utilizan para seleccionar y controlar actividades que se consideran sospechosas y que pueden influir en los recursos de datos de alguna manera u otra.

Disponibilidad: la propiedad establece que los datos son abiertos y utilizables por las personas debidamente aprobadas

Propietario del riesgo sobre el activo: Persona a cargo de tratar el peligro.

Impacto: Consecuencias del riesgo. Dimensión de falta de sinceridad en el recurso de datos producido cuando existe el peligro.

Incidente de seguridad de la información: una ocasión indeseable o sorprendente, que tiene la posibilidad de socavar la seguridad de los datos.

Integridad: Propiedad para proteger la exactitud y el cumplimiento de las ventajas.

Probabilidad de ocurrencia: posibilidad de mostrar una circunstancia u ocasión particular.

Responsables del Activo: responsables del recurso de datos.

Riesgo: Grado de presentación de un beneficio que permite la aparición de un peligro.

.

Riesgo Inherente: nivel de vulnerabilidad inherente a cada movimiento, sin la ejecución de ningún control.

Riesgo Residual: el nivel de peligro se mantiene debido al uso de esfuerzos de seguridad en la ventaja.

PSE: Proveedor de Servicios Electrónicos, es un mecanismo unificado a través del cual las organizaciones brindan a los clientes la posibilidad de realizar sus cuotas en la web.

Seguridad de la Información: preservación del secreto, honestidad y accesibilidad de los datos (ISO 27000: 2014).

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información. Sistema de gestión de seguridad de datos SGSI: permite crear, actualizar, mantener y mejorar constantemente la administración de la seguridad de datos según los requisitos previos de la norma NTC-ISO-IEC 27001: 2013.

Vulnerabilidad: la debilidad de un beneficio o la recopilación de recursos de datos que pueden ser utilizados por un riesgo. La indefensión se describe por falta de asistencia en los controles de seguridad que pueden ser mal utilizados.

Amenaza: es toda la actividad o el componente adecuado para atacar la seguridad de los datos.

Antivirus. El software antivirus es responsable de identificar, bloquear y prescindir de infecciones de PC o códigos vengativos.

Ataque: la demostración de obstaculizar o dañar un recurso de datos para causar problemas de calidad, accesibilidad y honestidad inquebrantables. O bien, también puede decir que es el punto en el que surge un peligro de seguridad.

.

Código malicioso: software destinado a ejecutar actividades nocivas (por ejemplo, dañar la programación de la PC, eliminar datos guardados en un marco de la PC, explotar los activos de la PC para realizar actividades diferentes inseguras para el cliente) e incluir proyectos, por ejemplo, infecciones, gusanos, spyware troyanos. Se puede utilizar como método de propagación, correo electrónico, configuraciones regionales, sistemas, teléfonos celulares, dispositivos extraíbles (por ejemplo, unidades de memoria).

Estándar de seguridad: muchas pautas o modelos destinados a dar respuestas marco para un territorio particular de conocimiento.

Firewall: un firewall o adicionalmente llamado firewall, es una programación o equipo que limita el acceso a sitios o un sistema sin aprobación de acceso

Incidente de seguridad: una ocurrencia de seguridad es cualquier actividad que comprometa la confiabilidad, accesibilidad y honestidad de los datos.

Ingeniería social: es la disposición de las actividades que tienen la razón para adquirir datos, la tergiversación o el acceso no aprobado a los marcos de PC, y eso ha incluido eventualmente el control mental de los individuos.

Intrusos: es un individuo que intenta acceder a un marco de PC sin aprobación, a través de estrategias y / o técnicas de PC que lo permiten.

ISO: (Organización Internacional del Foro de Normalización). Asociación mundial de puntos de referencia

Metodología: se trata de muchos principios o técnicas que se resuelven de manera fundamental con el objetivo de lograr la coherencia con un estándar o un estándar.

Phishing: suplantación de una página o sitio.

