IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LAS BASES DE DATOS ORACLE SISTEMA MUISCA DE LA SUBDIRECCIÓN DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES EN LA DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES

MARIO PEREZ LOZANO
LUIS OMAR CORREA VISBAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION DE SEGURIDAD INFORMÁTICA
2015

IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LAS BASES DE DATOS ORACLE SISTEMA MUISCA DE LA SUBDIRECCIÓN DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES EN LA DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES

MARIO PEREZ LOZANO
LUIS OMAR CORREA VISBAL

Monografía para optar al título de Especialista en Seguridad Informática

Director de Proyecto
MSC. Manuel Antonio Sierra Rodríguez

Universidad Nacional Abierta y a Distancia UNAD
Escuela de Ciencias Básicas Tecnología e Ingeniería
Especialización de Seguridad Informática
Bogotá D.C.
2015

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del Jurado

_____
Firma del Jurado

_____
Firma del jurado

Bogotá 02-11-2015

Contenido

1. INTRODUCCIÓN 13
1. MARCO CONCEPTUAL 14
1.1 FORMULACIÓN DEL PROBLEMA 14
1.2 JUSTIFICACIÓN 15
1.3 OBJETIVOS 16
1.3.1 Objetivo general 16
1.3.2 Objetivos específicos 16
2. MARCO DE REFERENCIA 17
2.1 MARCO TEÓRICO Y NORMATIVO 17
2.2 MARCO INSTITUCIONAL 18
2.2.1 Análisis de la empresa 18
3. ANALISIS DE LA INFORMACION. 22
3.1 ANALISIS DIFERENCIAL 22
3.2 DESCRIPCIÓN DE LA METODOLOGÍA DE EVALUACIÓN DE RIESGOS SELECCIONADA 24
3.3 IDENTIFICACIÓN DE LOS ACTIVOS. 25
3.3.1 Valoración de los activos 28
3.4 ANÁLISIS DE AMENAZAS 29
3.5 RIESGO INHERENTE 31
3.5.1 Valores de frecuencias del riesgo 31
3.5.2 Valores de impacto del riesgo 31
3.6 RIESGO RESIDUAL 35
3.7 TIPO DE MANEJO DE LOS RIESGOS 37
3.7.1 Evitar el riesgo 37
3.7.2 Reducir el riesgo 37
3.7.3 Dispersar y atomizar el riesgo 37
3.7.4 Trasferir el riesgo 37
3.7.5 Asumir el riesgo 38
3.8 TRATAMIENTO A LOS RIESGOS 40

3.8.1 Datos / Información 40
3.8.2 Software 41
3.8.3 Servicios 41
3.8.4 Aplicaciones 41
3.8.5 Equipamiento 41
3.8.6 Instalaciones 42
3.8.7 Personal 42
4. OBSERVACIONES PARA APLICACIÓN DE CONTROLES 43
4.1 Políticas de la seguridad de la información. 43
4.2 Organización de la seguridad de la información. 43
4.3 Seguridad de Recursos Humanos 43
4.4 Gestión de Activos de información 44
4.5 La seguridad física y medioambiental 44
4.6 Gestión de operaciones y Comunicaciones 45
4.7 Control de Acceso 46
4.8 Desarrollo, Mantenimiento y adquisición de Sistemas de Información 46
4.9 Gestión de Incidentes de Seguridad Información. 47
4.10 Gestión de Continuidad del Negocio 47
4.11 Cumplimiento Regulatorio 47
5. PROPUESTA PARA IMPLANTAR UN SGSI PARA LAS BASES DE DATOS ORACLE. 50
5.1 Definición del alcance y límites del SGSI 50
5.2 Definición de la Política del SGSI 51
5.3 Estructura del sistema documental 51
5.3.1 Política y Objetivos de SGSI 51
5.3.2 Desarrollo de los objetivos 53
5.3.3 Registros necesarios para el progreso del proceso 55
5.4 RECURSOS DISPONIBLES 67
5.5 CRONOGRAMA 68
5.6 RECOMENDACIONES 69
6. CONCLUSIONES 70

7. BIBLIOGRAFÍA 71
8. ANEXOS 72

Tablas

Tabla 1 Escala de valoración del nivel de madurez. 22
Tabla 2 Nivel de cumplimiento Controles 2012 23
Tabla 3 Identificación de activos 27
Tabla 4 Criterios de valoración 28
Tabla 5 Valoración de Activos Tipo: Datos / Información 28
Tabla 6 Amenazas 30
Tabla 7 Probabilidad de la frecuencia 31
Tabla 8 Clasificación del impacto 31
Tabla 9 Valoración del riesgo 31
Tabla 10 Medición del riesgo 32
Tabla 11 Riesgos Inherentes. 33
Tabla 12 Medición del riesgo. 35
Tabla 13 Riesgo residual 36
Tabla 14 Tratamiento a los riesgos. 39
Tabla 15 Nivel de cumplimiento Controles 2015. 48
Tabla 16 Controles Norma ISO 27001. 55

Figuras

Figura 1 Modelo PDCA aplicado a los procesos del SGSI. 17
Figura 2 Estructura orgánica – Nivel Central. 19
Figura 3 Modelo de Gestión – MUISCA. 20
Figura 4 Nivel de cumplimiento controles 2012 24
Figura 5 Nivel de cumplimiento controles 2015. 49
Figura 6 Nivel de cumplimiento controles 2015 y proyección 2017 50
Figura 7 Cronograma de actividades. 68

Anexos

Anexo 1 Procedimiento regulación de ingreso a las bases de datos Oracle 72
Anexo 2 Procedimiento contraseñas para ingreso a las bases de datos Oracle ...79
Anexo 3 Procedimiento copias de seguridad bases de datos Oracle 82
Anexo 4 Procedimiento restauración y recuperación bases de datos Oracle 86

RESUMEN

El proyecto presentado a continuación se encuentra enmarcado en la alternativa de grado para la especialización en seguridad informática en la modalidad de monografía y su objetivo es formular una propuesta de implantación de un Sistema de Gestión de Seguridad de la Información SGSI para el área de tecnología de la Dirección de Impuestos y Aduanas Nacionales DIAN, específicamente a las Bases de datos ORACLE que soportan el núcleo del negocio. La DIAN es una empresa de orden estatal encargada de recaudar los impuestos nacionales y los derechos aduaneros del país.
El SGSI es una parte del sistema global de gestión que, basado en un análisis de los riesgos del negocio, permite asegurar la información frente a la pérdida de: Confidencialidad, Integridad y Disponibilidad, de allí la importancia de implantar un sistema de este tipo. Este sistema que se pretende implantar se basa en la norma ISO/IEC 27001 y se realiza a través de la gestión de seguridad que tiende a una mejora continua a partir de un ciclo que comprende las fases de planificar, hacer, verificar y actuar, conocido como ciclo Deming.

Aunque la seguridad en el área de tecnología de la institución se encuentra diseminada en todos lados no está definida en base a controles, de igual manera no se encuentra formalizada ni definido en cuanto a responsables.

Abstract

The project presented below is enclosed in the alternative grade for specialization in Information Security in the monograph mode and its goal is to formulate a proposal for implementation of a Management System Information Security ISMS for the technology area National Tax and Customs DIAN, specifically for Oracle databases that support the core business. DIAN is a state order company responsible for collecting national taxes and customs duties in the country.

The ISMS is a part of the overall management system, based on an analysis of business risks, ensures the information against loss: confidentiality, integrity and availability, hence the importance of implementing a system of this type. This system is intended to implement is based on ISO / IEC 27001 and is performed through safety management tends to continuous improvement from a cycle which comprising the steps of plan, do, check and act, known as Deming cycle.

Although security in the technology area of the institution is scattered everywhere is not defined based on controls, just as it is not formalized or defined in terms of responsibility.

DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de TI, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

Este documento contiene información confidencial de la infraestructura tecnológica de la Dirección de Impuestos y Aduanas Nacionales DIAN.

TITULO DEL PROYECTO

Implantación del Sistema de Gestión de Seguridad de la Información para las bases de datos Oracle Sistema Muisca de la Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones en la Dirección de Impuestos y Aduanas Nacionales.

1. INTRODUCCIÓN

En la actualidad y debido a lo complejo de asegurar la información por el alto nivel de interconexión al que estamos enfrentados en el mundo, se requiere proveer de un método con el cual podamos tomar las medidas preventivas y reactivas al interior del entidad, de la misma manera nuestra infraestructura tecnológica que nos permitan enfrentar la complejidad de proteger nuestra información independientemente del medio en que esta se encuentre. Por supuesto manteniendo la confidencialidad, la integridad y la disponibilidad que son los principios básicos de la Seguridad de la Información.

Como podemos inferir la Seguridad de la información es un proceso continuo en donde se gestionan las amenazas identificándolas según el riesgo y el impacto que esta pueda tener y se ejecuta un proceso de mitigación donde se corrige la vulnerabilidad cerrando la brecha junto con la probabilidad que ocurra o que vuelva a ocurrir. Esto deja ver que la Seguridad de la Información es un asunto completamente administrativo y no propiamente técnico como muchos podrían verla, lo que deriva en que la seguridad de la información se convierta en una responsabilidad del gobierno institucional.

En la DIAN la seguridad de la información se trabaja desde la misma elaboración y ejecución de los planes misionales, estratégicos y de apoyo. Además está comprometida en todo un desarrollo global del Sistema de Seguridad de la Información (SGSI) observando el cumplimiento de los estándares fijados, y enmarcados dentro del NTC-ISO/IEC 27001.[1] Al SGSI se le fijan objetivos más allá de lo tecnológico, tales como apoyar eficaz y técnicamente la protección contra amenazas que puedan atentar contra la estabilidad fiscal del país y asegurar un comercio ágil y competitivo que garantice la prestación de los servicios de la entidad al contribuyente y ciudadanía en general.

La Seguridad Informática al interior de la Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones en la Dirección de Impuestos y Aduanas Nacionales es entendible, si observamos el impacto que una falla de seguridad podría ocasionar en una plataforma heterogénea, con muchos servicios de alta disponibilidad y de confidencialidad de la información que se maneja dentro de la DIAN.

[1] Norma Técnica colombiana – ISO/IEC 27001: Norma internacional emitida por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información en una empresa.

1. MARCO CONCEPTUAL

1.1 FORMULACIÓN DEL PROBLEMA

La Dirección de Impuestos y Aduanas Nacionales maneja tres pilares para cumplir con su misión básica que es la de garantizar la seguridad fiscal del Estado colombiano y la protección del orden público económico nacional, estos pilares son: las personas, los procesos y los sistemas. Los cuales tienen algo en común y es el manejo de la información. Dicha información como el principal activo de la entidad debemos darle el mejor de los tratamientos y con más altos estándares que nos permitan cumplir con los objetivos que garanticen la misión y la visión de la entidad.

La DIAN está expuesta a diferentes amenazas como cualquier organización gubernamental al igual que sus sistemas de información, su razón de ser es el recaudo y la prestación de un servicio de facilitación a los contribuyentes para el cumplimiento de sus obligaciones. Servicios que están expuestos y que podrían tener vulnerabilidades que podrían inducir a distintas formas de fraude, ataque de hackers, virus informáticos, sabotaje o denegación de servicios. Igualmente al interior de la entidad pueden existir riesgos de seguridad que afecten la confidencialidad de la información de los contribuyentes y sus actividades económicas. Sin dejar de lado las fallas técnicas, obsolescencia de las plataformas o catástrofes de orden natural.

La mayor parte de la información sensible de la entidad se encuentra en bases de datos, por lo cual se debe actuar para planear e implementar un sistema que asegure la información contra la perdida de confidencialidad, integridad y alta disponibilidad, de una manera proactiva salvaguardar la información contenida en las bases de datos y disminuir estos riesgos mediante un Sistema de Gestión de Seguridad de la Información SGSI.

La Dirección de Impuestos y Aduanas Nacionales requiere implantar un sistema SGSI en sus Bases de datos Oracle, que permitirá mejorar la seguridad de la información y aunque la seguridad total es inalcanzable, mediante el proceso de mejora continua del SGSI se espera lograr un nivel de seguridad altamente satisfactorio, que minimice los riesgos a los que está expuesta la entidad y el impacto que ocasionarían si efectivamente se materializaran los riesgos.

1.2 JUSTIFICACIÓN

El presente proyecto pretende proponer la implantación de un SGSI, tomando como referencia la Norma ISO/IEC 27001 en la Dirección de Impuestos y Aduanas Nacionales, definiendo su alcance inicial en las Bases de datos Oracle de la Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones.

Es importante aclarar que la única norma de la serie ISO 27000 certificable es la ISO 27001 (es una especificación, un estándar), todas las otras normas de esta serie son complementarias y sirven de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, en especial la ISO 27002 que es un código de buenas prácticas de implementación de la norma.

La ISO 27002 es una guía para, en distintos ámbitos, conocer qué se puede hacer para mejorar la seguridad de la información. Expone, en distintos campos, una serie de apartados a tratar en relación a la seguridad, los objetivos de seguridad a perseguir, una serie de consideraciones (controles) a tener en cuenta para cada objetivo y un conjunto de "sugerencias" para cada uno de esos controles. Sin embargo, la propia norma ya indica que no existe ningún tipo de priorización entre controles, y que las "sugerencias" que realiza no tienen por qué ser ni siquiera convenientes, en función del caso en cuestión.

1.3 OBJETIVOS

1.3.1 Objetivo general

Proponer la implantación de un SGSI para las bases de datos Oracle sistema MUISCA[2], que permita garantizar la seguridad contenida en las bases de datos Oracle que soportan los servicios informáticos electrónicos de la Dirección de Impuestos y Aduanas Nacionales, protegiendo los datos de los contribuyentes, la privacidad, la integridad de la información y prevenir los riesgos concernientes a la información y la sostenibilidad de los servicios que se prestan en la entidad.

1.3.2 Objetivos específicos

- Evaluar los riesgos existentes en las bases de datos Oracle y los activos que la circundan para determinar las medidas que disminuyan estos riesgos.

- Definir controles de seguridad que posibiliten asegurar la disponibilidad, confiabilidad y continuidad de las bases de datos Oracle, ofreciendo unos adecuados niveles de servicio.

- Propuesta para implantar un SGSI para las bases de datos Oracle.

[2] Modelo Único de Ingresos, Servicio y Control Automatizado

2. MARCO DE REFERENCIA

2.1 MARCO TEÓRICO Y NORMATIVO

De acuerdo a la Norma NTC-ISO/IEC 27001 un Sistema de Gestión de Seguridad de la Información (SGSI), es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Dejar de operar intuitivamente y se empieza a tomar el control sobre lo que sucede en las base de datos y sobre la propia información que se maneja en la organización, permitirá conocer mejor la organización, cómo funciona y qué se puede hacer para mejorar.

La norma NTC-ISO/IEC 27001 sigue el modelo PDCA o "Planificar–Hacer–Verificar–Actuar" (Plan–Do–Check–Act por sus siglas en inglés), y aplica para organizar todos los procesos del SGSI, como se muestra en la Figura 1.

Figura 1 Modelo PDCA aplicado a los procesos del SGSI.