Plan de contingencia: es una especie de disposición preventiva, profética y receptiva. Muestra una estructura vital y utilizable que controlará una circunstancia de crisis y limitará sus resultados negativos.

Riesgos: La probabilidad de que un riesgo abusa de una debilidad y dañe un recurso de datos. Departamento de Seguridad.

Repudio: Denegación, por una de las entidades implicadas en un a comunicación, de haber participado en la totalidad o en parte de dicha comunicación.

Seguridad lógica: conjunto de esfuerzos de seguridad y aparatos de PC para controlar el acceso a los sistemas de PC.

Seguridad física: controles externos a la PC, que intentan evitar peligros de tipo físico, por ejemplo, incendios, inundaciones, entre otros.

SGSI: Sistema de gestión de la seguridad de la información.

Teletrabajo: el teletrabajo es otro sistema de asociación de trabajo en el que el trabajo individual construye una parte importante de su trabajo fuera de la organización y por medios telemáticos.

Vulnerabilidad: la indefensión de la seguridad es una decepción o una deficiencia en el plan, la ejecución, la actividad o la junta directiva de un marco, que se puede abusar para ignorar el enfoque de seguridad del marco. UOC Guillermo Navarro Arribas. Prólogo a las vulnerabilidades.

Wi-Fi (Wireless fidelity o fidelidad sin cables): es un sistema de PC sin utilizar enlaces idénticos a la innovación remota 802.11 para la correspondencia remota.

Wi-phishing: Wi-phishing, disminución de información individual a través de un sistema falso de acceso a Wi-Fi.

DMZ: Una DMZ o una zona desmilitarizada, es una parte particular del sistema, en la que se encuentran administraciones explícitas de sistemas que están abiertas a sistemas no vinculados, por ejemplo, Internet.

Red de Datos: es la organización de la fundación o correspondencia que ha sido explícitamente destinada a transmitir datos a través del intercambio de información.

Diseño de Red Segura: la definición de un sistema conspira aplicando los esfuerzos de seguridad de la PC, que una vez ejecutados limitan los peligros de una interrupción.

Red Privada virtual VPN: técnica de telecomunicaciones que consta de una organización de información limitada a una reunión cerrada de clientes, que se

ensambla utilizando algunos o la mayoría de los activos de un sistema libre, es decir, es un aumento del sistema privado de un Asociación que utiliza un sistema abierto.

29. RECOMENDACIONES

El Instituto Financiero para el Desarrollo del Huila – INFIHUILA, tanto el gerente como sus funcionarios debe estar comprometida con la seguridad de los activos de su información los cuales garantice confiabilidad, integridad y disponibilidad ya que la seguridad es de todos.

La entidad debe proyectar anualmente presupuesto para los temas de seguridad e implementarlos y actualizar el SGSI por lo menos 1 vez al año.

Deben monitorear, actualizar las políticas periódicamente o en su defecto una vez al año.

Implementación de controles en toda la infraestructura tecnológica tanto hardware con software, garantizando su funcionalidad.

Realizar auditorías anuales, pruebas de test para que realice actualizaciones al sistema de gestión de seguridad de la información y este plan este en las mejores condiciones con su técnicas y metodologías para salvaguardar la información.

Capacitar y concientizar a funcionarios y contratista en temas de seguridad, tics de cómo pueden proteger sus activos de Información.

CONCLUSIONES

Se realizo un diagnóstico de la situación actual de seguridad de la información en el instituto Financiero para el Desarrollo del Huila y se idéntica riesgos y amenazas que atentan en su organización como el robo de información, licenciamientos entre otros.

Se define las primeras pautas como presupuesto, riesgos inherentes a la hora de elaborar el diseño de Sistema de Gestión de Seguridad de la información.