Fuente: El autor DEMING, William Eduards

2.2 MARCO INSTITUCIONAL

2.2.1 Análisis de la empresa

2.2.1.1 Descripción de la empresa

La Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales DIAN, tiene como objeto coadyuvar a garantizar la seguridad fiscal del Estado colombiano y la protección del orden público económico nacional, mediante la administración y control al debido cumplimiento de las obligaciones tributarias, aduaneras y cambiarias y la facilitación de las operaciones de comercio exterior en condiciones de equidad, transparencia y legalidad.

De acuerdo al Plan Estratégico DIAN 2010 – 2014, Aprobado en sesión del Comité de Coordinación Estratégica del 22 de diciembre de 2010, se definió lo siguiente:

2.2.1.2 Visión

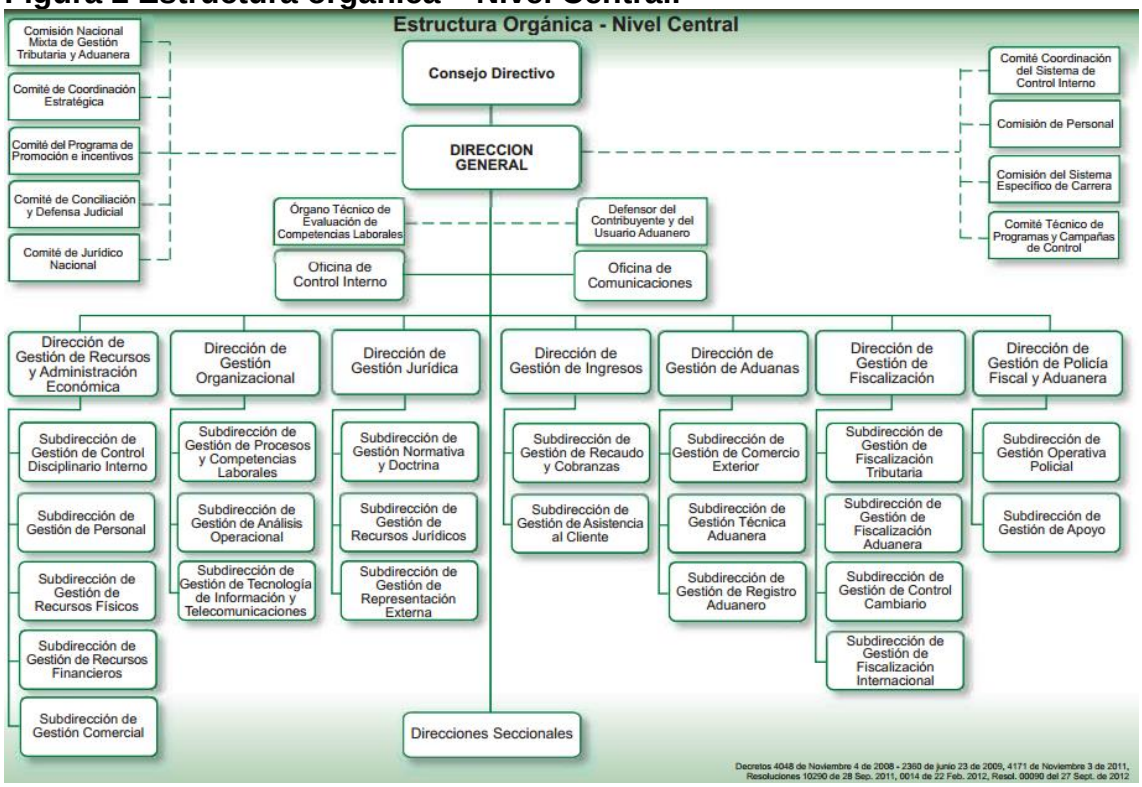
En el 2020, la Dirección de Impuestos y Aduanas Nacionales de Colombia genera un alto nivel de cumplimiento voluntario de las obligaciones tributarias, aduaneras y cambiarias, apoya la sostenibilidad financiera del país y fomenta la competitividad de la economía nacional, gestionando la calidad y aplicando las mejores prácticas internacionales en su accionar institucional.

2.2.1.3 Misión

En la Dirección de Impuestos y Aduanas Nacionales somos responsables de administrar con calidad el cumplimiento de las obligaciones tributarias, aduaneras y cambiarias, mediante el servicio, la fiscalización y el control; facilitar las operaciones de comercio exterior y proveer información confiable y oportuna, con el fin de garantizar la sostenibilidad fiscal del Estado colombiano.

2.2.1.4 Organigrama DIAN

Figura 2 Estructura orgánica – Nivel Central.



Fuente: Dirección de Impuestos y Aduanas Nacionales.

2.2.1.5 Requerimientos de seguridad de la empresa y de la seguridad de la información

La DIAN cuenta con un modelo de gestión que la conduce al cumplimiento de su misión y al logro de su propósito visional y objetivos estratégicos, el Modelo Único de Ingresos, Servicio y Control Automatizado – MUISCA se desarrolla sobre la base de la administración tributaria y aduanera articulada, coordinada y ordenada, para el cumplimiento cabal de su función dentro del Estado.

El modelo adoptado por la entidad se sustenta en su compromiso misional (Recaudo, Servicio y Control) y se enmarca en el principio de la Integralidad y el Sistema de Gestión de Calidad y Control Interno, lo cual implica un gerenciamiento coordinado y equilibrado de los aspectos organizacionales de la entidad, sus procesos, recursos, talento humano e información, tal como se refleja en la figura 3.

Figura 3 Modelo de Gestión – MUISCA.

Fuente: Dirección de Impuestos y Aduanas Nacionales

El modelo de gestión MUISCA se basa en tres principios estratégicos que lo fundamentan y le dan solidez. Estos son: la integralidad, la unidad y la viabilidad y trascendencia.

La integralidad, como principio en dicho modelo de gestión, implica la administración coordinada y equilibrada de los aspectos administrativos, organizacionales y humanos de la entidad, generando así escenarios adecuados a la eficacia de la entidad.

El principio de unidad en el MUISCA conduce a la DIAN a una gestión enfocada por procesos, claramente identificados e interrelacionados, dando lugar a condiciones de gestión fundamentados en criterios técnicos que propician la eficiencia de la entidad y la calidad de sus productos y servicios.

La viabilidad y trascendencia como principios del MUISCA exigen de la DIAN una gestión enfocada estratégicamente, que hace viable el cumplimiento de sus responsabilidades como entidad pública, en ambientes complejos, cambiantes y multidimensionales.

De acuerdo a lo antes señalado y a los puntos estratégicos con los que está comprometida la DIAN, se establecen como requerimientos los siguientes: seguridad, accesibilidad, calidad TIC, confianza o empatía, fiabilidad, responsabilidad, capacidad de respuesta y tangibilidad; sus objetivos se resumen así:

- Seguridad: Se buscan servicios más seguros, que protejan los datos personales de los contribuyentes, la integridad de su información además de su intimidad y se eviten ataques que expongan la información del contribuyente.

- Accesibilidad: Se pretende servicios más accesibles, que eliminen cualquier tipo de barrera de exclusión, incluso para los contribuyentes que no tengan una formación técnica avanzada en materia de impuestos y que faciliten la integración progresiva de todos los tipos de contribuyentes, de manera que puedan optar por los beneficios que ofrece la DIAN en cuanto a sus obligaciones impositivas.

- Calidad TIC: La DIAN promueve que sus servicios sean cada vez de mayor calidad, que se pueda garantizar unos mejores niveles de servicio y de esta manera tener una mayor robustez en sus sistemas y seguir adicionando servicios y a su vez que los actuales evolucionen.

- Confianza o empatía: Muestra de interés y nivel de atención individualizada que ofrece la DIAN a sus ciudadanos/clientes (agrupa criterios de accesibilidad, comunicación y compresión del ciudadano/cliente).

- Fiabilidad: Habilidad para ejecutar el servicio prometido de forma fiable y cuidadosa.

- Responsabilidad: Seguridad, conocimiento y atención de los empleados de la DIAN y su habilidad para inspirar credibilidad y confianza (agrupa criterios de profesionalidad, cortesía, credibilidad).

- Capacidad de respuesta: Disposición de la DIAN para ayudar a los ciudadanos/clientes y para prestarles un servicio rápido.

- Tangibilidad: Apariencia de las instalaciones físicas, equipos, personal y materiales de comunicación.

3. ANALISIS DE LA INFORMACION.

3.1 ANALISIS DIFERENCIAL

Se puede establecer el desempeño de la entidad a través de criterios que permitan evaluar procedimientos internos, controles, mejores prácticas y rutinas. Siguiendo el anexo A de la norma 27001 donde se definen los mínimos controles para una adecuada gestión de la información se puede mostrar el estado actual, las posibles deficiencias, lo que se debe cumplir y el progreso en el cumplimiento del estándar 27001.

Se define la escala de madurez definido por el estándar COBIT:

Tabla 1 Escala de valoración del nivel de madurez.

Escala para valoración nivel maduración ISO 27001		
Escala	**%**	**Descripción**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Definido	60	Los procesos y los controles se documentan y se comunican. Es poco probable la detección de desviaciones.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente: Autoría propia

Teniendo en cuenta una media de cumplimiento para cada uno de los controles de los 11 dominios y de acuerdo a la escala de valoración del nivel de madurez definida anteriormente se presenta la siguiente tabla resumen de cumplimiento de controles hace tres años.

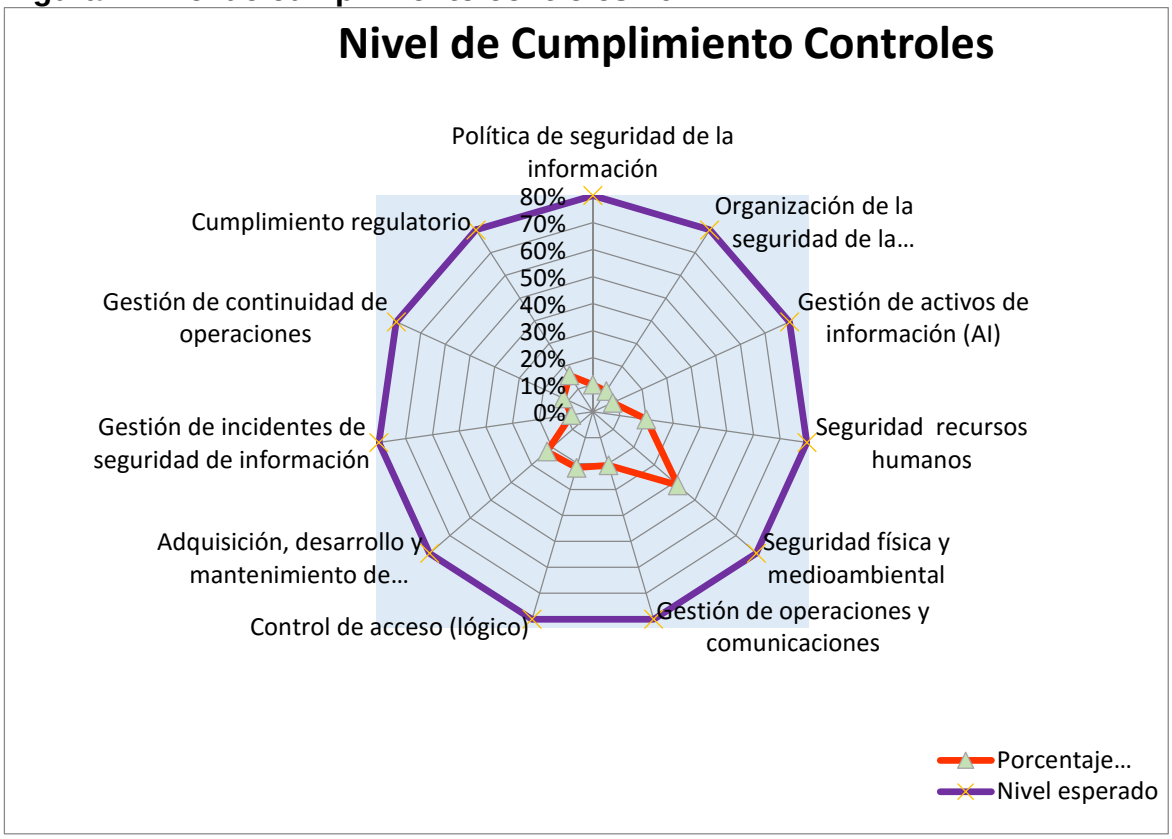
Tabla 2 Nivel de cumplimiento Controles 2012

	Cumplimiento		
Dominio	**Valor**	**Porcentaje**	**Objetivo**
Política de seguridad de la información	Inicial	10%	80%
Organización de la seguridad de la información	Inicial	9%	80%
Gestión de activos de información (AI)	Inicial	8%	80%
Seguridad recursos humanos	Inicial	20%	80%
Seguridad física y medioambiental	Definido	42%	80%
Gestión de operaciones y comunicaciones	Inicial	21%	80%
Control de acceso (lógico)	Repetible	22%	80%
Adquisición, desarrollo y mantenimiento de sistemas de información	Repetible	23%	80%
Gestión de incidentes de seguridad de información	Inicial	8%	80%
Gestión de continuidad de operaciones	Inicial	12%	80%
Cumplimiento regulatorio	Inicial	16%	80%
Promedio		17%	

Fuente: Autoría propia

Se grafican los datos correspondientes a la tabla 2:

Figura 4 Nivel de cumplimiento controles 2012



Fuente: Autoría propia.

El dominio de seguridad física y medioambiental es el único destacable dentro de los niveles de cumplimiento para los diferentes controles, se identifica la falta de controles en casi todos los demás dominios.

3.2 DESCRIPCIÓN DE LA METODOLOGÍA DE EVALUACIÓN DE RIESGOS SELECCIONADA

La metodología seleccionada para el análisis del riesgo es MAGERIT, esta metodología fue elaborada por el Ministerio de Administraciones Públicas con el fin de ayudar a todas las administraciones públicas del Estado español a mejorar diversos aspectos y puede ser aplicada a cualquier organización en el mundo.

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.

2. Determinar a qué amenazas están expuestos aquellos activos.

3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

3.3 IDENTIFICACIÓN DE LOS ACTIVOS.

La metodología Magerit agrupa los activos de acuerdo a su función, de la siguiente forma:

- **Datos** que materializan la información.

- **Servicios** auxiliares que se necesitan para poder organizar el sistema.

- **Las aplicaciones** informáticas (software) que permiten manejar los datos.

- **Los equipos informáticos** (hardware) y que permiten hospedar datos, aplicaciones y servicios.

- **Los soportes de información** que son dispositivos de almacenamiento de datos.

- **El equipamiento auxiliar** que complementa el material informático.

- **Las redes de comunicaciones** que permiten intercambiar datos.

- **Las instalaciones** que acogen equipos informáticos y de comunicaciones.

- **Las personas** que explotan u operan todos los elementos anteriormente citados.

En la Tabla 4 se relacionan los activos identificados en la DIAN para el alcance inicial indicado.