En la sociedad de información que se vive actualmente, es conveniente que toda empresa u organización de cualquier carácter o tamaño implemente mecanismos de seguridad, teniendo en cuenta la normatividad existente como la ISO/IEC 27001:2013 para buscar problemas de seguridad y establecer los controles necesarios para salvaguardar la información.[51]

Existen normas y metodologías como Magerit en el ambiente de seguridad, que permiten hacer análisis y estimación del riesgo de forma ordenada y sistemática para obtener resultados que ayudan de forma eficaz en el SGSI. [52]

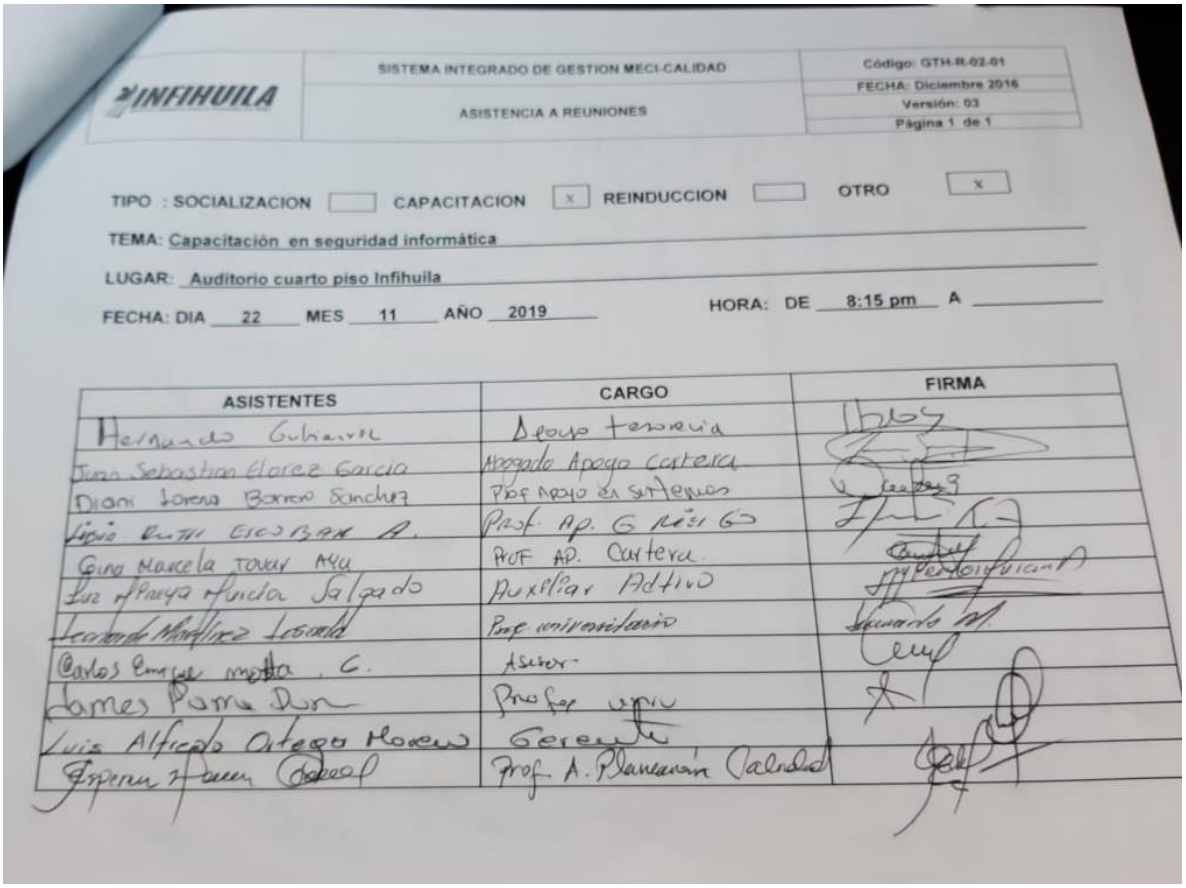
Concientizar a los funcionarios de la Entidad acerca de la seguridad de la información, labor que no es sólo de la dirección de Informática, sino que debe comprometer a toda la organización

[51] (TIC, s.f.)

[52] (INFORMACION)

ANEXOS

1. LISTADO DE ASISTENCIA A LAS CAPACITACIONES Y CAMPAÑAS PROPUESTAS PARA EL INSTITUTO



INFIHUILA | SISTEMA INTEGRADO DE GESTION MECI-CALIDAD | Código: GTH-R-02-01
ASISTENCIA A REUNIONES | FECHA: Diciembre 2016 | Versión: 03 | Página 1 de 1

TIPO : SOCIALIZACION [ ] CAPACITACION [X] REINDUCCION [ ] OTRO [X]

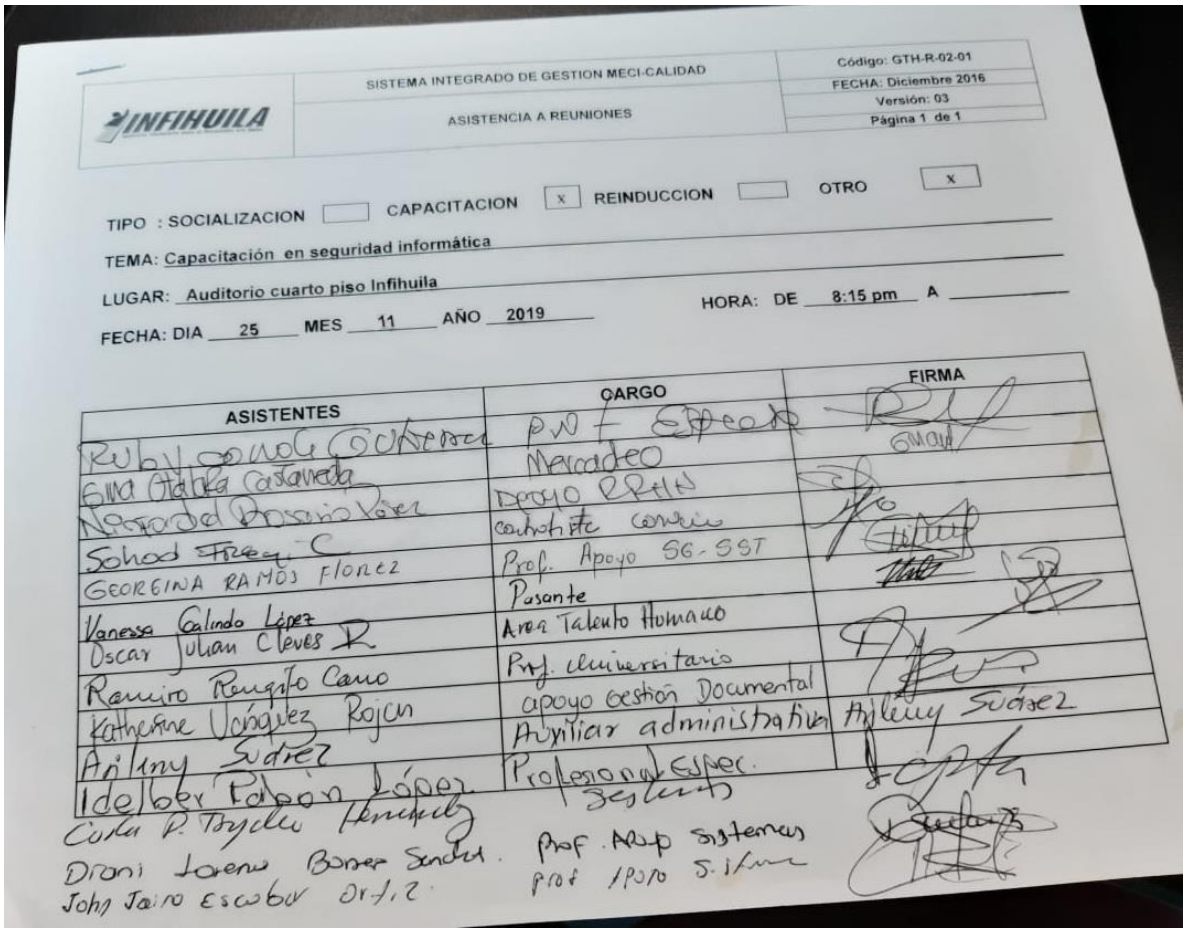
TEMA: Capacitación en seguridad informática