Tabla 3 Identificación de activos

TIPO DE ACTIVO	NOMBRE DEL ACTIVO
DATOS / INFORMACION	1. [BD_ALFA] Base Datos Alfa 2. [BD_BETA] Base Datos Beta 3. [BD_GAMMA] Base Datos Gamma 4. [BD_DELTA] Base de datos Delta 5. [BD_ZETA] Base de datos Zeta
SOFTWARE	6. [SOFT_OEM] Oracle Enterprise Manager 7. [SOFT_RAC] Oracle RAC 8. [SOFT_HMC] Particionamiento
SERVICIOS	9. [SERV_DA] Autenticación DA 10. [SERV_INFOR] Aplicaciones 11. [POR_WEB] Portal Web 12. [SERV_SO] Sistemas Operativos
APLICACIONES	13. [APL_JB] Aplicaciones en JBOSS 14. [ANT_VIR] Anti virus
EQUIPOS DE COMPUTO	15. [SRV_FIRE] Servidor de Firewall UTM 16. [SRV_BD] IBM 795 17. [SRV_HV] Hyper V. Virtualización 18. [EST_WORK] Estaciones de trabajo
COMUNICACIONES	19. [MPLS] Conexión a internet 20. [SAN] Red SAN
EQUIPAMIENTO AUXILIAR	21. [LIB_RES] Librerías respaldo
INSTALACIONES	22. [CC_LOC] Centro de Computo Local 23. [CC_ALT] Centro Alterno
PERSONAL	24. [G_ADM_BD] Grupo Base de Datos 25. [G_ADM_SO] Grupo Sistemas Operativos

Fuente: Autoría propia

3.3.1 Valoración de los activos

Teniendo en cuenta las dimensiones de seguridad: Disponibilidad, integridad, confiabilidad, autenticidad, y trazabilidad, considerados en la metodología Magerit.

Una valoración cualitativa y donde el impacto en caso de daño o pérdida maneja en una escala de criterios: muy alto (MA), alto (A), medio (M), bajo (B) y despreciable (D).

Tabla 4 Criterios de valoración

Valor			Criterio
10	Muy alto	MA	Daño muy grave a la organización.
7-9	Alto	A	Daño grave a la organización.
4-6	Medio	M	Daño importante a la organización.
1-3	Bajo	B	Daño menor a la organización.
0	Despreciable	D	Irrelevante a efectos prácticos.

Fuente: Autoría propia

Tabla 5 Valoración de Activos Tipo: Datos / Información

Activo	Dimensiones de Seguridad				
	[D] Disponibilidad	[I] Integridad	[C] Confiabilidad	[A] Autenticidad	[T] Trazabilidad
[BD_A] Base datos Oracle Alfa	10	9	9	7	7
[BD_B] Base datos Oracle Beta	10	9	9	7	7
[BD_G] Base datos Oracle Gamma	5	7	7	7	5
[BD_G] Base datos Oracle Delta	5	4	4	2	2
[BD_Z] Base datos Oracle Zeta	5	4	4	2	2
[O_DBE] Oracle Database Emterprise 11G	3				
[O_RAC] Oracle RAC	3				
[SO_AIX] AIX 7	3				
[STORAGE] IBM DS 8800	3				
[SERV_AIX] Servidores IBM 795	3				
[Red_Lan] Red Lan	3				
[Red_San] Red San	3				
[ING_BD] Ingenieros Bases de Datos	3				

Fuente: Autoría propia

3.4 ANÁLISIS DE AMENAZAS

Las amenazas son aquellas situaciones que podrían llegar a darse en una organización y que resultarían en un problema de seguridad. Se clasifican en:

- Accidentes: situaciones no provocadas voluntariamente y que generalmente no pueden evitarse. Pueden ser de los siguientes tipos: accidente físico, avería, interrupción de servicios esenciales, accidentes mecánicos o electromagnéticos.

- Errores: situaciones cometidas de forma involuntaria, por el desarrollo de las actividades propias de la empresa, ya sea por desconocimiento o descuido del personal o terceros. Dentro de estos se pueden encontrar: errores en la utilización de los sistemas, en el desarrollo de aplicaciones, de actualización en los sistemas o aplicaciones, en la monitorización, de compatibilidad entre aplicaciones, inesperados (virus, troyanos, etc.).

- Amenazas intencionales presenciales: provocadas por el personal de la empresa de forma voluntaria, al realizar acciones que saben que provocan un daño ya sea físico o lógico. Se pueden encontrar las siguientes: acceso físico no autorizado, acceso lógico no autorizado, indisponibilidad de recursos, filtración de datos a terceros.

- Amenazas intencionales remotas: provocadas por personas ajenas a la empresa y que consiguen dañarla. Se pueden encontrar, entre otras, las siguientes: acceso lógico no autorizado, suplantación del origen en una comunicación, gusanos, denegación de servicio.

Tabla 6 Amenazas

TIPO DE ACTIVO	NOMBRE DEL ACTIVO	AMENAZAS
DATOS / INFORMACION	1. [BD_ALFA] Base Datos Alfa 2. [BD_BETA] Base Datos Beta 3. [BD_GAMMA] Base Datos Gamma 4. [BD_DELTA] Base de datos Delta 5. [BD_ZETA] Base de datos Zeta	Autenticacion, contraseñas por defecto
		Fallo Electrico
		Daño de los datos
		Degradacion de la BD
		Sustraccion de los datos
		Errores de los usuarios
		Errores del administrador
		Errores de monitorización
		Errores de configuración
SOFTWARE	6. [SOFT_OEM] Oracle Enterprise Manager 7. [SOFT_RAC] Oracle RAC 8. [SOFT_HMC] Particionamiento	Modificacion Binarios
		Errores de configuracion
		Daño Particiones
SERVICIOS	9. [SERV_DA] Autenticación DA 10. [SERV_INFOR] Aplicaciones 11. [POR_WEB] Portal Web 12. [SERV_SO] Sistemas Operativos	Vencimiento Certificados de Autenticacion
		Instalacion Trotayanos
		Saturacion Conexiones
		Denegacion del servicio
APLICACIONES	13. [APL_JB] Aplicaciones en JBOSS 14. [ANT_VIR] Anti virus	Inyeccion de Codigo
		Falla en la Actualizacion
		Nuevos Virus
EQUIPOS DE COMPUTO	15. [SRV_FIRE] Servidor de Firewall UTM 16. [SRV_BD] IBM 795 17. [SRV_HV] Hyper V. Virtualización 18. [EST_WORK] Estaciones de trabajo	Desastres Naturales
		Uso no previsto
		Averia de origen fisico o logico
		Obsolecencia
		Condiciones inadecuadas de temperatura y/o humedad
COMUNICACIONES	19. [MPLS] Conexión a internet 20. [SAN] Red SAN	Sin servicio por proveedor
		Ataque destructivo
EQUIPAMIENTO AUXILIAR	21. [LIB_RES] Librerías respaldo	Fallos fisicos
INSTALACIONES	22. [CC_LOC] Centro de Computo Local 23. [CC_ALT] Centro Alterno	Accesos no aurtorizados, daños por agua o fuego
		Desastres Naturales
PERSONAL	24. [G_ADM_BD] Grupo Base de Datos 25. [G_ADM_SO] Grupo Sistemas Operativos	Errores de configuracion
		Ingenieria social, extorsion

Fuente: Autoría propia

3.5 RIESGO INHERENTE

El **riesgo inherente** es al que se enfrentan las entidades antes de asumir acciones que permitan reducir la probabilidad de ocurrencia o impacto.

Definimos un rango de probabilidad o frecuencia del riesgo y un rango de impacto, con los cuales generaremos una tabla de la valoración del riesgo.

3.5.1 Valores de frecuencias del riesgo

Tabla 7 Probabilidad de la frecuencia

FRECUENCIA	
PROBABILIDAD	VALOR
ALTA	3
MEDIA	2
BAJA	1

Fuente: Autoría propia

3.5.2 Valores de impacto del riesgo

Tabla 8 Clasificación del impacto

IMPACTO			
CLASIFICACION	Leve	Moderado	Catastrófica
VALOR	5	10	20

Fuente: Autoría propia

De acuerdo a los valores de los vectores de probabilidad e impacto obtenemos una tabla de valoración de riesgos.

Tabla 9 Valoración del riesgo

VALORACION RIESGO	
CLASIFICACION	CALIFICACION
GRAVE	[41 - 60]
ALTO	[21 -40]
MODERADO	[11 -20]
BAJO	[1 -10]

Fuente: Autoría propia

Con las tablas de Frecuencia impacto y valoración del riesgo se obtiene la tabla de medición de riesgos con la cual identificamos la zona del riesgo y las posibles tácticas que se usarán para mitigar el riesgo.

Tabla 10 Medición del riesgo

	IMPACTO	Catastrofico	Moderado	leve
	VALOR	20	10	5
FRECUENCIA	VALOR			
Alta	3	60 Zona Inaceptable Evitar, Reducir, Compartir o trasferir el riesgo	30 Zona Importante Evitar, Reducir, Compartir o trasferir el riesgo	15 Zona Moderada Evitar el riesgo
Media	2	40 Zona Importante Evitar, Reducir, Compartir o trasferir el riesgo	20 Zona Moderada Evitar, Reducir, Compartir o trasferir el riesgo	0 Zona Tolerable Reducir o asumir el riesgo
Baja	1	20 Zona Moderada Evitar, Reducir, Compartir o trasferir el riesgo	10 Zona Tolerable Reducir, Compartir o trasferir el riesgo	5 Zona Aceptable asumir el riesgo

Fuente: Autoría propia

Una vez realizado el análisis de riesgos tenemos herramientas para generar un diagnóstico sobre el estado de la seguridad.

Tabla 11 Riesgos Inherentes.

			RIESGO INHERENTE					
TIPO DE ACTIVO	NOMBRE DEL ACTIVO	AMENAZAS	FRECUENCIA	IMPACTO	TOTAL	ZONA	ESTRATEGIA A USAR	VULNERABILIDAD
DATOS / INFORMACION	1. [BD_ALFA] Base Datos Alfa 2. [BD_BETA] Base Datos Beta 3. [BD_GAMMA] Base Datos Gamma 4. [BD_DELTA] Base de datos Delta 5. [BD_ZETA] Base de datos Zeta	Autenticacion, contraseñas por defecto	2	20	40	IMPORTANTE	Evitar o Reducir	ALTA
		Fallo Electrico	1	20	20	MODERADO	Evitar, Reducir, Compartir o Transferir	MEDIA
		Daño de los datos	3	20	60	INACEPTABLE	Evitar o Reducir	ALTA
		Degradacion de la BD	1	20	20	MODERADO	Evitar, Reducir o Compartir	MEDIA
		Sustraccion de los datos	1	20	20	MODERADO	Evitar, Reducir o Compartir	MEDIA
		Errores de los usuarios	2	10	20	MODERADO	Evitar, Reducir o Compartir	MEDIA
		Errores del administrador	1	10	10	TOLERABLE	Asumir o Reducir	BAJA
		Errores de monitorización	1	10	10	TOLERABLE	Asumir o Reducir	BAJA
		Errores de configuración	1	20	20	MODERADO	Evitar, Reducir, Compartir o Transferir	MEDIA
SOFTWARE	6. [SOFT_OEM] Oracle Enterprise Manager 7. [SOFT_RAC] Oracle RAC 8. [SOFT_HMC] Particionamiento	Modificacion Binarios	2	20	40	IMPORTANTE	Evitar, Reducir, o Compartir	ALTA
		Errores de configuracion	2	20	40	IMPORTANTE	Evitar, Reducir, Compartir o Transferir	ALTA
		Daño Particiones	1	10	10	TOLERABLE	Asumir, Reducir o Compartir	BAJA
SERVICIOS	9. [SERV_DA] Autenticación DA 10. [SERV_INFOR] Aplicaciones 11. [POR_WEB] Portal Web 12. [SERV_SO] Sistemas Operativos	Vencimiento Certificados de Autenticacion	1	10	10	TOLERABLE	Asumir, Reducir o Compartir	BAJA
		Instalacion Trotayanos	2	20	40	IMPORTANTE	Evitar, Reducir o Compartir	ALTA
		Saturacion Conexiones	1	20	20	MODERADO	Evitar, Reducir, Compartir o Transferir	MEDIA
		Denegacion del servicio	2	20	40	IMPORTANTE	Evitar, Reducir, Compartir o Transferir	ALTA
APLICACIONES	13. [APL_JB] Aplicaciones en JBOSS 14. [ANT_VIR] Anti virus	Inyeccion de Codigo	2	20	40	IMPORTANTE	Evitar, Reducir, Compartir o Transferir	MEDIA
		Falla en la Actualizacion	2	10	20	MODERADO	Evitar, Reducir, Compartir o Transferir	MEDIA
		Nuevos Virus	1	10	10	TOLERABLE	Asumir o Reducir	BAJA
EQUIPOS DE COMPUTO	15. [SRV_FIRE] Servidor de Firewall UTM 16. [SRV_BD] IBM 795 17. [SRV_HV] Hyper V. Virtualización 18. [EST_WORK] Estaciones de trabajo	Desastres Naturales	1	20	20	MODERADO	Evitar, Reducir, Compartir o Transferir	MEDIA
		Uso no previsto	1	20	20	MODERADO	Evitar o Reducir	MEDIA
		Averia de origen fisico o logico	1	10	10	TOLERABLE	Evitar, Reducir, Compartir o Transferir	BAJA
		Obsolecencia	2	10	20	MODERADO	Evitar, Reducir, Compartir o Transferir	MEDIA
		Condiciones inadecuadas de temperatura y/o humedad	1	10	10	TOLERABLE	Evitar o Reducir	BAJA
COMUNICACIONES	19. [MPLS] Conexión a internet 20. [SAN] Red SAN	Sin servicio por proveedor	1	20	20	MODERADO	Compartir o Trasferir	MEDIA
		Ataque destructivo	1	20	20	MODERADO	Evitar, Reducir, Compartir o Transferir	MEDIA
EQUIPAMIENTO AUXILIAR	21. [LIB_RES] Librerías respaldo	Fallos fisicos	1	5	5	ACEPTABLE	Evitar, Reducir, Compartir o Transferir	BAJA
INSTALACIONES	22. [CC_LOC] Centro de Computo Local 23. [CC_ALT] Centro Alterno	Accesos no aurtorizados, daños por agua o fuego	1	20	20	MODERADO	Evitar, Reducir, Compartir o Transferir	MEDIA
		Desastres Naturales	1	20	20	MODERADO	Evitar, Reducir, Compartir o Transferir	MEDIA
PERSONAL	24. [G_ADM_BD] Grupo Base de Datos 25. [G_ADM_SO] Grupo Sistemas Operativos	Errores de configuracion	1	10	10	TOLERABLE	Asumir, Reduciir	BAJA
		Ingenieria social, extorsion	1	20	20	MODERADO	Evitar, Reducir, Compartir o Transferir	MEDIA

Fuente: Autoría Propia

En el análisis de riesgos inherentes para el activo de los datos/información tiene una zona inaceptable y una zona importante con vulnerabilidad alta en daños de los datos y autenticación de contraseñas.

Los activos de software también tiene una zona importante con vulnerabilidad alta para la modificación de binarios y errores de configuración.

En los activos de servicios tanto la instalación de troyanos y la denegación de servicio también se ubican en una zona importante y una vulnerabilidad alta.

En los activos de aplicaciones la inyección de código está en una zona importante y vulnerabilidad alta.

Los equipos de cómputo están en zona moderada o tolerable lo que nos ubica en una vulnerabilidad media o baja, se debe tener muy presente el tema de la obsolescencia.

El activo de comunicaciones en una zona moderada con vulnerabilidad media se les debe prestar atención.

El activo de equipamiento auxiliar se encuentra en una zona aceptable y vulnerabilidad baja.

Las instalaciones con una vulnerabilidad media y en una zona de riesgo moderado.

Para el activo de personal se debe revisar el tema de ingeniería social y extorsión ya que se encuentra en una zona de riesgo moderado y una vulnerabilidad media.

A los riesgos inherentes anteriormente identificados no se le han aplicado controles.

3.6 RIESGO RESIDUAL

Una vez aplicado el control sigue existiendo un riesgo, a este tipo de riesgo se denomina riesgo residual, por lo tanto al aplicar la salvaguarda o el control hemos modificado el riesgo desde un valor potencial a un valor residual. Es de anotar que el riesgo en la organización nunca podrá erradicarse en su totalidad. El riesgo residual refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente.

Tabla 12 Medición del riesgo.

	IMPACTO	Catastrofico	Moderado	leve
	VALOR	20	10	5
FRECUENCIA	VALOR			
Alta	3	60 Zona Inaceptable Evitar, Reducir, Compartir o trasferir el riesgo	30 Zona Importante Evitar, Reducir, Compartir o trasferir el riesgo	15 Zona Moderada Evitar el riesgo
Media	2	40 Zona Importante Evitar, Reducir, Compartir o trasferir el riesgo	20 Zona Moderada Evitar, Reducir, Compartir o trasferir el riesgo	0 Zona Tolerable Reducir o asumir el riesgo
Baja	1	20 Zona Moderada Evitar, Reducir, Compartir o trasferir el riesgo	10 Zona Tolerable Reducir, Compartir o trasferir el riesgo	5 Zona Aceptable asumir el riesgo

Fuente: Autoría propia

Utilizamos nuevamente la tabla de medición del riesgo, buscando determinar qué tan efectivo ha sido los controles aplicados al riesgo inherente

Tabla 13 Riesgo residual

			CONTROLES DE		RIESGO RESIDUAL					
TIPO DE ACTIVO	NOMBRE DEL ACTIVO	AMENAZAS	FRECUENCIA	IMPACTO	FRECUENCIA	IMPACTO	TOTAL	ZONA	ESTRATEGIA A USAR	VULNERABILIDAD
DATOS / INFORMACION	1. [BD_ALFA] Base Datos Alfa 2. [BD_BETA] Base Datos Beta 3. [BD_GAMMA] Base Datos Gamma 4. [BD_DELTA] Base de datos Delta 5. [BD_ZETA] Base de datos Zeta	Autenticacion, contraseñas por defecto	Politicas de seguridad, copias de seguridad, tuning (afinamiento)	Plan de contingencia	1	20	20	MODERADO	Evitar o Reducir	MEDIA
		Fallo Electrico			1	10	10	TOLERABLE	Asumir o Reducir	BAJA
		Daño de los datos			1	10	10	TOLERABLE	Asumir o Reducir	BAJA
		Degradacion de la BD			1	10	10	TOLERABLE	Asumir o Reducir	BAJA
		Sustraccion de los datos			1	10	10	TOLERABLE	Asumir o Reducir	BAJA
		Errores de los usuarios			1	5	5	ACEPTABLE	Asumir o Reducir	BAJA
		Errores del administrador			1	10	10	TOLERABLE	Asumir o Reducir	BAJA
		Errores de monitorización			1	10	10	TOLERABLE	Asumir o Reducir	BAJA
		Errores de configuración			1	10	10	TOLERABLE	Asumir o Reducir	BAJA
SOFTWARE	6. [SOFT_OEM] Oracle Enterprise Manager 7. [SOFT_RAC] Oracle RAC 8. [SOFT_HMC] Particionamiento	Modificacion Binarios	Politicas de seguridad, copias de seguridad, inspeccion	Soporte contratista	1	20	20	MODERADO	Evitar, Reducir, o Compartir	MEDIA
		Errores de configuracion			1	20	20	MODERADO	Evitar, Reducir, o Compartir	MEDIA
		Daño Particiones			1	5	5	ACEPTABLE	Asumir o Reducir	BAJA
SERVICIOS	9. [SERV_DA] Autenticación DA 10. [SERV_INFOR] Aplicaciones 11. [POR_WEB] Portal Web 12. [SERV_SO] Sistemas Operativos	Vencimiento Certificados de Autenticacion	Analisis de trafico, mantenimiento correctivo y preventivo, revisión de roles de usuarios, politicas de seguridad	SGSI	1	5	5	ACEPTABLE	Asumir, Reducir o Compartir	BAJA
		Instalacion Trotayanos			1	10	10	TOLERABLE	Asumir, Reducir o Compartir	BAJA
		Saturacion Conexiones			1	10	10	TOLERABLE	Asumir, Reducir o Compartir	BAJA
		Denegacion del servicio			1	10	10	TOLERABLE	Evitar, Reducir, Compartir o Transferir	BAJA
APLICACIONES	13. [APL_JB] Aplicaciones en JBOSS 14. [ANT_VIR] Anti virus	Inyeccion de Codigo	Mantenimiento correctivo y preventivo, Politicas de seguridad, seguridad perimetral	SGSI	1	10	10	TOLERABLE	Asumir o Reducir	BAJA
		Falla en la Actualizacion			1	5	5	ACEPTABLE	Asumir o Reducir	BAJA
		Nuevos Virus			1	10	10	TOLERABLE	Asumir o Reducir	BAJA
EQUIPOS DE COMPUTO	15. [SRV_FIRE] Servidor de Firewall UTM 16. [SRV_BD] IBM 795 17. [SRV_HV] Hyper V. Virtualización 18. [EST_WORK] Estaciones de trabajo	Desastres Naturales	Mantenimiento correctivo y preventivo (TERCEROS)	Plan de contingencia	1	5	5	ACEPTABLE	Asumir o Reducir	BAJA
		Uso no previsto			1	5	5	ACEPTABLE	Asumir o Reducir	BAJA
		Averia de origen fisico o logico			1	5	5	ACEPTABLE	Asumir o Reducir	BAJA
		Obsolecencia			1	5	5	ACEPTABLE	Asumir o Reducir	BAJA
		Condiciones inadecuadas de temperatura y/o humedad			1	5	5	ACEPTABLE	Asumir o Reducir	BAJA
COMUNICACIONES	19. [MPLS] Conexión a internet 20. [SAN] Red SAN	Sin servicio por proveedor	Mantenimiento correctivo y preventivo, Politicas de seguridad, seguridad perimetral	Plan de contingencia	1	5	5	ACEPTABLE	Asumir o Reducir	BAJA
		Ataque destructivo			1	5	5	ACEPTABLE	Asumir o Reducir	BAJA
EQUIPAMIENTO AUXILIAR	21. [LIB_RES] Librerías respaldo	Fallos fisicos	Mantenimiento correctivo y preventivo, Politicas de seguridad, copias de seguridad, sistemas de detección, seguridad perimetral , antivirus.	Soporte contratista	1	10	10	TOLERABLE	Asumir, Reducir o Compartir	BAJA
INSTALACIONES	22. [CC_LOC] Centro de Computo Local 23. [CC_ALT] Centro Alterno	Accesos no aurtorizados, daños por agua o fuego	liticas de seguridad, seguridad perimetral, sistemas de detección	Plan de contingencia	1	10	10	TOLERABLE	Asumir o Reducir	BAJA
		Desastres Naturales			1	10	10	TOLERABLE	Asumir o Reducir	BAJA
PERSONAL	24. [G_ADM_BD] Grupo Base de Datos 25. [G_ADM_SO] Grupo Sistemas Operativos	Errores de configuracion	Seguridad Perimetral, Politicas de claves seguras, Copias de seguridad, capacitaciones.	SGSI	1	10	10	TOLERABLE	Asumir o Reducir	BAJA
		Ingenieria social, extorsion			1	10	10	TOLERABLE	Asumir o Reducir	BAJA

Fuente: Autoría propia

3.7 TIPO DE MANEJO DE LOS RIESGOS

Para poder definir medidas de control antes se debe determinar qué manejo se le va a dar a los riesgos definidos, analizados y valorados en los pasos anteriores.

3.7.1 Evitar el riesgo

Es siempre la primera alternativa a considerar. Se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos.

3.7.2 Reducir el riesgo

Si el riesgo no puede ser evitado porque crea grandes dificultades operacionales, el paso a seguir es reducirlo al más bajo nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles. Ejemplo: Planes de contingencia.

3.7.3 Dispersar y atomizar el riesgo

Se logra mediante la distribución o localización del riesgo en diversos lugares. Es así como por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

3.7.4 Trasferir el riesgo

Hace referencia a buscar respaldo y compartir con otro parte del riesgo, como por ejemplo, tomar pólizas de seguros, así se traslada el riesgo a otra parte o

físicamente se traslada a otro lugar. Esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro, o de un grupo a otro. Así mismo, el riesgo puede ser minimizado compartiéndolo con otro grupo o dependencia.

3.7.5 Asumir el riesgo

Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Una vez establecidos cuáles de los anteriores manejos del riesgo se van a concretar, estos deben evaluarse con relación al beneficio/costo para definir, cuáles son susceptibles de ser aplicadas y proceder a elaborar el plan de manejo de riesgo, teniendo en cuenta, el análisis elaborado para cada uno de los riesgos de acuerdo con su impacto, probabilidad y nivel de riesgo.

Posteriormente se definen los responsables de llevar a cabo las acciones especificando el grado de participación de las dependencias en el desarrollo de cada una de ellas. Así mismo, es importante construir indicadores, entendidos como los elementos que permiten determinar de forma práctica el comportamiento de las variables de riesgo que van a permitir medir el impacto de las acciones.

Los riesgos que se identifican.

Tabla 14 Tratamiento a los riesgos.

RIESGO		TRATAMIENTO
DATOS/ INFORMACION		
R1.	Claves deficientes	Implementar controles
R2.	Implenetacion encripcion total delas bases de datos	Aceptar e implementar controles
R3.	Procesos de respaldo y restauracion completos	Implementar controles
R4.	Usuarios Autorizados y privilegiados	Aceptar y definir controles
R5.	Definicon de roles para los administradores de las Bases de Datos.	Implementar controles
SOFTWARE		
R6.	Inspección del software comercial.	Implementar controles, trasferir
R7.	Parches Actualizados	Aceptar e implementar controles
SERVICIO		
R8.	Implementación de seguridad lógica, Hacking	Implementar controles y aceptar
APLICACIONES		
R9.	Herramientas qu detecten codigo malicioso	Aceptar e implementar controles
R10.	Pruebas rigurosas de escritorio.	Implentar controles
EQUIPAMENTO		
R11.	Contratos de mantenimiento preventivo y correctivo	Implementar controles
INSTALACIONES		
R12.	Centro de cómputo alterno consolidado	Implementar controles, transferir
R13.	Ubicación centro Alterno	Aceptar e implementar controles
PERSONAL		
R14.	Personal y capacitación certificados	Establecer controles

Fuente: Autoría propia

3.8 TRATAMIENTO A LOS RIESGOS

3.8.1 Datos / Información

R1. Uso por parte de las usuarios de Claves obvias (longitud corta, números consecutivos, etc.) y/o uso de claves compartidas.

Existen usuarios de aplicación, administradores, y de consulta, estos últimos no se incluyeron dentro del proceso de control de claves por lo que sus claves no están cumpliendo con los mínimos requeridos. El control a aplicar es primero capacitar a dichos usuarios en el manejo de las claves y luego incluirlos en las políticas de control de claves.

R2. Falta Implementación de seguridad a nivel de encripción y cifrado de los datos.

Se observa que existe un proceso de encripción para algunas tablas que contiene información que se debe tratar como confidencial. Dicha información surte su proceso de encripción solamente en reposo, para lograr su encripción en línea se hace necesario actualizar la versión del motor Oracle a un reléase superior. Dada la complejidad del proceso se asume el riesgo y se implementan controles que custodien la información.

R3. Políticas de backup inadecuadas y procedimientos de restauración incompletos o sin las pruebas suficientes.

Aunque existen políticas de backup, el proceso de validación a dichos backup no se realizaba con un proceso y de manera periódica. Se crea una partición en el servidor ibm795 donde se implementan los script necesarios para que las pruebas de restauración y recuperación se puedan llevar a cabo sin afectar el servicio de producción.

R4. Falta de políticas de seguridad que limiten el acceso a los datos almacenados en las bases de datos Oracle de acuerdo a los diferentes tipos de usuarios autorizados.

Los usuarios de consulta en las bases de datos no tienen restricción referente a la información que pueden consultar pudiendo generar un riesgo de confidencialidad, se deben fijar políticas y controles para la autorización de dichos usuarios.

R5. Falta de perfiles funcionales que definan los diferentes permisos de acceso a los datos para los administradores de las Bases de Datos.

Se han definido unos perfiles o roles en la administración de las bases de datos Oracle, pero la carencia de personal impide que existan estos

perfiles nominalmente. Se asume el riesgo y se plantea la contratación de personal capacitado.

3.8.2 Software

R6. Manuales con procedimientos desactualizados para la inspección del software comercial.

Se deben implementar los controles necesarios para que los procedimientos existentes sean actualizados de manera constante.

R7. Actualización de seguridad al día, recomendadas por los proveedores.

Se asume el riesgo y se implementan controles que permitan instalar de manera controlada las actualizaciones necesarias u obligatorias que minimicen riesgos.

3.8.3 Servicios

R8. Implementación de seguridad lógica, Hacking

Se implementan controles que permiten asegurar adecuados mantenimientos.

3.8.4 Aplicaciones

R9. Falta de Herramientas que detecten código malicioso.

R10. Implementación de pruebas rigurosas de escritorio.

Tanto para el riesgo R9 y R10 se acepta el riesgo, la gran cantidad de solicitudes de cambio de software y la falta de herramientas y personal calificado para auditar el software desarrollado en casa no permiten activar controles que reduzcan el riesgo sustancialmente

3.8.5 Equipamiento

R11. Deficiencia en contratos de mantenimiento preventivo y correctivo.

Se implementan controles que permiten dar a los contratos de mantenimiento preventivo y correctivo el alcance suficiente para reducir el riesgo a una zona aceptable.

3.8.6 Instalaciones

R12. Falta de un centro de cómputo alterno consolidado para manejo de la contingencia.

R13. Mejor distribución geográfica que mitigue los desastres naturales.

Se acepta el riesgo. La información manejada por la DIAN es altamente confidencial y se deben realizar estudios para contratar un hosting que mantengan esta confidencialidad. Se debe implementar controles que permitan tener un centro de cómputo alterno para todos los activos.

3.8.7 Personal

R14. Falta de personal y capacitación certificada.

Implementar controles que obliguen a la alta gerencia a tomar medidas con respecto al personal que interviene con las bases de datos.