LUGAR: Auditorio cuarto piso Infihuila

FECHA: DIA 22 MES 11 AÑO 2019 HORA: DE 8:15 pm A _____

ASISTENTES	CARGO	FIRMA
Hernando Guharnal	Apoyo tesorería	
Juan Sebastian Elorez Garcia	Abogado Apoyo Cartera	
Diana Lorena Barrero Sanchez	Prof Apoyo en Sistemas	
Jairo [illegible]	Prof. Ap. Gestión	
Gina Marcela Tovar Ayu	PROF AP. Cartera	
Luz Mireya Murcia Salgado	Auxiliar Activo	
Leonardo Martínez Losada	Prof. universitario	
Carlos Emigdio motta . G.	Asesor	
James Parra Dun	Profesor UPIV	
Luis Alfredo Ortega Moreno	Gerente	
Esperanza Forero Ordoñez	Prof. A. Planeación Calidad	

CAPACITACION 2.



INFIHUILA

SISTEMA INTEGRADO DE GESTION MECI-CALIDAD	Código: GTH-R-02-01
	FECHA: Diciembre 2016
ASISTENCIA A REUNIONES	Versión: 03
	Página 1 de 1

TIPO : SOCIALIZACION [ ] CAPACITACION [X] REINDUCCION [ ] OTRO [X]

TEMA: Capacitación en seguridad informática

LUGAR: Auditorio cuarto piso Infihuila

FECHA: DIA 25 MES 11 AÑO 2019 HORA: DE 8:15 pm A

ASISTENTES	CARGO	FIRMA
Ruby [illegible] Gutierrez	PYF Especialista	
Gina Ofelia Castaneda	Mercadeo	
Nestor del Rosario Vera	Apoyo RRHH	
Sohad [illegible] C	contratista comercio	
GEORGINA RAMOS FLOREZ	Prof. Apoyo SG-SST	
Vanessa Calindo López	Pasante	
Oscar Julian Cleves R.	Area Talento Humano	
Ramiro Rengifo Cano	Prof. universitario	
Katherine Vásquez Rojas	apoyo gestion Documental	
Ailuny Suárez	Auxiliar administrativa	Ailuny Suárez
Idelber Fabian López	Profesional Espec. Gestion	
Carla P. Trujillo Hernandez		
Dioni Lorena Bonet Sanchez	Prof. Apoyo Sistemas	
John Jairo Escobar Ortiz	prof. Apoyo S.I.	

BIBLIOGRAFÍA

Bortnik, S. (s.f.). *revista.seguridad.unam.mx*. Obtenido de https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

Collazos, j. M. (s.f.). *derechodeautor.gov.co.* Obtenido de http://derechodeautor.gov.co/documents/10181/11769/La+proteccin+del+derecho+de+autor+y+los+derechos+conexos+en+el+ambito+penal+sep+15+de+2010.pdf/75686fc1-c9be-4dc3-b1d5-efcd5f4be949

Colombia, S. d. (s.f.). *cdn.actualicese.com.* Obtenido de https://cdn.actualicese.com/normatividad/2019/Conceptos/C2019081599-19.pdf

Colombia, s. F. (s.f.). *cdn.actualicese.com*. Obtenido de https://cdn.actualicese.com/normatividad/2019/Conceptos/C2019081599-19.pdf

conexionesan. (s.f.). *www.esan.edu.pe*. Obtenido de https://www.esan.edu.pe/apuntes-empresariales/2015/10/canales-comunicacion-existen-dentro-empresas/

DAFT , R. (2007). Teoría y Diseño Organizacional. 9na Edición, Cengage Learning Editores. Obtenido de Daft Richard, Teoría y Diseño Organizacional, 9na Edición, Cengage Learning Editores, México, 2007, p. 10.