4. OBSERVACIONES PARA APLICACIÓN DE CONTROLES

De acuerdo a la gráfica 4 se puede identificar la falta de controles en casi todos los dominios, algunos de los puntos que podemos destacar son:

4.1 Políticas de la seguridad de la información.

- Debe redactarse, aprobarse y difundirse una política de seguridad de la información que refleje la misión y visión de la Entidad.

4.2 Organización de la seguridad de la información.

- Se debe definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización; implementar y actuar en concordancia con las políticas de seguridad de la información de la Entidad; proteger los datos en contra de acceso, divulgación, modificación, destrucción o interferencia no autorizada.

- Se debe tener relación con grupos o foros de seguridad especializados.

- Se deben tener en cuenta todos los aspectos que puedan representar un riesgo de seguridad para la información corporativa.

4.3 Seguridad de Recursos Humanos

- Se debe verificar los documentos de acuerdo a la normatividad vigente y relevante al empleo y chequeo de la Hoja de vida, certificaciones de estudio y laborales.

- Definir roles y responsabilidades en concordancia con la política de seguridad de la información de la Entidad.

- Los usuarios empleados, contratistas y terceros debieran aceptar y firmar un contrato con los términos y condiciones de su empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.

- Antes de darse acceso a los sistemas de información se deben informar los roles y responsabilidades de seguridad.

4.4 Gestión de Activos de información

- Se debe identificar todos los activos y documentar la importancia de estos activos. El inventario de los activos debiera incluir toda la información necesaria para poder recuperarse de un desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial.

- Toda la información y los activos asociados con los medios de procesamiento de información deben ser propiedad de un asignado de la organización. Se debe clasificar apropiadamente los activos asociados con los medios de procesamiento de la información.

- Se debe seguir reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información por parte de todos los servidores.

- Se debe devolver todos los activos de la organización a la terminación del empleo, contrato o acuerdo. El proceso de desvinculación debe ser formalizado para incluir la devolución de todo el software, documentos corporativos y equipo entregado previamente. También se debieran devolver otros activos como dispositivos de cómputo móviles, tarjetas de crédito, tarjetas de acceso, software, manuales e información almacenada en medios electrónicos.

4.5 La seguridad física y medioambiental

- Se debe instalar perímetros de seguridad (paredes, mecanismos controlados por tarjetas o personas) para proteger las áreas que contienen información y medios de procesamiento de información.

- Se debe implementar controles de ingreso que permita el acceso al personal autorizado, con registro de fecha y hora de entrada y salida, con propósitos específicos y autorizados; solo personal autorizado tiene acceso a las áreas de proceso y almacenamiento de información.

- Se debe asignar y aplicar protección física contra incendio, inundación, terremoto, explosión, ataques de orden público por civiles, y otras formas de desastres naturales y/o causados por el hombre.

- Se debe estar al tanto de la existencia o actividades dentro del área asegurada; aquellas áreas vacías deben ser cerradas bajo llave; no se debe permitir el uso de equipo fotográfico, de video, audio y otro equipo de grabación.

- Se debe restringir a personal autorizado e identificado las zonas de entrega y carga desde el exterior.

4.6 Gestión de operaciones y Comunicaciones

- Se debe documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten.

- Los procedimientos de operación debieran especificar las instrucciones para la ejecución detallada de cada trabajo tales como:

    1. Procedimiento Manejo de información.
    2. Copia de seguridad o respaldo.
    3. Requerimientos de programación de horarios, incluyendo las interdependencias con otros sistemas, los tiempos de culminación y horarios de los primeros y últimos trabajos.
    4. Instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema.
    5. Contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas.
    6. Procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema.
    7. La gestión de la información del rastro de auditoría y registro del sistema.

- Se deben separar los recursos para el desarrollo, prueba y producción, es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.

4.7 Control de Acceso

- Se debe restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

- Se debe desconectar las sesiones tras un determinado periodo de inactividad.

- Se debe controlar la asignación de contraseñas mediante un proceso de gestión formal.

- Se debe controlar estrictamente el acceso al código fuente de los programas y los ítems asociados para evitar la introducción de una funcionalidad no-autorizada y para evitar cambios no-intencionados.

- Se debe utilizar controles cifrados en conformidad con todos acuerdos, leyes y regulaciones pertinentes.

- Se debe establecer una gestión de las claves que respalde el uso de las técnicas criptográficas.

4.8 Desarrollo, Mantenimiento y adquisición de Sistemas de Información

- Debe existir un procedimiento para el control del cambio.

- Se debe enunciar los requerimientos de los controles de seguridad para los sistemas de información en los requerimientos técnicos mínimos; los requerimientos de seguridad deben reflejar el valor económico de los activos de información involucrados y el daño potencial de una falla o ausencia de seguridad; ejecutar procesos de prueba a los productos adquiridos.

- Deben generarse y obtener certificados de claves públicas, así como verificar su autenticidad; se debe establecer controles que permitan salvaguardar la confidencialidad y la integridad de los datos que pasan a través de la red pública.

- Los paquetes de software no deben sufrir modificaciones; si se modifican, se debe contemplar la posibilidad de obtener del proveedor las actualizaciones, definir quien hará el mantenimiento y los riesgos de comprometer funcionalidad original.

4.9 Gestión de Incidentes de Seguridad Información.

- Se debe garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas.

- Se debe utilizar la información obtenida de la evaluación de los incidentes en la seguridad de la información para identificar los incidentes recurrentes o de alto impacto.

4.10 Gestión de Continuidad del Negocio

- Se debieran desarrollar e implementar planes para restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción, o falla, de los procesos comerciales críticos.

- Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempos requeridos, tras la interrupción o fallo de los procesos críticos de negocio.

- Se deberían probar regularmente los planes de continuidad del negocio para garantizar su actualización y eficacia.

4.11 Cumplimiento Regulatorio

- Se debe proteger los registros importantes de pérdida, destrucción, falsificación; en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.

- Se debiera asegurar la protección y privacidad de la data conforme lo requiera la legislación, regulaciones y, si fuesen aplicables, las cláusulas contractuales relevantes.

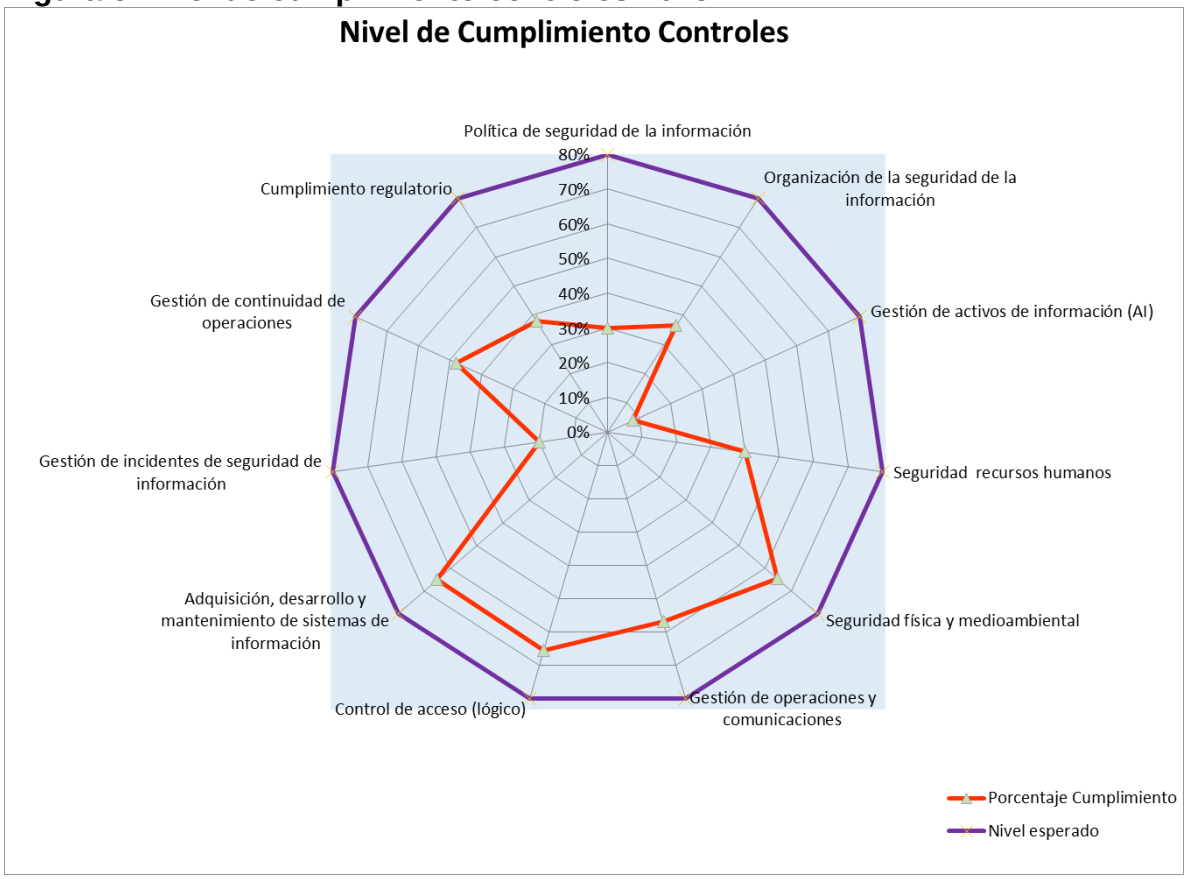
- Se debe considerar el cumplimiento de la normatividad vigente para las restricciones sobre la utilización de la codificación; métodos obligatorios o voluntarios para que las autoridades de los países tengan acceso a la información codificada por hardware o software para proporcionar confidencialidad del contenido.

Tabla 15 Nivel de cumplimiento Controles 2015.

	Cumplimiento		
Dominio	Valor	Porcentaje	Objetivo
Política de seguridad de la información	Repetible	30%	80%
Organización de la seguridad de la información	Repetible	36%	80%
Gestión de activos de información (AI)	Inicial	16%	80%
Seguridad recursos humanos	Repetible	40%	80%
Seguridad física y medioambiental	Definido	65%	80%
Gestión de operaciones y comunicaciones	Definido	57%	80%
Control de acceso (lógico)	Gestionado	66%	80%
Adquisición, desarrollo y mantenimiento de sistemas de información	Gestionado	65%	80%
Gestión de incidentes de seguridad de información	Inicial	20%	80%
Gestión de continuidad de operaciones	Definido	48%	80%
Cumplimiento regulatorio	Repetible	38%	80%
Promedio		44%	

Fuente: Autoría propia.

Figura 5 Nivel de cumplimiento controles 2015.

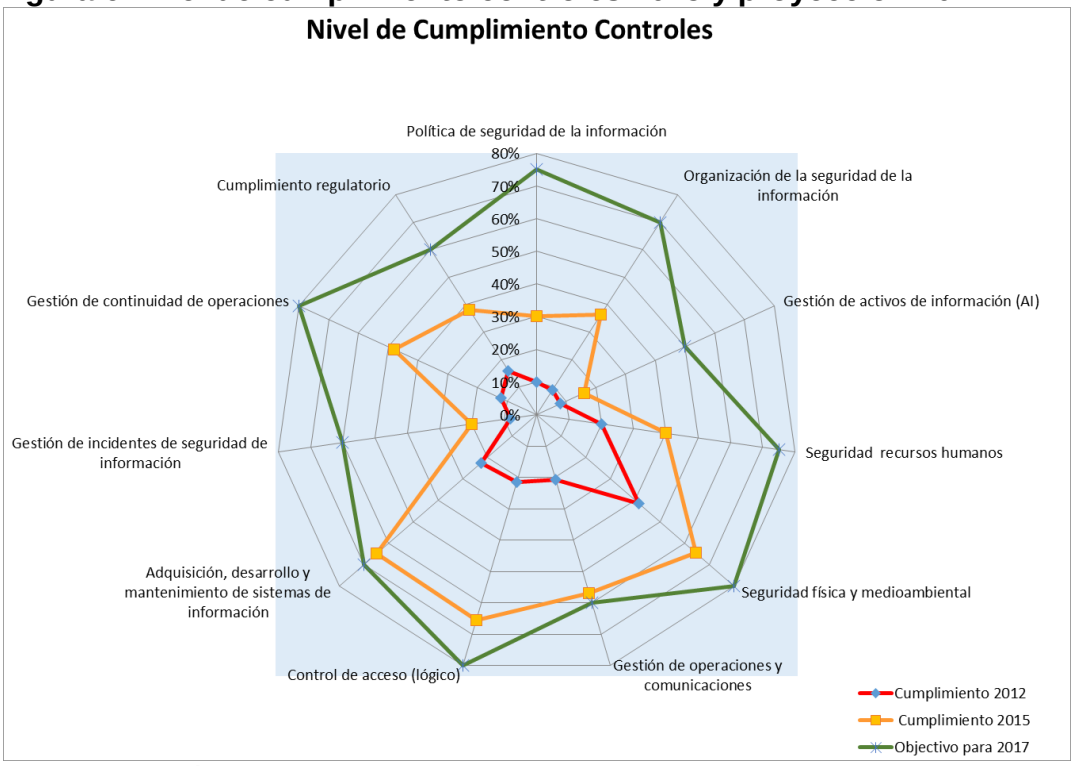


Fuente: Autoría propia.

Los controles observados para la gestión de activos de información se mantienen en un nivel muy bajo, es decir que se deben emprender actividades que permitan implementar y mejorar este dominio.

Los dominios de políticas de seguridad física y medioambiental, gestión de operación y comunicaciones, control de acceso lógico y adquisición, desarrollo y mantenimiento de sistemas de información han logrado un buen nivel de despliegue, faltándole muy poco para lograr el objetivo propuesto.

Figura 6 Nivel de cumplimiento controles 2015 y proyección 2017



Fuente: Autoría propia.

Se espera tener para el 2017 un cubrimiento aceptable en todos y cada uno de los dominios, eso sí enfatizando los dominios de gestión de activos de información y gestión de incidentes de seguridad.

5. PROPUESTA PARA IMPLANTAR UN SGSI PARA LAS BASES DE DATOS ORACLE.

5.1 Definición del alcance y límites del SGSI

El Sistema de Gestión de Seguridad de la Información para la Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones en la Dirección de Impuestos y Aduanas Nacionales, comprende las siguientes coordinaciones:

- Coordinación para el Apoyo a los Sistemas de Información
- Coordinación de Infraestructura Tecnológica
- Coordinación de Soporte Técnico al Usuario
- Coordinación de Proyectos

Hay que resaltar el hecho que la Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones depende de la Dirección de Gestión Organizacional y aunque sea un área de apoyo dentro de la organización es un área neurálgica para todas las áreas misionales de la entidad.

La subdirección incluye los servicios, procesos y activos correspondientes a las coordinaciones que forman parte de la subdirección y que son necesarios para garantizar la disponibilidad de los servicios informáticos electrónicos que la Dirección de Impuestos y Aduanas Nacionales presta, tanto a nivel interno como externo; sin desmejora de cualquier otro componente de la seguridad como lo son la confidencialidad y la integridad de la información y de los valores corporativos de Dirección de Impuestos y Aduanas Nacionales: Respeto, Honestidad, Responsabilidad y Compromiso.

5.2 Definición de la Política del SGSI

Los servicios que la Dirección de Impuestos y Aduanas Nacionales presta a través de la Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones, tanto a sus clientes internos y externos son diversos, estos servicios se surten a través de sus diferentes coordinaciones, entre ellos están los servicios informáticos electrónicos y las aplicaciones, la granja de servidores, el almacenamiento, las bases de datos, las redes de comunicaciones y los equipos de escritorio en donde convergen clientes de correo y los cuales pertenecen a un directorio activo que maneja políticas tanto a nivel de equipos y usuario. De igual manera un gran número de proyectos que se manejan en la coordinación de proyectos. Así mismo el componente humano que es responsable de mantener la prestación de dichos servicios con una disponibilidad de 7 días por 24 horas, sin deterioro de la integridad y de la confidencialidad necesaria para que los servicios se mantengan funcionando. Así mismo, como objetivo de acción se velará porque los usuarios de DIAN reciban un servicio seguro, accesible y de calidad.

5.3 Estructura del sistema documental

5.3.1 Política y Objetivos de SGSI

Alcance del SGSI

El Sistema de Gestión de Seguridad de la Información cubrirá la Gestión de la seguridad de la información contenida en la bases de datos ORACLE de la entidad, la cual es gestionada por los aplicativos de la plataforma MUISCA.

Con el fin de que los servicios informáticos de facilitación a los contribuyentes se presten eficazmente, la Dirección de impuestos y Aduanas Nacionales está comprometida con el desarrollo de un Sistema de Gestión de la Seguridad de la Información (SGSI), el cual bajo lo establecido en la Norma internacional NTC/ISO-IEC 27001, establece un conjunto de medidas técnicas y organizativas para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

Este sistema de gestión cubre toda la información, sistemas de información, activos y personas para los procesos en los siguientes servicios:

Servicios de la Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones, que comprende la Coordinación para el apoyo a los sistemas de Información, la Coordinación de infraestructura tecnológica, la Coordinación de soporte técnico al Usuario y la Coordinación de proyectos

Los servicios que presta la Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones están ubicados en la siguiente dirección: Carrera 8 No. 6c-34 piso 5, sede del nivel central de la Dirección de impuestos y Aduanas Nacionales; esta ubicación queda incluida en el alcance del SGSI.

La Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones, en conjunto con todos sus funcionarios, ha decidido impulsar y difundir a todos los niveles de la subdirección la siguiente Política:

“Cada Responsable de la información en la Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su correspondiente coordinación, manteniendo una adecuada protección de los activos, impidiendo accesos no autorizados a la información”.

De igual manera se fija un compromiso ético en el proceso que lleva a cabo la subdirección el cual reza los siguiente: “Doy mi palabra que asumo que las dificultades de tipo tecnológico se pueden resolver si tengo la actitud, el compromiso y el deseo de resolverlas”

Esta Política se fundamenta en los siguientes principios:

- Proteger los recursos de información y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, para asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

- Incorporar medidas de seguridad en los sistemas de información desde su desarrollo e implementación y durante su mantenimiento, con el fin de reducir los riesgos de error humano y sucesos de origen natural.

- Garantizar la seguridad continua de la información:

  - ✓ Mantener la Política de Seguridad de la Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones actualizada, con el fin de asegurar su vigencia y nivel de eficacia.
  - ✓ Sensibilizar al personal de la Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones con relación a su responsabilidad frente a la utilización de contraseñas.
  - ✓ Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
  - ✓ El Comité de Seguridad de la Información revisará anualmente la Política, con el fin de mantenerla actualizada. Igualmente efectuará las modificaciones que sean necesarias en razón a posibles cambios que puedan afectar su definición, como cambios tecnológicos, impacto de los incidentes de seguridad, etc.

Procedimientos de la organización ajustados

- Procedimiento Regulación de acceso a las bases de datos Oracle – Sistema Muisca.
- Procedimiento Contraseñas para ingreso a las bases de datos Oracle – Sistema Muisca
- Procedimiento Copias de seguridad bases de datos Oracle – Sistema Muisca.
- Restauración y recuperación bases de datos Oracle – Sistema Muisca

5.3.2 Desarrollo de los objetivos

De acuerdo a como lo establece la norma ISO/IEC 27001 y al modelo PDCA, se siguen los pasos descritos en la Figura 1. Para el proceso de implementación del SGSI, así:

1. Definición del alcance

2. Análisis y gestión del riesgo

3. Generación y gestión de los diferentes proyectos de seguridad para implantar las medidas ISO 27002

4. Implantar las medidas y controles

5. Creación del marco de gestión ISO 27001
    5.1. Gestión de la documentación
    5.2. Gestión de la formación y concienciación
    5.3. Gestión de la auditoria interna
    5.4. Gestión de la revisión del sistema
    5.5. Gestión de la mejora continua: acciones preventivas y correctivas

6. Elaboración de la documentación formal necesaria para construir el SGSI
    6.1. Normas de seguridad
    6.2. Procedimientos de seguridad

7. Acciones formativas y de concienciación

5.3.3 Registros necesarios para el progreso del proceso

Se deben mantener registros que evidencie la aprobación entre los requisitos y actividades del SGSI. Registros protegidos y controlados y legibles, fácilmente identificables y recuperables. Se deben tener en cuenta también los registros que sean necesarios por requerimiento legal o establecido por la empresa.

Declaración de aplicabilidad

De acuerdo al análisis de riesgo, se deben destacar los controles a implementar y a excluir, con su correspondiente argumento, se mencionan los controles ya implementados; también es recomendable mencionar cómo se realizará la implementación, este documento debe ser aprobado por la Subdirección de Tecnología.

Tabla 16 Controles Norma ISO 27001.

Controles de la Norma ISO 27001		Controles Actuales	Justificación para la exclusión	Controles seleccionados y razón para su selección				Observaciones
Clausula	Numeral, Controles y Objetivos de control			RL	OC	RM/MP	RAR	
5. POLITICA DE SEGURIDAD	**5.1 Política de seguridad de la información**							
	5.1.1 Documento de política de seguridad de la información							
	5.1.2 Revisión de la política de seguridad de la información							
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	**6.1 Organización interna**							
	6.1.1 Comité de gestión de seguridad de la información							
	6.1.2 Coordinación de la seguridad de la información							
	6.1.3 Asignación de responsabilidades relativas a la seguridad de la información							
	6.1.4 Proceso de autorización de recursos para el tratamiento de la información							

Controles de la Norma ISO 27001		Controles Actuales	Justificación para la exclusión	Controles seleccionados y razón para su selección				Observaciones
Clausula	Numeral, Controles y Objetivos de control			RL	OC	RM/MP	RAR	
	6.1.5 Acuerdos de confidencialidad							
	6.1.6 Contacto con las autoridades							
	6.1.7 Contacto con grupos de interés especial							
	6.1.8 Revisión independiente de la seguridad de la información							
	6.2 Terceros							
	6.2.1 Identificación de los riesgos derivados del acceso de terceros							
	6.2.2 Tratamiento de la seguridad en la relación con los clientes							
	6.2.3 Tratamiento de la seguridad en contratos con terceros							
7. GESTIÓN DE ACTIVOS	**7.1 Responsabilidad sobre los activos**							
	7.1.1 Inventario de activos							
	7.1.2 Propiedad de los activos							
	7.1.3 Uso aceptable de los activos							
	7.2 Clasificación de la información							
	7.2.1 Directrices de clasificación							
	7.2.2 Etiquetado y manipulado de la información							
8. SEGURIDAD LIGADA A	**8.1 Antes del empleo**							
	8.1.1 Funciones y responsabilidades							
	8.1.2 Investigación de antecedentes							

Controles de la Norma ISO 27001		Controles Actuales	Justificación para la exclusión	Controles seleccionados y razón para su selección				Observaciones
Clausula	Numeral, Controles y Objetivos de control			RL	OC	RM/MP	RAR	
LOS RECURSOS HUMANOS	8.1.3 Términos y condiciones de contratación							
	8.2 Durante el empleo							
	8.2.1 Responsabilidades de la Dirección							
	8.2.2 Concienciación, formación y capacitación en seguridad de la información							
	8.2.3 Proceso disciplinario							
	8.3 Cese del empleo o cambio de puesto de trabajo							
	8.3.1 Responsabilidad del cese o cambio							
	8.3.2 Devolución de activos							
	8.3.3 Retirada de los derechos de acceso							
9. SEGURIDAD FÍSICA Y AMBIENTAL	**9.1 Áreas seguras**							
	9.1.1 Perímetro de seguridad física							
	9.1.2 Controles físicos de entrada							
	9.1.3 Seguridad de oficinas, despachos e instalaciones							
	9.1.4 Protección contra las amenazas externas y de origen ambiental							
	9.1.5 Trabajo en áreas seguras							
	9.1.6 Áreas de acceso público y de carga y descarga							
	9.2 Seguridad de los equipos							
	9.2.1 Emplazamiento y protección de equipos							

Controles de la Norma ISO 27001		Controles Actuales	Justificación para la exclusión	Controles seleccionados y razón para su selección				Observaciones
Clausula	Numeral, Controles y Objetivos de control			RL	OC	RM/MP	RAR	
	9.2.2 Instalaciones de suministro							
	9.2.3 Seguridad del cableado							
	9.2.4 Mantenimiento de los equipos							
	9.2.5 Seguridad de los equipos fuera de las instalaciones							
	9.2.6 Reutilización o retirada segura de equipos							
	9.2.7 Retirada de materiales propiedad de la empresa							
10. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES	**10.1** Responsabilidades y procedimientos de operación							
	10.1.1 Documentación de los procedimientos de operación							
	10.1.2 Gestión de cambios							
	10.1.3 Segregación de tareas							
	10.1.4 Separación de los recursos de desarrollo, prueba y operación							
	10.2 Gestión de la provisión de servicios por terceros							
	10.2.1 Provisión de servicios							
	10.2.2 Supervisión y revisión de los servicios prestados por terceros							
	10.2.3 Gestión de cambios en los servicios prestados por terceros							
	10.3 Planificación y aceptación del sistema							

Controles de la Norma ISO 27001		Controles Actuales	Justificación para la exclusión	Controles seleccionados y razón para su selección				Observaciones
Clausula	Numeral, Controles y Objetivos de control			RL	OC	RM/MP	RAR	
	10.3.1 Gestión de capacidades							
	10.3.2 Aceptación del sistema							
	10.4 Protección contra código malicioso y descargable							
	10.4.1 Controles contra el código malicioso							
	10.4.2 Controles contra el código descargado en el cliente							
	10.5 Copias de seguridad							
	10.5.1 Copias de seguridad de la información							
	10.6 Gestión de la seguridad de las redes							
	10.6.1 Controles de red							
	10.6.2 Seguridad de los servicios de red							
	10.7 Manipulación de los soportes							
	10.7.1 Gestión de soportes extraíble							
	10.7.2 Retirada de soportes							
	10.7.3 Procedimientos de manipulación de la información							
	10.7.4 Seguridad de la documentación del sistema							
	10.8 Intercambio de información							
	10.8.1 Políticas y procedimientos de intercambio de información							

Controles de la Norma ISO 27001		Controles Actuales	Justificación para la exclusión	Controles seleccionados y razón para su selección				Observaciones
Clausula	Numeral, Controles y Objetivos de control			RL	OC	RM/MP	RAR	
	10.8.2 Acuerdos de intercambio							
	10.8.3 Soportes físicos en tránsito							
	10.8.4 Mensajería electrónica							
	10.8.5 Sistemas de información corporativo/de negocio							
	10.9 Servicios de comercio electrónico							
	10.9.1 Comercio electrónico							
	10.9.2 Transacciones en línea							
	10.9.3 Información puesta a disposición pública							
	10.10 Supervisión							
	10.10.1 Registro de auditorias							
	10.10.2 Supervisión del uso del sistema							
	10.10.3 Protección de la información de los registros							
	10.10.4 Registros de administración y operación							
	10.10.5 Registro de fallos							
	10.10.6 Sincronización del reloj							
11. CONTROL DE ACCESO	**11.1** Requisito del negocio para el control de acceso							
	11.1.1 Política de control de acceso							
	11.2 Gestión de acceso de usuario							

Controles de la Norma ISO 27001		Controles Actuales	Justificación para la exclusión	Controles seleccionados y razón para su selección				Observaciones
Clausula	Numeral, Controles y Objetivos de control			RL	OC	RM/MP	RAR	
	11.2.1 Registro de usuario							
	11.2.2 Gestión de privilegios							
	11.2.3 Gestión de contraseñas de usuarios							
	11.2.4 Revisión de los derechos de acceso de usuario							
	11.3 Responsabilidades de usuario							
	11.3.1 Uso de contraseña							
	11.3.2 Equipo de usuario desatendido							
	11.3.3 Política de puesto de trabajo despejado y pantalla limpia							
	11.4 Control de acceso a la red							
	11.4.1 Política de uso de los servicios en red							
	11.4.2 Autenticación de usuario para conexiones externas							
	11.4.3 Identificación de los equipos en las redes							
	11.4.4 Diagnóstico remoto y protección de los puertos de configuración							
	11.4.5 Segregación de las redes							
	11.4.6 Control de conexión a la red							
	11.4.7 Control de encaminamiento (router) de red							
	11.5 Control de acceso al sistema operativo							

Controles de la Norma ISO 27001		Controles Actuales	Justificación para la exclusión	Controles seleccionados y razón para su selección				Observaciones
Clausula	Numeral, Controles y Objetivos de control			RL	OC	RM/MP	RAR	
	11.5.1 Procedimientos seguros de inicio de sesión							
	11.5.2 Identificación y autenticación de usuario							
	11.5.3 Sistema de gestión de contraseñas							
	11.5.4 Uso de los recursos del sistema							
	11.5.5 Desconexión automática de sesión							
	11.5.6 Limitación del tiempo de conexión							
	11.6 Control de acceso a las aplicaciones y a la información							
	11.6.1 Restricción del acceso a la información							
	11.6.2 Aislamiento de sistemas sensibles							
	11.7 Ordenadores portátiles y teletrabajo							
	11.7.1 Ordenadores portátiles y comunicaciones móviles							
	11.7.2 Teletrabajo							
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE	**12.1 Requisitos de seguridad de los sistemas de información**							
	12.1.1 Análisis y especificaciones de los requisitos de seguridad							
	12.2 Tratamiento correcto de las aplicaciones							
	12.2.1 Validación de los datos de entrada							
	12.2.2 Control del tratamiento interno							

Controles de la Norma ISO 27001		Controles Actuales	Justificación para la exclusión	Controles seleccionados y razón para su selección				Observaciones
Clausula	Numeral, Controles y Objetivos de control			RL	OC	RM/MP	RAR	
INFORMACIÓN	12.2.3 Integridad de los mensajes							
	12.2.4 Validación de los datos de salida							
	12.3 Controles criptográficos							
	12.3.1 Política de uso de los controles criptográficos							
	12.3.2 Gestión de claves							
	12.4 Seguridad de los archivos del sistema							
	12.4.1 Control del software en explotación							
	12.4.2 Protección de los datos de prueba del sistema							
	12.4.3 Control de acceso al código fuente de los programas							
	12.5 Seguridad en los procesos de desarrollo y soporte							
	12.5.1 Procedimientos de control de cambios							
	12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo							
	12.5.3 Restricciones a los cambios en los paquetes de software							
	12.5.4 Fugas de información							
	12.5.5 Externalización del desarrollo de software							
	12.6 Gestión de la vulnerabilidad técnica							
	12.6.1 Control de las vulnerabilidades técnicas							