ESPITIA, R. M. (s.f.). *repository.unad.edu.co.* Obtenido de https://repository.unad.edu.co › bitstream › handle

García, S. R. (s.f.). */mestrado.prpg.ufg.br/up/97/o/IA._Madrid.pdf.* Obtenido de https://mestrado.prpg.ufg.br/up/97/o/IA._Madrid.pdf

INFIHUILA. (s.f.). */www.infihuila.gov.co*. Obtenido de https://www.infihuila.gov.co/participacionciudadana.html

INFORMACION, S. G. (s.f.). *www.iso27000.es.* Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Instituto Financiero para el Desarrollo del Huila. (s.f.). *Infihuila*. Obtenido de www.infihuila.gov.co

KAST FREEMONT;ROSENZWEIG JAMES. (1989,). *Administración en las Organizaciones: Enfoque de sistemas y de contingencias, 2da Edición,.* Obtenido de Kast Freemont y Rosenzweig James, Administración en las Organizaciones: Enfoque de sistemas y de contingencias, 2da Edición, McGRAW HILL, México, 1989, p. 7.

LOPEZ, G. (s.f.). *blogs.imf-formacion.com*. Obtenido de https://blogs.imf-formacion.com/blog/tecnologia/organigrama-departamento-it-201707/

Mimenza, O. C. (s.f.). *psicologiaymente.com/miscelanea/tipos-de-investigacion*. Obtenido de https://psicologiaymente.com/miscelanea/tipos-de-investigacion

MINTIC. (s.f.). *mintic.gov.co*. Obtenido de https://www.mintic.gov.co/portal/604/articles-3559_documento.pdf

Mintic. (s.f.). *www.mintic.gov.co*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

MInTic. (s.f.). *www.mintic.gov.co*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

MINTIC. (s.f.). *www.mintic.gov.co*. Obtenido de https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

OVADE LOZANO, M. (2017). *alejandria.poligran.edu.co.* Obtenido de http://alejandria.poligran.edu.co/bitstream/handle/10823/1004/3.Documento%20final_Plan%20Estrategico%20de%20Seguridad%20de%20la%20Informaci%C3%B3n%20para%20una%20compa%C3%B1ia%20de%20seguros.pdf?isAllowed=y&sequence=1

PALOMO, D. F. (2019). *Guia de proyecto aplicado escenario 2.* NEIVA: UNAD.

Pérez, I. (2015). *welivesecurity.com*. Obtenido de https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/

RODRIGUEZ, D. (1996). Gestion Organizacional:Elementos para su estudio. Obtenido de , Gestión Organizacional: Elementos para su estudio, Universidad Iberoamericana, México, 1996, p. 66

SFC. (2014). Circular externa 034 de 2014. Bogota, Colombia. Obtenido de superintendencia financiera de Colombia. Financiera de Colombia. circular externa 034 de 2014.

TIC. (s.f.). *www.mintic.gov.co*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Universidad Nacional autonoma de Mexico. (s.f.). *revista.seguridad.unam.m*. Obtenido de https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

Valencia, F. (s.f.). *www.sic.gov.co/ normatividad*. Obtenido de https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Villamizar, C. (agosto de 2013). *www.magazcitum.com*. Obtenido de https://www.magazcitum.com.mx/?p=2361#.XeQxyugzbIU

Villegas, B. M. (s.f.). *funcionpublica.gov.co*. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488