Controles de la Norma ISO 27001		Controles Actuales	Justificación para la exclusión	Controles seleccionados y razón para su selección				Observaciones
Clausula	Numeral, Controles y Objetivos de control			RL	OC	RM/MP	RAR	
13. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	**13.1 Notificación de eventos y puntos débiles de la seguridad de la información**							
	13.1.1 Notificación de los eventos de seguridad de la información							
	13.1.2 Notificación de puntos débiles de la seguridad							
	13.2 Gestión de incidentes de seguridad de la información y mejoras							
	13.2.1 Responsabilidades y procedimientos							
	13.2.2 Aprendizaje de los incidentes de seguridad de la información							
	13.2.3 Recopilación de evidencias							
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**14.1 Aspectos de seguridad en la gestión de la continuidad del negocio**							
	14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio							
	14.1.2 Continuidad del negocio y evaluación de riesgos							
	14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información							
	14.1.4 Marco de referencia para la							

Controles de la Norma ISO 27001		Controles Actuales	Justificación para la exclusión	Controles seleccionados y razón para su selección				Observaciones
Clausula	Numeral, Controles y Objetivos de control			RL	OC	RM/MP	RAR	
	planificación de la continuidad del negocio							
	14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio							
15. CUMPLIMIENTO	**15.1 Cumplimiento de los requisitos legales**							
	15.1.1 Identificación de la legislación aplicable							
	15.1.2 Derechos de propiedad intelectual (IPR)							
	15.1.3 Protección de los documentos/de la organización							
	15.1.4 Protección de datos y privacidad de la información personal							
	15.1.5 Prevención y uso indebido de los recursos de tratamiento de la información							
	15.1.6 Regulación de los controles criptográficos							
	15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico							
	15.2.1 Cumplimiento de las políticas y normas de seguridad							
	15.2.2 Comprobación del cumplimiento técnico							
	15.3 Consideraciones sobre las auditorias de los sistemas de información							
	15.3.1 Controles de auditoria de los sistemas de información							

Controles de la Norma ISO 27001		Controles Actuales	Justificación para la exclusión	Controles seleccionados y razón para su selección				Observaciones
Clausula	Numeral, Controles y Objetivos de control			RL	OC	RM/MP	RAR	
	15.3.2 Protección de las herramientas de auditoria de los sistemas de información							

RL: Requerimientos legales. **RN/MP**: Requerimientos del negocio/mejores prácticas.

OC: Obligaciones contractuales. **RAR**: Resultados del Análisis de riesgos.

5.4 RECURSOS DISPONIBLES

Desde el año de 2011 la Subdirección de Gestión de Tecnología de la Información y Telecomunicaciones, viene renovando la infraestructura tecnológica y adquiriendo aplicaciones especializadas que soportan un gran número de servicios que se prestan en la Dirección de Impuestos y Aduanas Nacionales, ha ampliado la planta de personal con personas administrativamente calificadas, esto con el propósito de administrar y reforzar las políticas de seguridad que se vienen manejando en la actualidad, e iniciar la implementación de Sistema de Gestión de Seguridad de la Información SGSI acorde con el crecimiento y necesidades de la misma.

Dentro de los elementos de infraestructura ya adquiridos podemos destacar la adquisición de:

- Dos servidores AIX de última tecnología con los recursos que nos permitirán consolidar cerca de 20 servidores Unix grandes.
- Un sistema de almacenamiento multiplataforma para los servidores Unix y Windows
- Un sistema de seguridad
- Un Sistema de red central

Aplicaciones Especializadas:

- Sistema de identificación
- Software para el respaldo de aplicaciones y máquinas con uso de librería
- Sistema de mensajería
- Un sistema herramientas de seguridad para manejo de conexiones y fuga de información

Contratos:

- Casa de software
- Centro de respuesta a Incidentes nacionales

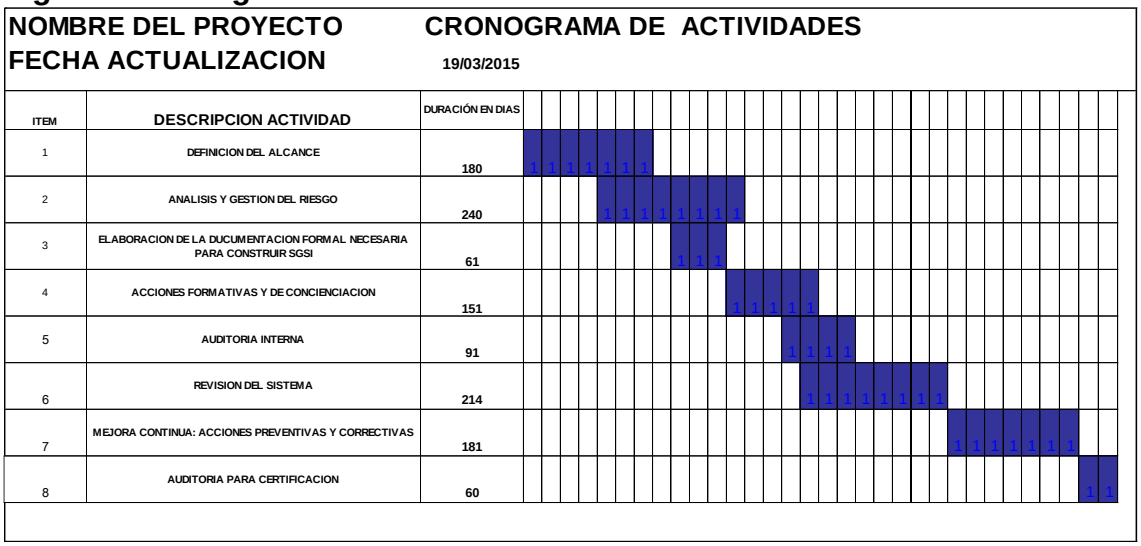
Personal:

- Apoyo manifiesto del director de la DIAN
- Asesores Calificados
- Ingenieros para el manejo de nuevas herramientas y hardware

5.5 CRONOGRAMA

Desde finales del año 2011 se vienen desarrollando en la Subdirección de tecnología los planes concernientes a implementar los más altos estándares de seguridad en la DIAN, el propósito es que el año 2016 la entidad pueda dar cumplimiento de leyes ISO cifrado DBA.

Figura 7 Cronograma de actividades.



Fuente: Autoría propia.

5.6 RECOMENDACIONES

- Se debe buscar el apoyo de la alta gerencia para la realización un plan de implementación de un Sistema de Gestión de Seguridad de la Información – SGSI que contemple todos los activos de la subdirección.

- El área de las Tics debe gestionar los controles de seguridad para entrar en concordancia con la ISO 27002.

- Debe redactarse, aprobarse y difundirse una política de seguridad de la información que refleje la misión y visión de la Entidad.

- Se debe definir y documentar e informar los roles de los responsables de administrar los recursos informáticos de acuerdo a las políticas de seguridad.

- Se debe identificar ciclos productivos o de vida para todos los activos de la entidad, documentar y clasificar su información hasta que sean dados de baja.

- Se deben implementar controles biométricos que aseguren la identificación de todos los usuarios internos que utilizan los sistemas de información.

- Los ambientes de desarrollo, pruebas técnicas, pruebas funcionales y producción deben estar bien definidos, de tal manera que los riesgos identificables sean totalmente independientes.

- Los procedimientos de operación deben estar a disposición de todos los usuarios que los requieran.

- Se debe actualizar la versión Oracle a 11.2.0.4 que permita cumplir con el requerimiento de enmascaramiento en tiempo de ejecución de los datos en los sistemas de información en acuerdo con la normatividad vigente que exige confidencialidad.

6. CONCLUSIONES

- El proceso de análisis e identificación de riesgos informáticos es necesario llevarlo a cabo sobre todos los recursos asociados a un área.

- La probabilidad y el impacto son determinantes para que la clasificación de los riesgos sea lo más acertada y permita catalogar cada uno de los activos.

- Se deben llevar los procesos existentes a un buen grado de maduración y así poder llegar a tener unos procedimientos que sean gestionables que cumplan con los controles establecidos en la noma 27001.

- Se pueden tener varias formas para llegar a valor los diferentes riesgos existentes, sin embargo el proceso más adecuado es tener un método de análisis de riesgos, el cual se debe ir adaptando a los sistemas de información.

- La seguridad de la información mantiene una mayor objetividad si se realiza a través de contratos con entidades externas.

7. BIBLIOGRAFÍA

Alberto G. Alexander, 2005 Diseño de un sistema de gestión de seguridad de información. Óptica ISO 27001:

Sabogal, M. (2013), Módulo Proyecto de Seguridad Informática II, Recuperado de http://www.unadvirtual.edu.co.

Martin Iglesias L., 2009, Diseño de un SGSI.
Muestra cómo se debe realizar un SGSI de acuerdo a la norma 27001

Definición un sistema de gestión de seguridad informática, recuperado de http://www.iso27000.es/sgsi.html
Define que es un SGSI, para que sirve, como se implementa y la ISO 27000

Rodríguez J. R., 2007 Gestión de proyectos informáticos, describe las recomendaciones para una buena gestión de proyectos

Conceptos Básicos SGSI, ISO 27000, recuperado de http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos
Describe como conocer riesgos, establecer controles, políticas y procedimientos como parte del SGSI

Martínez J. G., 2004 Planes de Contingencia, descripción de la continuidad del negocio en las organizaciones

Presentación DIAN, recuperado de http://www.dian.gov.co/Content/sobredian/presenta.htm
Presenta el organigrama, visión y misión de la Dirección de Impuestos y Aduanas Nacionales

Burgos Salazar J., 2008, Modelo para la seguridad de la información en las TIC, muestra un modelo para lograr un adecuado nivel de riegos en las TIC

Infosec 101: Seguridad Informática vs Seguridad de la Información, recuperado de https://delfinabzueta.wordpress.com/2014/12/05/infosec-101-seguridad-informatica-vs-seguridad-de-la-informacion/
Diferencia conceptos de seguridad informática y seguridad de la información, además define los dominios en la norma ISO 27001

8. ANEXOS

Anexo 1 Procedimiento regulación de ingreso a las bases de datos Oracle

	PROCEDIMIENTO REGULACIÓN DE INGRESO A LAS BASES DE DATOS ORACLE – SISTEMA MUISCA			
DIAN	**Código** RA-BD-SM-1	**Fecha Revisión** Julio 2013	**Versión** 1.0	**Pagina** 1 de 4

ÍNDICE

1. Objetivo..... 2
2. Alcance..... 2
3. Cumplimiento con los requisitos legales y estándares de seguridad…..... 2
4. Descripción..... 2
4.1 Identificación y autenticación para usuarios del Sistema Informático…..... 2
4.2 Contraseñas..... 3
4.3 Puesto de trabajo..... 3
4.4 Control de acceso a las bases de datos corporativos..... 3
5. Control..... 3
6. Penalizaciones..... 3
7. Divulgación..... 3
8. Revisión..... 3

ANEXO 1 - ACUERDO DE CONFIDENCIALIDAD, NO DIVULGACION Y BUEN USO..... 4

Versión	**Redactado / revisado por**	**Aprobado por**	**Fecha aprobación**	**Fecha publicación**
00001	Comité de seguridad de la Información	Subdirector Informática	Noviembre 2013	Diciembre 2013

Referencia en ISO 27001: A.11.1., A.11.2., A.11.3., A.11.5., A.11.6.

RESPONSABLE DEL DOCUMENTO:

1. Objetivo

Redactar el procedimiento para regular el acceso a las bases de datos Oracle - Sistema Muisca de la Dirección de Impuestos y Aduanas nacionales DIAN.

Para garantizar la protección de las bases de datos, es necesario definir un procedimiento que establezca las medidas de seguridad, organizativas y técnicas que protejan la información en las bases de datos de la empresa.

2. Alcance

Usuarios internos que consultan las bases de datos Oracle 11G; alfa, beta, gamma, delta y zeta
Regirá desde el primero de marzo del 2014 y permanecerá vigente hasta la próxima versión aprobada de la misma.

3. Cumplimiento con los requisitos legales y estándares de seguridad

El presente procedimiento proporciona cobertura a aspectos recogidos en los siguientes controles de la ISO 27001, Anexo A:
A.11.1 Requisitos de negocio para el control de acceso
A.11.2 Gestión de acceso de usuario
A.11.3 Responsabilidades de usuario
A.11.6 Control de acceso a las aplicaciones y a la información

4. Descripción

4.1 Identificación y autenticación para usuarios Internos Sistema Muisca

Para acceder a las bases de datos Oracle 11G, es necesario contar con un usuario, el cual está identificado en el dominio del sistema y además debe estar incluido en el directorio LDAP de la empresa. El usuario será autenticado por una contraseña, a partir de esta autenticación, se le asignarán roles que determinan las actividades que podrá desarrollar dentro del Sistema

Para que el usuario sea asignado, previamente se debe firmar el “Acuerdo de Confidencialidad y Buen Uso de los Sistemas Informáticos”, Anexo 1 de este procedimiento, el documento define el buen uso, disponibilidad y nivel de servicio, así como la responsabilidad y confidencialidad exigida para el mismo.

Las bases de datos Oracle 11G dispone de mecanismos para identificar a los usuarios que acceden al mismo, así como para controlar si están autorizados a

acceder a los recursos y el modo (lectura, modificación, inserción y borrado) en que pueden realizar el acceso.

4.2 Contraseñas
Para la gestión y manejo de contraseñas, se debe cumplir lo establecido en la Norma de Contraseñas.

4.3 Puesto de trabajo
Cuando se finaliza la realización de las tareas, se debe salir del Sistema Informático desconectándose, de tal manera que nadie pueda trabajar con el usuario/contraseña de otra persona. Se debe mantener el protector de pantalla con contraseña y con lapso de activación no superior a cinco (5) minutos. Ante la ausencia temporal, se debe activar el protector de pantalla y no dejar expuestos dispositivos de almacenamiento externos. La sesión de usuario se cancelara automáticamente por inactividad después de 15 minutos. No se debe anotar la contraseña en ningún papel que quede en el puesto de trabajo del usuario.

4.4 Control de acceso a las bases de datos corporativas
El Responsable de Seguridad dará acceso para consulta, inserción, borrado y modificación a las bases de datos Oracle- sistema Muisca de acuerdo a las autorizaciones definidas por los roles asignados a cada usuario. Se llevará registro de auditoria de todas las transacciones realizadas en las bases de datos. La información de las base de datos hace parte del “Acuerdo de Confidencialidad y buen uso de los Sistemas Informáticos”, suscrito por los usuarios.

5. Control
La Empresa realizará auditorías internas periódicas para garantizar el cumplimiento de los controles establecidos en este procedimiento.

6. Penalizaciones
Cuando el Administrador de las bases de datos Oracle 11G detecte incumplimiento en este procedimiento, puede tomar cualquiera de las siguientes medidas:

- Notificar la incidencia al Responsable de Seguridad.
- Suspender o restringir el acceso o uso de los servicios mientras dure la investigación, de ser necesario.
- Con el permiso del Responsable de Seguridad y la correspondiente justificación, examinar ficheros o dispositivos de almacenamiento del usuario implicado.

7. Divulgación
Publicado el 30 de noviembre de 2013.

8. Revisión
Este documento se revisará anualmente.

ANEXO 1 - PACTO DE CONFIDENCIALIDAD, NO DIVULGACION Y BUEN USO DE LAS BASES DE DATOS ORACLE – SISTEMA MUISCA

En carácter de Representante Legal de la ***Dirección de Impuestos y Aduanas Nacionales*** y bajo el contrato Número ***00001*** me comprometo a:

- Acceder a la información de las Bases de datos a través de los aplicativos instalados y autorizados por la empresa aceptando el "Convenio de Confidencialidad y de No Divulgación" en los términos que amparan los derechos propietarios.

- No copiar, traducir, desencriptar, información contenida en las bases de datos, o usar la información con propósitos de divulgación y/o venta sin autorización.

Con respecto al personal de mi empresa me comprometo a:

- Capacitar a los mismos en el conocimiento y uso de las bases de datos Oracle 11G y de la información contenida en estas.

- Hacer firmar y respetar al personal de mi dependencia el "Acuerdo de Confidencialidad y Buen uso de la información contenida en las bases de datos".

Ante el incumplimiento de todo lo mencionado en este convenio, el funcionario será objeto de la aplicación de las sanciones consideradas en el contrato respectivo.

_____ _____

Representante Legal Fecha

NOTA: Sólo las personas debidamente designadas podrán ejecutar aquellas operaciones o consultas sobre las bases de datos muiscas.

Anexo 2 Procedimiento contraseñas para ingreso a las bases de datos Oracle

	PROCEDIMIENTO *CONTRASEÑAS PARA INGRESO A LAS BASES DE DATOS ORACLE – SISTEMA MUISCA*			
	Código C-BD-M-1	**Fecha Revisión** Julio 2013	**Versión** 1	**Pagina** 1 de 2

1. Objetivo

Definir las normas a aplicar en la configuración y uso de las contraseñas de las bases de datos del sistema muisca.

Para garantizar la protección y autenticación de acceso a los sistemas, es importante que las contraseñas cumplan unos requisitos mínimos que garanticen la robustez del sistema.

2. Alcance

A todos los usuarios que ingresan a las bases de datos Oracle 11G sistema muisca, ya sea por los aplicativos, Sqldeveloper, Toad y menú de consultas.

Regirá desde el día primero de diciembre del 2013 y permanecerá vigente hasta la próxima versión aprobada de la misma.

3. Cumplimiento con los requisitos legales y estándares de seguridad

La presente norma proporciona cobertura a aspectos recogidos en los siguientes controles de la ISO 27001, Anexo A:

A.11.2.3. Gestión de las contraseñas de usuario
A.11.3.1. Uso de las contraseñas
A.11.5.3. Sistema de gestión de las contraseñas

4. Descripción de la norma

4.1. Las contraseñas en todos los usuarios tienen una longitud mínima de 14 caracteres, la cual debe incluir mínimo 1 dígito, 1 caracteres alfabéticos y un carácter especial; y no debe incluir o ser igual al nombre del usuario.

4.2. El número de intentos sucesivos fallidos en la introducción de contraseña es de cinco (5), después de lo cual será bloqueado el usuario.

4.3. Los usuarios administradores y de consulta se obligan a cambiar la contraseña cada mes, no debe usarse ninguna de las anteriores cinco (5) claves.

4.4. La contraseña se debe cambiar cuando se sospeche que otras personas puedan tener conocimiento de la misma.

4.5. La contraseña es de uso exclusivo del usuario al que pertenece.

4.6. Las contraseñas se fijaran por los usuarios en los puestos de los administradores de las bases de datos.

4.7. Los usuarios deben seleccionar contraseñas seguras, de acuerdo a las siguientes recomendaciones:

a. Se debe evitar repetir la misma contraseña en todas las bases de datos disponibles.
b. No utilizar información personal en la contraseña: nombre del usuario o de familiares, ni los apellidos, ni la fecha de nacimiento. Se recomienda la utilización de letras mayúsculas y minúsculas en la contraseña.
c. Es responsabilidad del usuario mantener en secreto su contraseña. Se debe evitar escribir la contraseña.

5. Controles

5.1. La asignación del identificador único para los usuarios se debe realizar mediante un proceso formal denominado Acuerdo sobre el uso de los sistemas de información, donde queda establecida la responsabilidad y obligaciones en el uso de dicho identificador, especialmente que se comprometen a mantener sus contraseñas personales en secreto y las posibles consecuencias de un mal uso.

5.2. Las claves se controlaran a través de los profile y funciones de las bases de datos Oracle 11G del esquema sys.

5.3. Los usuarios se deben obligar a cambiar las contraseñas iniciales, una vez ingresen al sistema por primera vez. Contraseñas momentáneas se asignan cuando los usuarios olvidan su contraseña, se suministran una vez identificado el usuario.

5.4. Cuando se introduzca la contraseña en los sistemas, nunca debe aparecer de forma visible y legible en la pantalla.

5.5. Las políticas de control de accesos se realizan en base a las necesidades de seguridad de la DIAN, las cuales se revisaran periódicamente.

5.6. Debe existir un procedimiento formal para dar de alta y baja a los usuarios, con el fin de garantizar y cancelar los accesos a todas las bases de datos existentes en la compañía.

5.7. Se habilita la Auditoria general y granulada en las bases de datos para garantizar que se cumplen los controles. Se debe mantener registro de las excepciones a disposición de las auditorias.

Anexo 3 Procedimiento copias de seguridad bases de datos Oracle

	PROCEDIMIENTO COPIAS DE SEGURIDAD BASES DE DATOS ORACLE – SISTEMA MUISCA			
	Código CS-BD-SM-1	**Fecha Revisión** Julio 2013	**Versión** 1.0	**Pagina** 1 de 5

ÍNDICE

1. Objetivo..... 2
2. Alcance..... 2
3. Responsables..... 2
4. Cumplimiento con los requisitos legales y estándares de seguridad..... 2
5. Descripción..... 2
5.1 Métodos de copias..... 2
5.2 Periocidad…….. 3
5.3 Identificación de copias..... 3
5.4 Almacenamiento de las copias de seguridad..... 3
5.5 Recuperación de las copias de seguridad..... 3
6. Control..... 3
7. Penalizaciones..... 4
8. Divulgación..... 4
9. Revisión..... 4
ANEXO 1 – PLANILLA DE COPIAS DESEGURIDAD..... 5

Versión	**Redactado / revisado por**	**Aprobado por**	**Fecha aprobación**	**Fecha publicación**
00001	Comité de seguridad de la Información	Subdirector Informática	Noviembre 2013	Diciembre 2013

Referencia en ISO 27001: A.10.5.

RESPONSABLE DEL DOCUMENTO:

1. Objetivo

Garantizar la seguridad de la información contenida en las bases de datos Oracle 11G Sistema Muisca de la DIAN. El procedimiento establecido para la realización de copias de seguridad y para la recuperación de los datos, deberá garantizar su reconstrucción en el estado en el que se encontraban al tiempo de producirse cualquier tipo de pérdida o destrucción.

2. Alcance

Este procedimiento aplica a las bases de datos alfa, beta, gamma, delta y zeta de la DIAN donde reside la información corporativa.
Regirá el día primero de febrero del 2014 y permanecerá vigente hasta la próxima versión aprobada de la misma.

3. Responsables

Este procedimiento aplica a los administradores de las bases de datos y sistemas operativos AIX, de los servidores correspondientes, a los operadores del Centro de Cómputo y cintoteca que se encarga de la custodia de la información.

4. Cumplimiento con los requisitos legales y estándares de seguridad

El presente procedimiento proporciona cobertura a aspectos recogidos en los siguientes controles de la ISO 27001, Anexo A: A.10.5. Copias de seguridad

5. Descripción

5.1 Métodos de copias

Los respaldos se realizarán a través de la herramienta tivoli storage manager (TSM) y Oracle rman en la librería IBM T3500, los cuales se programan de manera automática verificados centro de cómputo.

Se definen los siguientes métodos de copias de seguridad a utilizar:

- Copia de seguridad completo: toma copia a todos los archivos en línea de cada una de las bases de datos e inserta un registro en el sistema operativo que indica que se ha hecho una copia completa de seguridad de la base de datos.

- Copia de seguridad de archive log: toma copia a todos los archivelog generados en cada una de las bases de datos e inserta un registro en el sistema operativo que indica que se ha hecho una copia de archive log de seguridad de la base de datos.

5.2 Periocidad

Todos los días se tomarán tres copias de los archive log de las cinco bases de datos en los horarios de las 11:00 PM, 7:00 AM y 1:00 PM que se identificarán como diarios y los cuales tendrán una vigencia de 15 días.

Todos los sábados tomará una copia completa que se identificará como semanal y tendrá una vigencia de 60 días

Todos los primero de cada mes se tomará una copia completa que se identificará como mensual y tendrá una vigencia de 400 días.

Todos los primero de enero se tomará una copia completa que se identificará como anual y tendrá una vigencia de 2000 días.

5.3 Identificación Copias

Todos los días, el personal de centro de cómputo llenará la Planilla de copias de seguridad de cada una de las bases de datos con los registros guardados en el sistema operativo (ver Anexo 1).

5.4 Almacenamiento de las copias de seguridad

Las cintas para los respaldos diarios se mantiene en la librería hasta que se llenen, las cintas para los respaldos semanales, mensuales y anuales se retiran de la librería una vez terminen los respaldos y deberán ser guardados en un lugar externo a la empresa, para lo cual se establecerá un contrato con una empresa de seguridad que ofrezca el servicio de almacenaje y conservación de copias de seguridad. Se mantendrá una copia activa en sitio alterno con la herramienta Active Data Guard de Oracle.

5.5 Recuperación de las copias de seguridad

Cada meses se debe realizar una simulación de restauración de las copias de seguridad, y dejar registrado el resultado de la simulación, e informando al Administrador del sistema si se obtuvo errores, PROCEDIMIENTO RESTAURACION COPIAS DE RESPALDO.

6. Control

La Empresa realizará auditorías internas periódicas para garantizar el cumplimiento de los controles establecidos en este procedimiento.

7. Penalizaciones
Cuando el Administrador del Sistema Informático detecte incumplimiento en este procedimiento, puede tomar cualquiera de las siguientes medidas:

- Notificar la incidencia al Responsable de Seguridad.

8. Divulgación
Publicado el 30 de noviembre de 2013.

9. Revisión
Anualmente se realizara una revisión.

ANEXO 1 – PLANILLA DE COPIAS DE RESPALDO BD SIGMA

TIPO COPIA	FECHA	HORA INICIO	HORA FINAL	FECHA VENCIMIENTO	OPERADOR	OBSERVACIONES

Anexo 4 Procedimiento restauración y recuperación bases de datos Oracle

	PROCEDIMIENTO RESTAURACION Y RECUPERACION BASES DE DATOS ORACLE – SISTEMA MUISCA			
	Código CS-BD-SM-1	**Fecha Revisión** Marzo 2014	**Versión** 1.0	**Pagina** 1 de 4

ÍNDICE

1. Objetivo..... 2
2. Alcance..... 2
3. Responsables..... 2
4. Cumplimiento con los requisitos legales y estándares de seguridad..... 2
5. Descripción..... 2
5.1 Método de restauracion..... 2
5.2 Periocidad……..... 2
5.3 Identificación de restauraciones..... 2
6. Control..... 3
7. Penalizaciones..... 3
8. Divulgación..... 3
9. Revisión..... 3
ANEXO 1 – PLANILLA DE RESTAURACION Y RECUPRACION..... 4

Versión	**Redactado / revisado por**	**Aprobado por**	**Fecha aprobación**	**Fecha publicación**
00001	Comité de seguridad de la Información	Subdirector Informática	Julio 2014	Diciembre 2014

Referencia en ISO 27001: A.10.5.

RESPONSABLE DEL DOCUMENTO:

1. Objetivo

Garantizar la recuperación de la información contenida en las cintas que sirven de respaldo a las bases de datos Oracle 11G Sistema Muisca de la DIAN. El procedimiento debe garantizar la consistencia de los datos en el tiempo.

2. Alcance

Este procedimiento aplica a las bases de datos alfa, beta, gamma, delta y zeta de la DIAN donde reside la información corporativa.

Regirá el día primero de Septiembre del 2014 y permanecerá vigente hasta la próxima versión aprobada de la misma.

3. Responsables

Este procedimiento aplica a los administradores de las bases de datos y sistemas operativos AIX, de los servidores correspondientes.

4. Cumplimiento con los requisitos legales y estándares de seguridad

El presente procedimiento proporciona cobertura a aspectos recogidos en los siguientes controles de la ISO 27001, Anexo A: A.10.5. Copias de seguridad

5. Descripción

5.1 Método de restauración

Se realizarán a través de la herramienta tivoli storage manager (TSM) y Oracle rman desde una partición dispuesta para este proceso (i795f1p29) de manera exclusiva.

5.2 Método de recuperación

Se realizaran pruebas de recuperación como perdida de data files, corrupción de bloques, borrado y modificación de objetos de las bases de datos.

Se establecen directorios y scripts que generan más scripts por cada una de las cinco bases de datos a restaurar y que se ejecutan por los administradores de las bases de datos y sistemas operativos

5.2 Periodicidad

El primer miércoles de cada mes se realiza el procedimiento de recuperación para una de las cinco bases de datos del sistema

5.3 Identificación de restauraciones
Los administradores dejarán registrado el resultado de la restauración, en el formato de restauración y recuperación de respaldos (ver Anexo 2).

6. Control
La Empresa realizará auditorías internas periódicas para garantizar el cumplimiento de los controles establecidos en este procedimiento.

7. Penalizaciones
Cuando el Administrador del Sistema Informático detecte incumplimiento en este procedimiento, puede tomar cualquiera de las siguientes medidas:

- Notificar la incidencia al Responsable de Seguridad.

8. Divulgación
Publicado el 30 de Agosto de 2014.

9. Revisión
Anualmente se realizará una revisión.

ANEXO 1 – FORMATO DE RESTAURACION Y RECUPERACION

FORMATO RESTAURACION Y RECUPERACION BASES DE DATOS MUISCA

FECHA: _____ FECHA RESPALDO _____

RESPONSABLE: _____ TOTAL DATAFILES: _____

SCN FINAL: _____ TAMAÑO: _____

BASE DE DATOS

ALFA | BETA | GAMMA | DELTA | ZETA

RESTAURACION	BIEN	MAL
SPFILE		
CONTROL FILE		
DATAFILES		

RECUPERACION	BIEN	MAL
INICIAL		
BLOQUE		
DATAFILE		
TABLA		

OBSERVACIONES: