AUDITORÍA AL SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁCION EN EL PROCESO DE DESARROLLO DE SOFTWARE DE ACUERDO A LA NORMA ISO/IEC 27001:2013 EN LA EMPRESA IT STEFANINI COLOMBIA

ING. JAVIER OLIVO GARCIA ARAQUE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

PROGRAMA DE ESPECIALIZACION EN SEGURIDAD INFORMATICA

BOGOTA – COLOMBIA

2017

AUDITORÍA AL SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁCION EN EL PROCESO DE DESARROLLO DE SOFTWARE DE ACUERDO A LA NORMA ISO/IEC 27001:2013 EN LA EMPRESA IT STEFANINI COLOMBIA

ING. JAVIER OLIVO GARCIA ARAQUE

Trabajo de grado para optar por el título de especialista en seguridad Informática

Director

Esp. SALOMON GONZALEZ GARCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

PROGRAMA DE ESPECIALIZACION EN SEGURIDAD INFORMATICA

BOGOTA – COLOMBIA

2017

Nota de Aceptación:

Aprobado por el comité de grado en cumplimiento de los requisitos exigidos por la Universidad Nacional Abierta y a Distancia UNAD Colombia Para optar por el título de Especialista en Seguridad Informática.

Ing. Yina Alexandra Gonzalez_____

Jurado

_____

Jurado

Bogotá D.C Marzo 2017.

CONTENIDO

Pág.

Pág.

Pág.

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

1. TÍTULO DEL PROYECTO

AUDITORÍA AL SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁCION EN EL PROCESO DE DESARROLLO DE SOFTWARE DE ACUERDO A LA NORMA ISO/IEC 27001:2013 EN LA EMPRESA IT STEFANINI COLOMBIA.

2. INTRODUCCION

La seguridad Informática y de la información es un concepto de vital importancia para cualquier organización en la actualidad, esto se debe a la necesidad de proteger la información propia, de clientes y terceros que cada día se vuelve relevante si se quiere mantener cualquier negocio.

Garantizar al mercado y público en general que una determinada organización cumple con los requerimientos de seguridad ha sido un tema complicado a tal punto que hoy las organizaciones exigen a sus proveedores la implementación de un sistema de gestión de seguridad de la información, y a su vez certificar este ante un organismo competente.

En este proyecto se pretende revisar el cumplimiento de un sistema de gestión de seguridad de la información de acuerdo a la norma estandarizada ISO 27001:2013 en su anexo A, este procedimiento de revisión se llevara a cabo de manera metodológica a través de una auditoria, la cual será el pilar fundamental de este proyecto de grado, donde se documentara las fases, procesos, evidencias y reportes que se requieren para la entrega final de un informe en el cual se exponen las opciones de mejora que permitan a la empresa (I&T STEFANINI Colombia S.A) tomar la decisión de incluir en el plan estratégico del siguiente año la implementación y certificación del sistema de gestión de seguridad basado en la norma ISO/IEC 27001:2013.

3. DEFINICION DEL PROBLEMA

3.1 ANTECEDENTES

Actualmente en IT Stefanini Colombia existe un procedimiento de seguridad controlado en su fábrica de software, este proceso se queda en manejo interno de la organización y no existe una certificación oficial que permita a otras organizaciones tener la certeza de contratar un proveedor que garantice conservar las características de seguridad de la información durante el ciclo de vida de los aplicativos, estas características son integridad, disponibilidad y confidencialidad, debido a ello cuando un cliente requiere el desarrollo de alguna aplicación o la celebración de un contrato de provisión de software y soporte al mismo debe solicitar una serie de evidencias que acompañadas por una auditoria evalúan la posibilidad de la celebración de dicho contrato provocando retrasos, sobrecostos y dilaciones que pueden llevar a la perdida de la oportunidad comercial.

De acuerdo al anterior análisis de la problemática se puede definir el problema al que se buscara solución mediante este proyecto.

3.2 FORMULACION DEL PROBLEMA

¿Por qué la auditoría al sistema de gestión de seguridad información de acuerdo a la norma ISO/IEC 27001:2013 permitirá establecer el estado actual de la seguridad de la información en el proceso de desarrollo de software en la empresa IT STEFANINI COLOMBIA?

4. JUSTIFICACIÓN

ISO 27001:2013 actualmente es la norma internacional más importante en gestión de seguridad de la información y muchas empresas han certificado su cumplimiento en el mundo y Colombia, es por esto que IT Stefanini Colombia con la intención optimizar y controlar sus procesos ha decidido optar por evaluar el estado actual de la gestión de seguridad informática especialmente en el proceso de desarrollo de software; esto le permitirá tener un diagnostico general de que medidas debe tomar para implementar y certificar el cumplimiento de la norma de manera oficial con la cual puede robustecer la marca en el mercado y cumplir aspectos regulatorios de las organizaciones contratantes y el entorno, así como establecer una línea de sinergia con la certificación actual de la norma ISO 9001:2008.

Con la ejecución de la auditoria al SGSI basado en la ISO 27001:2013 y sus resultados se beneficia principalmente la empresa ya que se dispondrá del diagnóstico del SGSI actual y las medidas que se deben tomar para lograr la implementación y certificación.

Se beneficiarán también los desarrolladores porque se optimizará la gestión y la documentación en el proceso de construcción de productos software con base en las oportunidades de mejora, aumentando la seguridad del mismo al interior de la organización.

Adicionalmente se beneficiarán los clientes de la organización ya que se dispondrá de un socio de negocios garante de toda confiabilidad en cuanto al desarrollo del software que se contrate.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Establecer el estado actual de la gestión de seguridad información en el proceso de desarrollo de software mediante una auditoria interna teniendo como referente la norma ISO/IEC 27001:2013, lo cual permitirá generar un informe final de auditoria con oportunidades de mejora que permitan a la alta dirección contemplar en el plan estratégico la implementación y certificación del estándar ISO 27001:2013.

5.2 OBJETIVOS ESPECÍFICOS

- Conocer el funcionamiento de los procesos de desarrollo de software al interior de la empresa para establecer la situación actual en cuanto a la seguridad informática y de la información.

- Elaborar el plan de auditoría y diseñar los instrumentos para recolección de información y pruebas que se llevarán a cabo para determinar los recursos necesarios para realizar la auditoría al SGSI

- Verificar la existencia de las áreas de proceso, seguimiento y ejecución de las prácticas y metas genéricas y especificas del modelo CMMI L3 para lo cual se realizará una evaluación SCAMPI C del proceso, aplicar los instrumentos y pruebas de auditoria que permitan conformar los hallazgos de seguridad encontrados en el proceso de desarrollo de software.

- Elaborar y entregar a la gerencia de IT Stefanini el informe final de auditoria con recomendaciones y observaciones del auditor que permita a la alta dirección contemplar la decisión de implementar y certificar el estándar ISO 27001:2013 en el proceso de desarrollo de software.

6. ALCANCE Y DELIMITACION DEL PROYECTO

Realizar una auditoría al sistema de gestión de seguridad información en el proceso de desarrollo de software en IT Stefanini Colombia según los requisitos contemplados en la norma ISO/IEC 27001:2013 y los objetivos de control contemplados en la norma ISO/IEC 27002:2013, con la finalidad de entregar un informe de auditoría a la alta dirección en el cual se refleje el estado actual de la seguridad de la información en el proceso y permita contemplar la implementación y certificación del estándar en el plan estratégico de la organización.

7. MARCO REFERENCIAL

7.1 ANTECEDENTES

Desde finales del siglo XX junto al auge de las tecnologías de la información y su uso productivo en las empresas se identificaron debilidades en la conformación de sistemas informáticos e infraestructuras tecnológicas que en ocasiones significaban la destrucción parcial o total de un sistema informático ya sea por accidente, desastre o de manera intencional. En vista de esto las organizaciones idearon la manera de poder protegerse de estas amenazas y garantizar a sus clientes el cumplimiento de estándares que les permitieran tener la confianza para establecer un negocio con ellas, es así que aparecen normas como BS 7799-2:1999 Information Security Managment que sirvieron de base para la creación y consolidación de normas reconocidas hoy mundialmente por la ISO y el IEC como la ISO/IEC 27001 y que fundamentan las certificaciones de gestión de la seguridad de la información que el mercado requiere para garantizar un correcto, seguro y optimizado manejo de las tecnologías de la información y de la informática, así como los datos y la información que reside y es procesada por estas.

En Colombia se pueden encontrar casos de implementación de la norma ISO 27001:2013 en empresas como Unisys Colombia o Redcom ltda, además de otros adicionales promovidos por las áreas internas de calidad o por aporte de algún estudiante en su proyecto de grado a las organizaciones, en ambos casos es notorio el aporte que se realiza a la seguridad de la información y a la estandarización de la norma como elemento diferenciador en el proceso de gestión de la seguridad informática en cualquier empresa.

Se puede citar el trabajo desarrollado por Diana Marcela Cortes y Alix Victoria Ardila denominado *metodología para la implementación de un sistema integrado de gestión con las normas ISO 9001, ISO 20000 e ISO 27001* presentado en Junio de 2012 en la universidad EAN de Colombia, con el cual se realiza un acercamiento al objetivo común de cualquier estándar que desee certificar una organización, este objetivo común se centra en la mejora continua de los procesos que se vean involucrados, sea calidad, gestión informática, o gestión de la seguridad de la información; es posible visualizar en este trabajo una metodología para la implementación y apoyo en la implementación de un sistema de gestión, lo cual presta utilidad para este proyecto en el momento de diferenciar cada etapa del proceso de implementación y las ventajas que con ello se obtiene.

Se tiene en cuenta de la misma manera el trabajo realizado por Andrea Ariza Díaz denominado *Elaboración de un plan de implementación de la ISO/IEC 27001:2005* presentado en Junio de 2013 en la Universidad Autónoma De Barcelona, España,

en el cual se realiza una descripción paso a paso de la auditoria de preparación e implementación de un SGSI basado en la norma ISO 27001:2005 en una entidad financiera en Colombia; este trabajo permitirá orientar en este proyecto el proceso de planificación y ejecución de la auditoria de preparación para la certificación en ISO/IEC 27001:2013 en el proceso de desarrollo de software y en toda la organización IT Stefanini Colombia (2).

7.2. MARCO TEORICO

7.2.1 La Auditoria

La auditoría de un sistema de gestión, para nuestro caso gestión de la seguridad de la información es un instrumento metódico que nos permite evaluar el estado actual de un proceso.

Se debe establecer un diagnóstico inicial de los procesos a auditar, para posteriormente planear como realizar la auditoría, que recursos se van a necesitar y en qué tiempo se llevara a cabo; luego de ejecutar la auditoria como tal, se revisa el proceso de gestión que llevó a realizar la auditoria para evaluarlo y así poder emitir un informe con las opciones de mejora y sugerencias para optimizar el proceso o sistema de gestión auditado, es decir, que en la auditoria se puede identificar 4 etapas claramente que serán las que se desarrollaran durante este proyecto, estas son:

- Diagnosticar el estado actual del SGSI.
- Planear la auditoria al SGSI
- Ejecutar la auditoria al SGSI
- Reporte de la auditoria del SGSI

Las auditorias generalmente tienen una finalidad, para el caso de este trabajo de grado será realizar las observaciones necesarias a la alta dirección mediante el informe de auditoría con lo cual se podrá contemplar en el plan estratégico de la organización la implementación del SGSI basado en la norma NTC ISO/IEC 27001:2013 en el proceso de desarrollo de software en la empresa IT Stefanini Colombia.

7.2.2 La Auditoria Informática

Nace en los últimos años como una rama alterna de la auditoría financiera o contable en la cual el profesional tiene cierta especialidad en las tecnologías de la información y por medio de esta puede profundizar más en dicha auditoria detectando fallas en procesos en los que se vean involucrados activos informáticos, su finalidad sigue siendo la misma, la protección de activos y la

integridad de los datos y por medio de estos conservar la efectividad y eficiencia de los procesos organizacionales. Las actividades del auditor informático de deben centrar en la evaluación y prueba de los controles informáticos más complejos en los cuales se hace uso de herramientas mecanizadas y automatizadas como programas informáticos conocidos como CAAT, Computer Asisted Audit Tools, esto debido a que hoy día es muy difícil poder cubrir de manera manual los procesos informáticos de las organizaciones.

7.2.3 El auditor informático

Es el responsable de la revisión de los controles implantados informando a la dirección de la organización sobre su funcionamiento y opciones de mejora, el auditor debe ser una persona confiable y perspicaz ya que debe detectar desviaciones en los procesos los cuales muchas veces solo conoce por medio de información suministrada en informes previos o manuales de operación.

Algunas de las funciones principales del auditor informático son:

- Ser participe y garante en todas las fases del ciclo de desarrollo de software.
- Efectuar revisiones a los controles implantados en las aplicaciones informáticas validando que se adapten al marco legal, mejores prácticas del sector en cuanto a requisitos funcionales y no funcionales y al contrato de solicitud de la aplicación o requerimientos de usuario.
- Realización de pruebas de rendimiento, capacidad, eficiencia y confiabilidad de los equipos y programas informáticos.

7.2.4 Estándar ISO/IEC 27001

Es una norma que ha sido establecida para ilustrar los requisitos de establecimiento, implementación, mantenimiento y mejora continua de una SGSI en organizaciones de todo tipo, estas organizaciones pueden decidir su implementación como una decisión estratégica influenciada por los objetivos y necesidades de sus partes interesadas y su entorno.

Un sistema de gestión de seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgo basado en la norma ISO/IEC 27005 y brinda confianza a todas las partes interesadas de que los riesgos son gestionados de manera adecuada.

El ente propietario del estándar y responsable de su actualización es el International Standart Organization y el International Electrothecnical Commission, en Colombia la organización encargada de velar por la actualización y traducción fidedigna al español colombiano de la norma es el Instituto Colombiano de Normas Técnicas ICONTEC, y la última actualización del estándar se realiza en octubre de 2013.

Esta norma está compuesta por 10 numerales que se tomaran como referencia de auditoria en el proceso de desarrollo de software, adicionalmente esta norma enmarca también los objetivos de control y controles de referencia que permitirán que el Sistema de Gestión de Seguridad de la Información en el proceso funcione de manera efectiva y eficiente, estos controles son los mencionados en la norma NTC ISO/IEC 27002:2013 y se componen de:

14 Dominios.

35 Objetivos de Control.

114 controles.

7.2.5 Estándar CMMI

Capability Maturity Model Integration

Es un modelo enfocado en las fábricas de software para la mejora y evaluación de procesos, especialmente enfocado en el desarrollo, mantenimiento, operación y retiro de sistemas, lo que se denomina ciclo de vida del software.

Incluye:

Buenas prácticas reconocidas en el mercado.

Referencias para fijar objetivos.

Referencias para dar prioridades.

Se puede decir que es producto de la integración de varios estándares como ISO 9001, Marcos de buenas prácticas como ITIL, COBIT, 6Sigma y la experiencia de la industria global.

CMMI posee 5 niveles de calificación y certificación respecto al nivel de madurez de la empresa, la certificación de un nivel se realiza bajo la metodología SCAMPI la cual se analiza en el marco metodológico.

Los organismos responsables de la creación y actualización del estándar son el Software Engineering Institute y la Universidad Carnegie Mellon.

Actualmente IT Stefanini Colombia es participe de la convocatoria del ministerio TICS de Colombia para certificar el proceso de desarrollo de software y las fabricas continuas en el nivel CMMI nivel 5, sin embargo, para este proyecto se auditara el nivel 3 ya certificado, esto se realizara mediante la evaluación SCAMPI C por su sencillez y flexibilidad debido a que este proceso de recertificación por si solo conlleva un trabajo extenso que requiere de aplicación de una metodología más extensa y rigurosa como SCAMPI A que por sí solo podría ser considerada como otro proyecto de grado.

7.2.6 metodología SCAMPI: CMMI

Standard CMMI Appraisal Method for Process Improvement (Método estándar de evaluación CMMI para mejora de procesos)

La evaluación SCAMPI determina el nivel, de madurez o capacidad, que ha alcanzado una organización que aplica CMMI en sus procesos.

Existen tres clases de evaluaciones SCAMPI:

- Clase A: El más amplio y reconocido oficialmente.

Este tipo de evaluación solamente puede ser realizada por un auditor entrenado por el SEI o institución asociada y debe contar con autorización del Software Engineering Institute

- Clase B: Es menos amplio y detallado que la clase “A” y más económico.

Este tipo de evaluación debe ser realizada por un personal experto y certificado por el SEI o institución asociada, para esta evaluación no hay reconocimiento

oficial por ende no es necesario que este autorizado por el Software Engineering Institute.

- Clase C: Es el más sencillo, económico y requiere una capacitación menor.

Este tipo de evaluación puede ser realizada por una persona con conocimientos en CMMI y SCAMPI, no requiere estar certificado por SEI o Institución asociada y tampoco requiere estar autorizado por el Software Engineering Institute.

Las 4 funciones principales de las evaluaciones son:

Analizar,

– Como trabaja la organización respecto a una referencia que comúnmente se encuentra en el mercado o sector económico.

– Como la estabilización de procesos influye en fuentes de cambio.

Motivar,

– Como soporte para una cultura de cambio organizacional.

– Al cambio incluyendo procesos de autoanálisis al interior de las organizaciones.

Transformar

– Haciendo que todos los involucrados vean las cosas de la misma forma.

– Impulsando los esfuerzos de la gerencia.

– Permitiendo al personal involucrado una libre manera de pensar enfocándose en lo que se está haciendo mal y como corregirlo.

– Impulsando y comunicando las mejoras.

– Fomentando una cultura de análisis riguroso

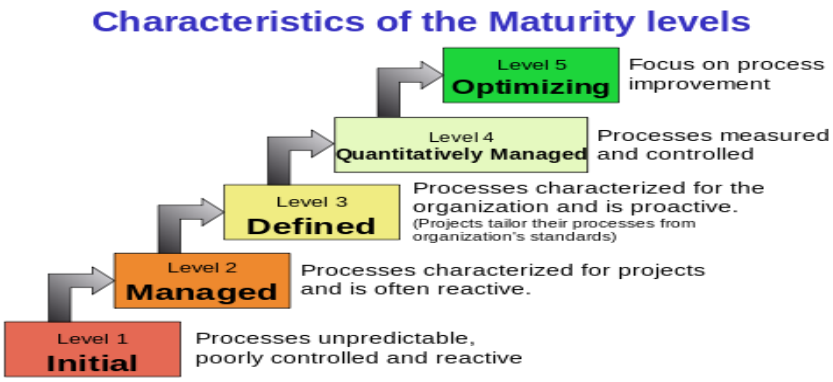
Educar

– Las organizaciones comprenden y aplican las mejores prácticas del sector.

– La mejora continua es producto de la evaluación constante, por medio de las evaluaciones los interesados conocen su entorno, su organización y sus procesos, de esta manera pueden compararlos frente a la competencia y el mercado.

Los niveles de certificación de SCAMPI son:

Fig. 1: Niveles de madurez CMMI.



Nombre de la fuente: Internet https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration

7.3 MARCO LEGAL

Aunque en Colombia no existe ninguna norma que reglamente la auditoria informática ni tampoco la certificación de sistemas de gestión en las empresas de orden privado o público existen algunas normas a través de la historia colombiana que permiten tener un acercamiento al objetivo de una auditoria informática y la certificación por entes nacionales o internacionales sobre la madurez de sus sistemas de gestión, sean estos, calidad, ambiental, informática o seguridad de la información.

De esta manera se exponen:

Ley 1712 de 2014 por la cual se regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y excepciones a la publicidad de la información.

Decreto 2124 de 2012, el Gobierno Nacional reitera al ONAC, como organismo nacional de acreditación para ejercer y coordinar las funciones relacionadas con los objetivos del Sistema Nacional de Normalización, Certificación y Metrología fundamentalmente para promover en los mercados la seguridad, la calidad y la competitividad del sector productivo o importador de bienes y servicios y proteger los intereses de los consumidores.

Ley 1581 de 2012 por la cual se reglamenta el régimen general de la protección de datos personales en Colombia.

Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 de 2009, sobre principios y conceptos sobre la Sociedad de la Información y la Organización de las Tecnologías de la Información y las Comunicaciones.

Decreto 4738 de 2008, se designó al ONAC como Organismo Nacional de Acreditación y se le señalaron las funciones que en esa condición le corresponde cumplir. *En febrero de 2009 el ONAC emitió las primeras acreditaciones.*

Decreto 2870 de 2007, por medio del cual se adoptan medidas para facilitar la Convergencia de los servicios y redes en materia de Telecomunicaciones.

Decreto 600 de 2003, por medio del cual se expiden normas sobre los servicios de valor agregado y telemáticos y se reglamente el Decreto-ley 1900 de 1990.

Resolución 36904/2001, de 6 de noviembre de la Superintendencia de Industria y Comercio, Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.

7.4 MARCO CONTEXTUAL

7.4.1 HISTORIA

Nace en 1987 como una compañía de capacitación en Jaguariouna San Pablo-Brasil, a través del tiempo se ha convertido en una importante empresa multinacional de tecnología a nivel mundial, su representación se asegura en varios países por medio de compañías filiales las cuales han sido adquiridas por el grupo central, estas compañías subsidiarias se ubican en países estratégicos que permiten ampliar la cobertura de la organización en zonas de alto impacto para los servicios de consultoría y desarrollo de sistemas proyectando cada vez un crecimiento mayor. Como antecedentes importantes es posible mencionar cronológicamente los eventos más importantes como 1987 cuando es fundada Stefanini como una compañía de capacitación, posteriormente en el año de 1989 se abre la primera oficina en la misma ciudad, hasta este momento los servicios ofrecidos continúan centrándose en la capacitación de personal de empresas privadas y públicas nacionales en el manejo de sistemas, en 1990 se inicia la fábrica de software y con ella los servicios de mantenimiento y soporte a sistemas, luego en 1994 se inicia con fábricas especializadas dedicadas al desarrollo de soluciones de software personalizadas o a la medida según la industria o el mercado, al ampliarse los servicios ofrecidos se debe ampliar la organización por lo que en el año de 1995 se abren las primeras oficinas fuera de la ciudad de San Paulo, ubicadas en Campiñas, Curitiba y Porto Alegre, debido a los buenos resultados y la estrategia corporativa es posible en el año de 1996 iniciar operaciones en el extranjero, dando apertura a una oficina en Argentina, de esta manera Stefanini cambia su proyección en el horizonte enfocándose en el mercado internacional donde los negocios de software, entrenamiento, consultoría y servicios empiezan a aumentar su demanda.

El nuevo siglo trae nuevos desafíos para los cuales Stefanini refuerza su estrategia internacional abriendo oficinas en Chile y México en el año 2000, ampliando operaciones en el continente norte americano donde en el año 2001 se consolida abriendo oficinas en Estados Unidos y en Suramérica adquiriendo subsidiarias en Colombia y Perú. Para el año 2003 Stefanini incursiona en el continente europeo realizando la apertura de oficinas en España, Portugal e Italia, durante el año 2005 Stefanini obtienen la certificación CMMI Nivel 5 a nivel global excluyendo las compañías subsidiarias de Colombia y Perú, sin embargo, se inicia en estas el proceso de certificación donde más adelante se logrará obtener el nivel 3 de CMMI.

En el año 2006 Stefanini confirma su presencia global con una nueva oficina en Londres y otra en la India., y en el año 2008 se abre la representación en Canadá.

En 2009 Nace Stefanini Document Solutions a partir de la adquisición de la empresa Callere. Stefanini obtiene la Certificación MPS.BR nivel A. y en 2010: Stefanini compra Tech Team, una importante adquisición que da impulso a la continuación del proceso de globalización. Además, crece y adquiere una empresa brasilera con una cartera centrada en seguridad, la VANguard, continuando la nueva estrategia de crecimiento global en 2011 Stefanini adquiere CXI en los EEUU e Informática & Tecnología en Colombia, además de crecer de forma orgánica, inaugurando 7 nuevas oficinas en Brasil, en 2015: Stefanini continua expandiendo a nivel global abriendo oficinas en Indonesia de esta manera reafirma y se consolida en oriente, se esperan nuevas adquisiciones a nivel global para los años siguientes los cuales fortalecerán la marca y sentido de pertenencia de sus funcionarios.

Sobre IT Stefanini Colombia S.A

Informática y Tecnología S.A., inicios Stefanini Colombia

Fundada en noviembre de 1990 en sus inicios se dedicaba al desarrollo e implementación de sistemas administrativos-financieros para el sector industrial y de servicios en Colombia.

7.4.2 Misión

Transformar en realidad los sueños de nuestros clientes, colaboradores y accionistas, por medio de soluciones de Tecnología e Innovación[1].

7.4.3 Visión

Ser el mejor proveedor de Tecnología, ser reconocido a nivel global, y admirado como un socio estratégico, actuando con pasión y energía para conquistar nuevos clientes[2].

[1] Tomado de http://www.stefaninicolombia.com/mision-vision-valores/

[2] Tomado de http://www.stefaninicolombia.com/mision-vision-valores/

7.4.4 Certificaciones en Colombia

ISO 9001: 2008.

CMMI Nivel 3. Del Software Engineering Institute

7.4.5 Certificaciones Global

ISO 9001: 2008.

ISO 20000: 2011.

ISO 27001: 2013.

CMMI Nivel 5. Del Software Engineering Institute

MPS/BR – Nivel A: El sistema de reutilización de valores MPS.BR cuenta con siete niveles que van desde un mayor grado de madurez, G. En la actualidad, además de Stefanini, un selecto grupo de sólo cuatro compañías han alcanzado esta misma hazaña a nivel mundial.

7.5. MARCO CONCEPTUAL

Durante el desarrollo del proyecto de auditoria se evaluarán los siguientes criterios de acuerdo al estándar ISO/IEC 27001:2013.

7.5.1 La Confidencialidad: Se refiere al aseguramiento de que la información solo es conocida por las personas autorizadas y con interés en dicha información.

7.5.2 La Integridad: Se refiere a que la información permanezca completa y sin alteraciones, que sea confiable y si es modificada existan soportes de la modificación y sus causas, y esta modificación solo ha sido realizada por las personas autorizadas para ello.

7.5.3 La Disponibilidad: Se refiere a que la información siempre esté disponible para quien la requiere y está autorizado para verla o manipularla, se debe asegurar la información sin importar el medio en el cual es accedida.

7.5.4 La Autenticidad: Es el atributo de la información que la hace verdadera y confiable.

7.5.5 La Trazabilidad: Es el atributo de la información que nos permite establecer una historia de cambios y quien los realiza, también nos permite validar la identidad de la persona o proceso que realiza un cambio, esto comúnmente es llamado como no repudio.

7.5.6 La Conformidad: Indican las actividades que cumplen con los lineamientos de una norma, también se pueden mencionar como oportunidades de mejora como se define en la ISO 9001, el elemento funciona, pero se puede tener mayor beneficio de su uso.

7.5.7 La No conformidad: Las no conformidades son instancias donde los requisitos de la norma no son cumplidos, las cuales pueden ser una opción de mejora del sistema de gestión.

7.5.8 No conformidad Menor: Un único lapso, caso, ocurrencia o falta parcial observada en la aplicación práctica de un procedimiento durante una auditoria., también se denomina como mal uso, por ejemplo: Está definido un documento, pero no se usa a cabalidad, en el caso de un proceso o formato no se diligencia completamente o se ha modificado sin reportar el cambio.

7.5.9 No conformidad Mayor: Incumplimiento en relacionar cualquier cláusula de la norma u otros criterios contra los cuales se está realizando la auditoria. Puede ser también el Incumplimiento en la ejecución de uno de los requisitos de la norma o falla sistemática para seguir los requisitos del sistema de gestión de la organización, también se denomina como no uso, por ejemplo: Está definido un documento o proceso, pero no es usado o no se sigue en la ejecución de una acción.

7.5.10 La Observación: Catalogación interna de las debilidades en el sistema que encuentra el auditor y que no pueden ser soportadas contra la norma y/o contra los documentos definidos en el Sistema.

7.5.11 La Acción correctiva u oportunidad de mejora: Una acción para eliminar la causa de una No Conformidad, detectada u otra situación indeseable existente, con el propósito de evitar que vuelva a ocurrir.

7.5.12 La Acción preventiva: Una acción para evitar a priori el suceso que da origen a una no conformidad, son acciones antes de una auditoria.

7.5.13 La Corrección: Acción tomada para eliminar una no conformidad detectada, específicamente antes de ejecutar un plan de acción, la corrección siempre debe ser adecuada a los efectos de las no conformidades encontradas.

8. MARCO METODOLÓGICO

El proyecto de grado se encuentra orientado a la realización de una Investigación de campo de tipo explorativa como se denominara a la auditoria interna respecto a la norma ISO 27001:2013 en el proceso de desarrollo de software, actualmente el proceso se encuentra certificado con el estándar CMMI Nivel 3 por el Software Engineering Institute y la Universidad Carnegie Mellon y en cuanto a calidad del software por la norma ISO 9001:2008, por tanto para la para revisión del estado actual del proceso se requiere la programación de una evaluación de la existencia de las áreas de proceso, metas y prácticas genéricas del proceso de desarrollo de software, la cual junto con una auditoria reflejara el estado actual de la seguridad de la información en el proceso:

8.1. METODOLOGIA DE DESARROLLO

Se debe programar y realizar una visita de reconocimiento a la fábrica de software para verificar el funcionamiento del proceso de construcción de software, las instalaciones, los equipos y programas utilizados, reconocer al recurso humano que desarrolla la labor y evaluar las medidas de seguridad de la información existentes.

Posteriormente se procederá a la realización del plan de auditoria para lo cual se debe definir una fecha inicial y final junto con el área de calidad, infraestructura y los directores de proyectos de la fábrica de software, en este momento se deben definir los recursos que se requieren para el desarrollo de la auditoria como son, presupuesto, tiempo, recurso humano, equipos informáticos, instrumentos de auditoria, auditor líder, etc…

Al haber definido los recursos y el plan de auditoria se procederá con la ejecución según lo pactado entre las gerencias, la dirección y el equipo auditor, durante la auditoria el equipo auditor tomará parte objetiva del proceso y anotará los hallazgos encontrados para posteriormente elaborar un dictamen preliminar y presentarlo a discusión con el equipo auditor.

Por ultimo después de haber discutido los hallazgos con el equipo auditor se procederá a la realización del dictamen final y realización del informe de auditoría en el cual se muestren las oportunidades de mejora en la seguridad de la información del proceso respecto a la norma ISO/IEC 27001:2013, este informe se entregara a la Gerencia General de IT Stefanini para que se implementen las

opciones de mejora que permitan contemplar la implementación del estándar ISO 27001:2013 en el plan estratégico organizacional.

9. PLANEACION DE LA AUDITORIA

9.1 Recursos Necesarios para el desarrollo:

9.1.1 Recursos Humanos:

Es el personal que desarrollara la auditoria, el recurso humano debe reunir algunas características como son el conocimiento de la norma ISO/IEC 9001, ISO/IEC 27001 y el estándar CMMI, adicionalmente debe estar acreditado como auditor de sistemas de gestión y para esta auditoria se podrá optar por usar recursos propios como funcionarios asignados al área de calidad, control interno o proyectos externos.

9.1.2 Equipamiento informático:

Es el equipo tecnológico que se utilizara para la planeación, desarrollo e informe final de auditoria, entre el equipamiento necesario se puede considerar: computadores portátiles, tabletas, pdas, cámaras, dispositivos USB, módems portátiles.

9.1.3 Instalaciones:

Se debe disponer de un sitio sobrio y organizado, con escritorios de trabajo y sillas, separado del lugar auditado en el cual los auditores puedan reunirse para realizar discusiones de auditoria, planeación, ingreso de datos al software y realizar la preparación del informe final de auditoria.

9.1.4 Tiempo:

Es el espacio temporal durante el cual se desarrollará la auditoria, desde la visita de reconocimiento y planeación hasta la entrega y exposición a la gerencia del informe final de auditoria, se puede definir en días o meses.

9.1.5 Documentos de auditoria:

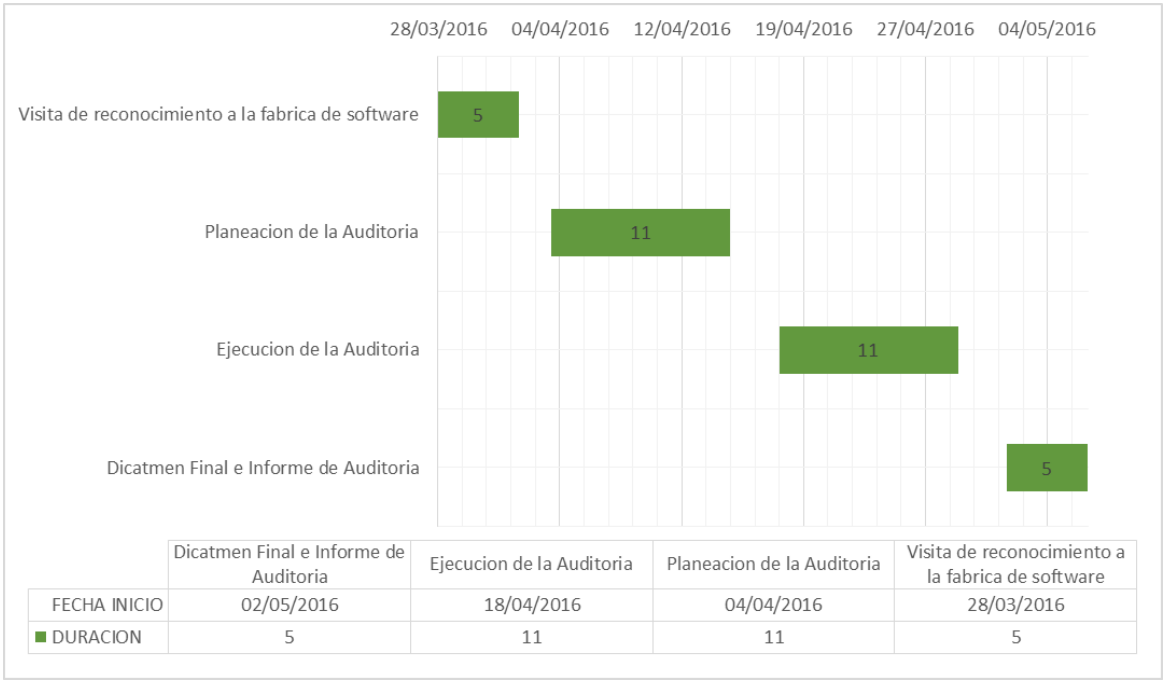
Son los materiales que permitirán llevar a cabo el correcto y organizado desarrollo de la auditoria, estos se van a definir durante la fase de planeación y pueden incluir: check list, formatos de entrevistas, cuestionarios generales, informes parciales de auditoria o notas de auditoria.

9.1.6 Instrumentos de Auditoria

Son los materiales con los cuales se apoyará el desarrollo de la auditoria y facilitaran tanto el desarrollo como la entrega del informe final de auditoria, entre ellos se incluyen: estándares, informes de auditorías previas, matrices de riesgos y software de auditoria.

9.1.7 Plan de tiempo

Fig. 2. Cronograma de actividades



	Dicatmen Final e Informe de Auditoria	Ejecucion de la Auditoria	Planeacion de la Auditoria	Visita de reconocimiento a la fabrica de software
FECHA INICIO	02/05/2016	18/04/2016	04/04/2016	28/03/2016
DURACION	5	11	11	5

Nombre de la fuente: El autor

9.1.8 Talento Humano del Proyecto

Auditor Interno: Javier Olivo García Araque

10. AUDITORIA AL SGSI DEL PROCESO DE DESARROLLO DE SOFTWARE EN IT STEFANINI COLOMBIA

10.1 PROCESO DE DESARROLLO DE SOFTWARE IT STEFANINI COLOMBIA.

Por ser uno de los servicios y procesos CORE de la compañía existen varias fábricas de software que desarrollan programas a la medida para diferentes organizaciones privadas, publicas, nacionales y extranjeras, adicionalmente apoyados en la presencia mundial de la organización es posible hacer uso de los recursos humanos ubicados en otras fábricas de software ubicadas en otros países y de esta manera coordinar las tareas y entregas dentro de cada proyecto de fábrica.

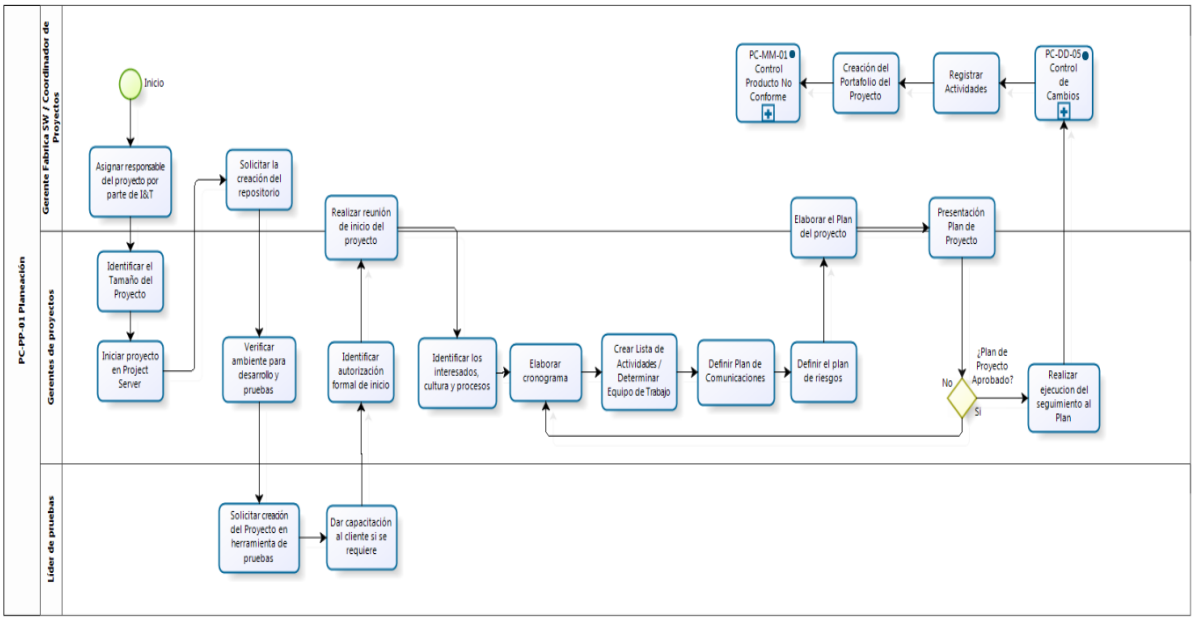
IT Stefanini Colombia aplica el desarrollo de las prácticas de desarrollo ágil de software lo que le permite tener gran competencia en el sector y ser diferente a las demás empresas que ofrecen servicios similares, la práctica ágil por excelencia utilizada se basa en la metodología SCRUM y el desarrollo se planifica y optimiza utilizando los sprint que ofrece esta metodología.

Sin embargo, el proceso de desarrollo de software en IT Stefanini Colombia va mucho más allá al punto que goza de 2 estándares independientes que garantizan su correcto desempeño, el CMMI L3 y el ISO 9001:2008 en la calidad de software.

Para tener un completo entendimiento de cómo funciona el proceso internamente en la organización se puede visualizar como está diseñado y su operabilidad.

A continuación, se observará los diagramas BRM del proceso de desarrollo de software y fábricas continuas de software en la organización IT Stefanini Colombia junto con la descripción del proceso.

Figura 3. Proceso de planeación del desarrollo de software,



Fuente: procesos IT Stefanini Colombia.

10.1.1 Objetivo

Definir todas las actividades que le permitan a los líderes de proyecto por parte de I&T STEFANINI y por parte del cliente saber:

- Qué se debe hacer – objetivos y magnitud o alcance del trabajo
- Cómo se debe hacer – estrategia
- Quién lo debe hacer – roles y responsabilidades
- Para cuándo se debe hacer – cronograma
- Cuánto costará – presupuesto
- Qué tan bueno tiene que ser – calidad
- Qué desempeño se requiere – especificaciones
- Qué riesgos existen

10.1.2 Alcance

Para todos los contratos u órdenes de trabajo desarrollados por I&T STEFANINI, y que hayan sido clasificados como “PROYECTOS” de acuerdo con el instructivo IN-PP-01 Guía para la ejecución de proyectos en I&T STEFANINI.

10.1.3 Descripción del proceso:

El primer paso del proceso describe la selección del responsable del proyecto por parte de I&T STEFANINI; lo anterior consiste en la validación de los recursos humanos disponibles dentro de la compañía que cumplen los requisitos y perfil requerido por el trabajo a desarrollar. Esta actividad es desarrollada por el gerente de la fábrica de software.

El segundo paso consiste en el dimensionamiento del proyecto, aquí se define el tamaño y los entregables con fechas de compromiso, esta actividad es desarrollada por el responsable del proyecto elegido en el paso uno.

El tercer y cuarto paso tiene que ver con la configuración de ambientes y repositorios, la infraestructura que se utilizara para el desarrollo del proyecto, esta actividad es desarrollada por el área técnica de infraestructura, el gerente de la fábrica de software y el gerente de proyecto.

El quinto paso se relaciona con la configuración y verificación de los ambientes suministrados para desarrollo y pruebas, compatibilidad con versiones de producción y que la arquitectura se adapte al plan de proyecto.

El sexto y séptimo paso se relaciona la creación de las herramientas de pruebas de software y la capacitación al cliente para que este pueda realizar el seguimiento, esta actividad es desarrollada por quien desempeña el rol de líder de pruebas.

Octavo y noveno pasos son desarrollados por el gerente del proyecto y se relacionan con la autorización del cliente del inicio del proyecto y la realización de la reunión de apertura de proyecto donde se dejan claras las reglas de juego durante el proyecto.

El décimo paso se relaciona con la identificación de los interesados, la cultura y los procesos de los clientes, esta actividad la desarrolla el gerente de proyectos.

El paso once y doce se relacionan con la lista de actividades a desarrollar y el cronograma, se define el tiempo y equipo de trabajo. Estos son desarrollados por el representante del cliente del software y el gerente de proyecto.

Los pasos trece y catorce se relacionan con la definición del plan de comunicaciones y el plan de riesgos del proyecto, esta actividad se realiza por el gerente de proyecto y el representante del cliente.

Los pasos quince y dieciséis se relacionan con la elaboración del plan de proyecto en la cual se incluyen los presupuestos, y la presentación del plan a los interesados del cliente y equipo de trabajo que desarrollara el proyecto, esta actividad es realizada por el gerente de la fábrica de software y el gerente del proyecto.

El paso diecisiete se relaciona con la ejecución del plan del proyecto según lo presupuestado, esta actividad es liderada por el gerente de proyecto y desarrollada por el equipo de trabajo.

El paso dieciocho se relaciona con la fase del ciclo de vida del software denominada control de cambios, donde se evalúan los impactos y presupuestos, esta actividad es desarrollada por el gerente de la fábrica de software.

Los pasos diecinueve y veinte se relacionan con el registro de las actividades del proyecto en la bitácora y la creación del portafolio del proyecto, esta actividad se realiza por el gerente de proyecto y gerente de la fábrica de software.

La fase final se relaciona con la entrega de producto conforme o revisión del producto no conforme y devolución en el ciclo hasta un nuevo cronograma, si el producto es conforme se realiza la entrega de fuentes, líneas base, documentación, manuales, licencias y de más documentación y herramientas del proyecto al cliente quien es su propietario, de aquí se saltaría a otro proceso relacionado con el soporte post implementación y garantía según lo contratado, finalmente se cierra el proyecto.

10.1.4 Seguridad del proceso:

Actualmente I&T STEFANINI recarga las actividades concernientes a la seguridad de la información en el gerente de proyecto, el gerente de la fábrica de software y el gerente de infraestructura, quienes de acuerdo a reuniones efectuadas, acuerdos interoperabilidad y contratación entre áreas y políticas de seguridad existentes en la organización manejan y coordinan la administración segura de los recursos, físicos, humanos y la información bajo un esquema de gobernabilidad y control fundamentado en la supervisión de actividades desarrolladas.

El acceso internet es controlado y filtrado, sin embargo, el acceso es abierto para todo el personal de la organización con restricción de sitios de ocio o de alto uso de recursos de conexión.

Adicionalmente se tienen en cuenta los requerimientos de seguridad del cliente que solicita o requiere un producto, es decir que si un cliente solicita que se realice estudio de seguridad sobre el equipo de trabajo, analistas, ingenieros, desarrolladores y en general todo el personal que tendrán acceso a la información este se realiza y se factura al cliente de lo contrario no se realiza abaratando el costo total del producto ofrecido al cliente minimizando costos y gastos que se van a transferir a él en la factura del producto, sin embargo en toda la planta humana de la organización existe un estricto control de ingreso de personal el cual valida experiencias anteriores y referencias personales y laborales.

Por otra parte las instalaciones de la fábrica de software ubicadas en la sede en la cual se realizara la auditoria se encuentran separadas en un piso diferente a la gestión administrativa, pero contigua al área de infraestructura, la gerencia de calidad y operaciones, no existe un aislamiento físico de las áreas de desarrollo, prueba y producción ya que en algunas ocasiones estos ambientes son dispuestos a través de enlaces VPN a las arquitecturas de los clientes ubicadas dentro de sus entornos empresariales, tampoco existe vigilancia en la sede contratada directamente por la organización, solo se cuenta con la vigilancia del edificio donde funciona la misma, el CCTV y las tarjetas inteligentes para acceder a los pisos del edificio.

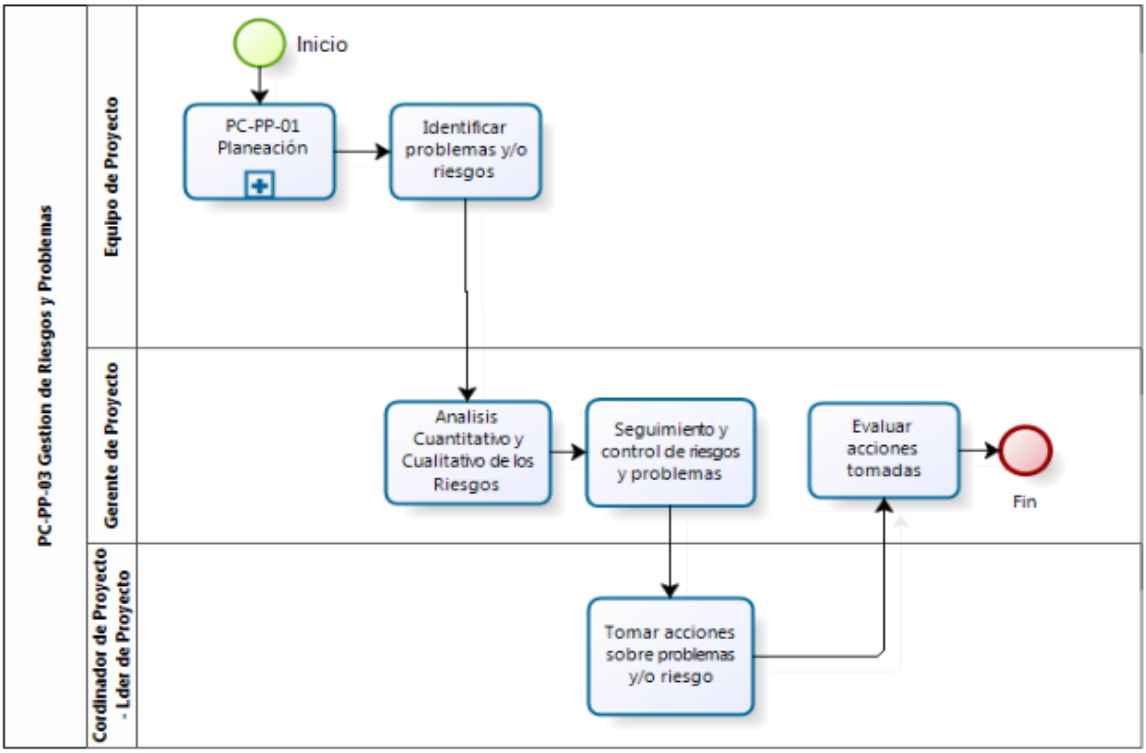
Existe un control de acceso para los visitantes el cual consta de acompañamiento del personal por la persona anfitriona, este registro se lleva en archivos físicos en la recepción del edificio y en la recepción de la empresa.

En cuanto al sistema de seguridad eléctrico y de incendios, el edificio cuenta con seguridad de altas de tensión, planta eléctrica y un sistema de extinción de incendios el cual se certifica cada año y se revisa con el cuerpo de bomberos de la localidad por lo menos dos veces al año.

Se puede decir que actualmente la seguridad de las operaciones en la fábrica de software se basa en el control, la supervisión y la confianza en los individuos más no en un estándar certificado.

10.2 PROCESO DE GESTION DE RIESGOS Y PROBLEMAS

Figura 4. Proceso Gestión de riesgos y problemas



Fuente: procesos IT Stefanini Colombia.

10.2.1 Objetivo

Mostrar las actividades necesarias para gestionar los problemas y riesgos en el proyecto, relacionadas con la identificación, seguimiento y despliegue de planes para su solución o mitigación.

10.2.2 Alcance

Estas actividades son aplicables en los proyectos de software que maneja la organización.

10.2.3 Descripción del proceso:

El proceso de gestión de riesgos es un subproceso del proceso de planificación, y tiene que ver con la identificación de los riesgos inherentes al proyecto los cuales pueden ser visualizados por cualquier integrante del equipo de proyecto.

El segundo paso se relaciona con la identificación propiamente de dichos riesgos, para ello se acude a diferentes metodologías como entrevistas, observación directa, lluvias de ideas o sugerencias del cliente.

El tercer paso se relaciona con el análisis de los riesgos identificados para lo cual el gerente de proyecto aplica técnicas cualitativas y cuantitativas.

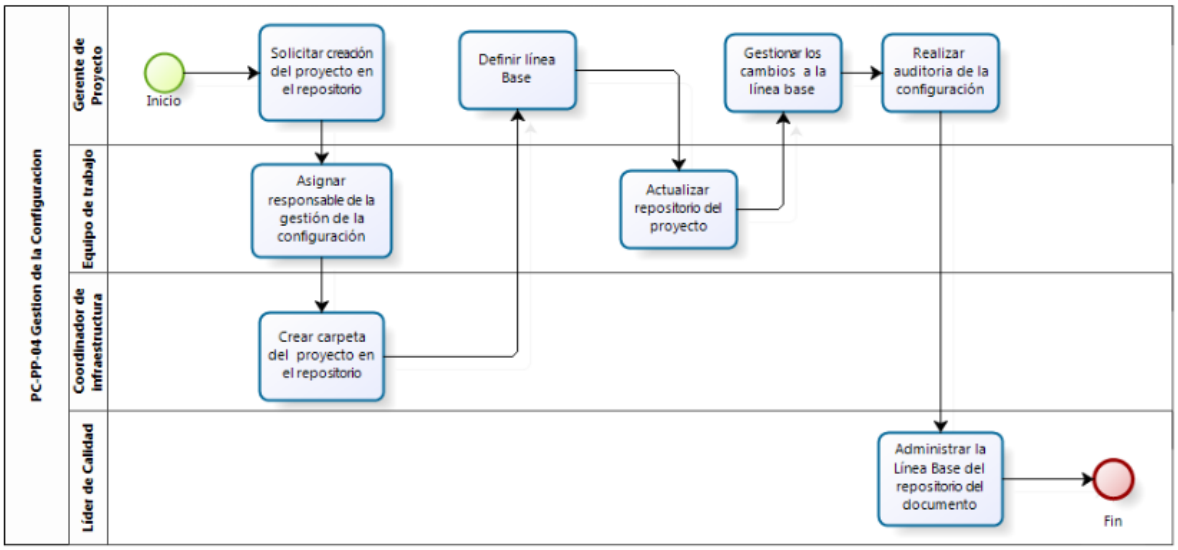
El cuarto paso se relaciona con el seguimiento y mitigación o control de los riesgos identificados y calificados con una importancia mayor, esta actividad la desarrolla el gerente de proyectos.

El quinto paso se relaciona con la toma de decisiones respecto a los riegos detectados, esta actividad es desarrollada por el gerente de proyectos y el gerente de la fábrica de software.

Por último, se evalúan por parte del gerente del proyecto las acciones tomadas y se concluye si se aceptan, transfieren o mitigan los riesgos.

10.3 PROCESO DE GESTION DE LA CONFIGURACION

Figura 5. Proceso de gestión de la configuración.



Fuente: procesos IT Stefanini Colombia.

10.3.1 Objetivo

Establecer la metodología para la gestión de los documentos, carpetas y líneas base en los proyectos de la organización.

10.3.2 Alcance

Para todos los contratos u órdenes de trabajo desarrollados por I&T STEFANINI definidos como proyectos de desarrollo de software.

10.3.3 Descripción del proceso:

El proceso de gestión de la configuración es un subproceso del proceso de planeación, en él se describen las actividades concernientes a la configuración de ambientes y entornos de trabajo.

Los tres primeros pasos se relacionan precisamente con la creación de los repositorios, la asignación del responsable de la gestión de la configuración y la creación de la unidad del proyecto en el repositorio.

El cuarto paso se relaciona con la definición de las líneas base a partir de las cuales se realizarán los desarrollos, esta actividad es realizad por el gerente del proyecto.

Los pasos cinco y seis se relacionan con la actualización del repositorio de documentos con las líneas bases y la gestión de los cambios a las mismas, esta actividad es realizada por el gerente de proyecto y el equipo de trabajo.

El paso siete se relaciona con la auditoria que realiza el gerente de proyecto a la gestión de las líneas base y su documentación adecuada.

Por último, el responsable de QA es quien administra la línea base en el repositorio del documento.

10.4 ESTRUCTURA ORGANICA DEL AREA DESARROLLO DE SOFTWARE

La estructura orgánica del área de desarrollo de software está compuesta normalmente por:

1 Gerente de Fábrica de Software.

2 Gerentes de proyectos.

X. Líderes técnicos por cada lenguaje de programación o herramienta.

X. Equipo de desarrolladores, que varía de 4 a 6 por cada fábrica continua o proyecto.

X. Líderes funcionales, 1 por cada fabrica continua o proyecto.

X. Ingenieros de requerimientos, 2 por cada fábrica continúa o proyecto.

X. Analistas de soporte post Implementación, 1 por cada fabrica continua o proyecto.

X. Analistas de QA, 2 por cada fábrica continúa o proyecto.

Cuando se utiliza la variable “X” se hace para indicar que precisamente es un número que cambia y está relacionado a la cantidad de fábricas o proyectos que en el momento se encuentren activos y la demanda de estos. Para el momento del desarrollo de este trabajo existen 7 fábricas de software y el cálculo de los recursos humanos a utilizar en cada proyecto, así como la distribución de tareas se maneja bajo la metodología SCRUM.

10.5 ÁREAS DE PROCESOS CMMI V 1.3 NIVEL 3 A EVALUAR Y EVALUACIÓN SCAMPI.

A pesar de que son 22 áreas de proceso en CMMI v 1.3 para los 5 niveles, se tienen en cuenta solamente las áreas de proceso hasta nivel 3 debido a que este es el nivel en el que actualmente se encuentra certificada la fábrica de software de IT Stefanini.

Para el nivel 3, se tienen en cuenta 18 áreas de proceso, las cuales contienen las:

SG = Metas Específicas

SP = Practicas Específicas.

GG = Metas Genéricas.

GP = Practicas Genéricas.

El nivel 1 considerado inicial no se tiene en cuenta ya que en este nivel no existe documentación, simplemente se trata como referencia para el inicio de las medidas de los indicadores de madurez y capacidad de la organización.

Se debe mencionar que la evaluación SCAMPI tipo C que será la utilizada en este proyecto solamente evalúa la existencia formal de las áreas de proceso y la aplicación de las metas y prácticas, esta evaluación prepara a la organización para la aplicación de una evaluación SCAMPI B o SCAMPI A que son realizadas por personal certificado por el Software Engineering Institute y para el caso de SCAMPI A, el personal debe estar autorizado para realizar la evaluación y certificación.

Se recuerda en este punto que a pesar de lo riguroso de la evaluación SCAMPI C, para CMMI L3 este proyecto pretende evaluar la seguridad de la información del proceso de desarrollo de software no su capacidad ni su madurez, por lo tanto, solo se incluye el apartado de evaluación y la matriz de CMMI como evidencia de la existencia de las áreas de proceso, cumplimiento de metas y prácticas específicas.

10.5.1 Áreas de proceso

Tabla 1. Áreas de ´proceso, metas y prácticas genéricas

Process Area	Level	Goals	Practices	Established
Configuration Management	A support process area at maturity level 2	SG 1. Establish baselines	S.P 1.1. Identify Configuration items.	1
			S.P 1.2. Establish a configuration management system.	1
			S.P 1.3. Create or release Baseline.	1
		SG 2. Track and control changes	S.P 2.1. Track change request.	1
			S.P 2.2. Control configuration Items.	1
		SG 3. Establish Integrity	S.P 3.1. Establish configuration management record.	1
			S.P 3.2. Perform configurations audit.	1
Measurement and analysis	A support process area at maturity level 2	SG 1. Align measurement and analysis activities	S.P 1.1. Establish measurement objective.	1
			S.P 1.2. Specify measures.	1
			S.P 1.3. Specify data collection and storage procedures.	1
			S.P 1.4. Specify analysis procedures.	1
		SG 2. Provide measurements results	S.P 2.1. Collect measurement data.	1
			S.P 2.2. Analyse measurement data.	1
			S.P 2.3. Store data and results.	1
			S.P 2.4. Communicate results.	1

Continúa…

Tabla 1. Áreas de ´proceso, metas y prácticas genéricas (Continuación)

Process Area	Level	Goals	Practices	Established
Project Monitoring and control	A project management process area at maturity level 2	SG 1 Monitor Project against Plan	SP 1.1 Monitor Project Planning Parameters	1
			SP 1.2 Monitor Commitments	1
			SP 1.3 Monitor Project Risks	1
			SP 1.4 Monitor Data Management	1
			SP 1.5 Monitor Stakeholder Involvement	1
			SP 1.6 Conduct Progress Reviews	1
			SP 1.7 Conduct Milestone Reviews	1
		SG 2 Manage Corrective Action to Closure	SP 2.1 Analyse Issues	1
			SP 2.2 Take Corrective Action	1
			SP 2.3 Manage Corrective Action	1
		SG 1 Establish Estimates	SP 1.1 Estimate the Scope of the Project	1
			SP 1.2 Establish Estimates of Work Product and Task Attributes	1
			SP 1.3 Define Project Life Cycle	1
			SP 1.4 Determine Estimates of Effort and Cost	1

Continúa…

Tabla 1. Áreas de ´proceso, metas y prácticas genéricas (Continuación)

Process Area	Level	Goals	Practices	Established
Project Planning	**A project management process area at maturity level 2**	SG 2 Develop a Project Plan	SP 2.1 Establish the Budget and Schedule	1
			SP 2.2 Identify Project Risks	1
			SP 2.3 Plan for Data Management	1
			SP 2.4 Plan for Project Resources	1
			SP 2.5 Plan for Needed Knowledge and Skills	1
			SP 2.6 Plan Stakeholder Involvement	1
			SP 2.7 Establish the Project Plan	1
		SG 3 Obtain Commitment to the Plan	SP 3.1 Review Plans that Affect the Project	1
			SP 3.2 Reconcile Work and Resource Levels	1
			SP 3.3 Obtain Plan Commitment	1
Process and product quality assurance	**A support process area at maturity level 2**	SG 1 Objectively Evaluate Processes and Work Products	SP 1.1 Objectively Evaluate Processes	1
			SP 1.2 Objectively Evaluate Work Products and Services	1
		SG 2 Provide Objective Insight	SP 2.1 Communicate and Ensure Resolution of Noncompliance Issues	1
			SP 2.2 Establish Records	1

Continúa…

Tabla 1. Áreas de ´proceso, metas y prácticas genéricas (Continuación)

Process Area	Level	Goals	Practices	Established
Requirements Management	**An Engineering process area at Maturity Level 2**	SG 1 Manage Requirements	SP 1.1 Obtain an Understanding of Requirements	1
			SP 1.2 Obtain Commitment to Requirements	1
			SP 1.3 Manage Requirements Changes	1
			SP 1.4 Maintain Bidirectional Traceability of Requirements	1
			SP 1.5 Identify Inconsistencies between Project Work and Requirements	1
Supplier Agreement Management	**A project management process area at maturity level 2**	SG 1 Establish Supplier Agreements	SP 1.1 Determine Acquisition Type	1
			SP 1.2 Select Suppliers	1
			SP 1.3 Establish Supplier Agreements	1
		SG 2 Satisfy Supplier Agreements	SP 2.1 Execute the Supplier Agreement	1
			SP 2.2 Monitor Selected Supplier Processes	1
			SP 2.3 Evaluate Selected Supplier Work Products	1
			SP 2.4 Accept the Acquired Product	1
			SP 2.5 Transition Products	1

Continúa…

Tabla 1. Áreas de ´proceso, metas y prácticas genéricas (Continuación)

Process Area	Level	Goals	Practices	Established
Decision Analysis and Resolution	A support process area at maturity level 3	SG 1. Evaluate Alternatives	S.P 1.1. Establish Guidelines for decision analysis.	1
			S.P 1.2. Establish evaluation criteria.	1
			S.P 1.3. Identify alternative solutions.	1
			S.P 1.4. Select evaluation methods.	1
			S.P 1.5. Evaluate alternatives	1
			S.P 1.6. Select solutions.	1
Integrated project management + IPPD	A project management process area at maturity level 3	SG 1 Use the projects defined process	S.P 1.1. Establish the project defined process.	1
			S.P 1.2. Use Organizational process assets for planning process activities.	1
			S.P 1.3. Establish the project Works environments.	1
			S.P 1.4. Integrate Plans.	1
			S.P 1.5. Manage the project using the integrated plans	1
			S.P 1.6. Contribute to the organizational process assets.	1
		SG 2 Coordinate and collaborate with relevant stakeholders	S.P 2.1. Manage Stakeholders involvement.	1
			S.P 2.2. Manage Dependencies.	1
			S.P 2.3. Resolve coordination Issues.	1

Continúa…

Tabla 1. Áreas de ´proceso, metas y prácticas genéricas (Continuación)

Process Area	Level	Goals	Practices	Established
		SG 3. Apply IPPD Principles IPPD Addition	S.P 3.1. Establish the project shared vision.	1
			S.P 3.2. Establish the integrated team structure.	1
			S.P 3.3. Allocate requirements to integrated teams.	1
			S.P 3.4. Establish integrated teams.	1
			S.P 3.5. Ensure collaboration among interfacing teams.	1
Organizational process focus	**A process management process area at maturity level 3**	SG 1 Determine Process Improvement Opportunities	SP 1.1 Establish Organizational Process Needs	1
			SP 1.2 Appraise the Organization's Processes	1
			SP 1.3 Identify the Organization's Process Improvements	1
		SG 2 Plan and Implement Process Improvement Activities	SP 2.1 Establish Process Action Plans	1
			SP 2.2 Implement Process Action Plans	1
		SG 3 Deploy Organizational Process Assets and Incorporate Lessons Learned	SP 3.1 Deploy Organizational Process Assets	1
			SP 3.2 Deploy Standard Processes	1
			SP 3.3 Monitor Implementation	1
			SP 3.4 Incorporate Process-Related Experiences into the Organizational Process Assets	1

Continúa…

Tabla 1. Áreas de ´proceso, metas y prácticas genéricas (Continuación)

Process Area	Level	Goals	Practices	Established
Organizational Training	**A process management process area at maturity level 3**	SG 1 Establish an Organizational Training Capability	SP 1.1 Establish the Strategic Training Needs	1
			SP 1.2 Determine Which Training Needs Are the Responsibility of the Organization	1
			SP 1.3 Establish an Organizational Training Tactical Plan	1
			SP 1.4 Establish Training Capability	1
		SG 2 Provide Necessary Training	SP 2.1 Deliver Training	1
			SP 2.2 Establish Training Records	1
			SP 2.3 Assess Training Effectiveness	1
Product integration	**An Engineering process area at maturity level 3**	SG 1 Prepare for Product Integration	SP 1.1 Determine Integration Sequence	1
			SP 1.2 Establish the Product Integration Environment	1
			SP 1.3 Establish Product Integration Procedures and Criteria	1
		SG 2 Ensure Interface Compatibility	SP 2.1 Review Interface Descriptions for Completeness	1
			SP 2.2 Manage Interfaces	1
		SG 3 Assemble Product Components and Deliver the Product	SP 3.1 Confirm Readiness of Product Components for Integration	1
			SP 3.2 Assemble Product Components	1
			SP 3.3 Evaluate Assembled Product Components	1
			SP 3.4 Package and Deliver the Product or Product Component	1

Continúa…

Tabla 1. Áreas de ´proceso, metas y prácticas genéricas (Continuación)

Process Area	Level	Goals	Practices	Established
Requirements Development	An Engineering process area at maturity level 3	SG 1 Develop Customer Requirements	SP 1.1 Elicit Needs	1
			SP 1.2 Develop the Customer Requirements	1
			SG 2 Develop Product Requirements	1
		SP 2.1 Establish Product and Product-Component Requirements	SP 2.2 Allocate Product-Component Requirements	1
			SP 2.3 Identify Interface Requirements	1
		SG 3 Analyse and Validate Requirements	SP 3.1 Establish Operational Concepts and Scenarios	1
			SP 3.2 Establish a Definition of Required Functionality	1
			SP 3.3 Analyse Requirements	1
			SP 3.4 Analyse Requirements to Achieve Balance	1
			SP 3.5 Validate Requirements	1
Risk Management	A project management process area at maturity level 3	SG 1 Prepare for Risk Management	SP 1.1 Determine Risk Sources and Categories	1
			SP 1.2 Define Risk Parameters	1
			SP 1.3 Establish a Risk Management Strategy	1
		SG 2 Identify and Analyse Risks	SP 2.1 Identify Risks	1
			SP 2.2 Evaluate, Categorize, and Prioritize Risks	1

Continúa…

Tabla 1. Áreas de ´proceso, metas y prácticas genéricas (Continuación)

Process Area	Level	Goals	Practices	Established
		SG 3 Mitigate Risks	SP 3.1 Develop Risk Mitigation Plans	1
			SP 3.2 Implement Risk Mitigation Plans	1
Technical Solution	An Engineering process area at maturity level 3	SG 1 Select Product-Component Solutions	SP 1.1 Develop Alternative Solutions and Selection Criteria	1
			SP 1.2 Select Product Component Solutions	1
		SG 2 Develop the Design	SP 2.1 Design the Product or Product Component	1
			SP 2.2 Establish a Technical Data Package	1
			SP 2.3 Design Interfaces Using Criteria	1
			SP 2.4 Perform Make, Buy, or Reuse Analysis	1
		SG 3 Implement the Product Design	SP 3.1 Implement the Design	1
			SP 3.2 Develop Product Support Documentation	1
Validation	An Engineering process area at maturity level 3	SG 1 Prepare for Validation	SP 1.1 Select Products for Validation	1
			SP 1.2 Establish the Validation Environment	1
			SP 1.3 Establish Validation Procedures and Criteria	1
		SG 2 Validate Product or Product Components	SP 2.1 Perform Validation	1
			SP 2.2 Analyse Validation Results.	1

Continúa…

Tabla 1. Áreas de ´proceso, metas y prácticas genéricas (Continuación)

Process Area	Level	Goals	Practices	Established
Verification	An Engineering process area at maturity level 3	SG 1 Prepare for Verification	SP 1.1 Select Work Products for Verification	1
			SP 1.2 Establish the Verification Environment	1
			SP 1.3 Establish Verification Procedures and Criteria	1
		SG 2 Perform Peer Reviews	SP 2.1 Prepare for Peer Reviews	1
			SP 2.2 Conduct Peer Reviews	1
			SP 2.3 Analyse Peer Review Data	1
		SG 3 Verify Selected Work Products	SP 3.1 Perform Verification	1
			SP 3.2 Analyse Verification Results	1
Organizational process definition +PDD	A process management process area at maturity level 3	SG 1 Establish Organizational Process assets.	S.P 1.1. Establish standard process.	1
			S.P 1.2. Establish life cycle model description.	1
			S.P 1.3. Establish tailoring criteria and guidelines.	1
			S.P 1.4. Establish the organization measurement repository.	1
			S.P 1.5. Establish the organizational process asset library.	1
		SG 2 Enable IPPD Management	S.P 2.1. Establish empowerment mechanisms.	1
			S.P 2.2. Establish rules and guidelines for integrated teams.	1
			S.P 2.3. Balance team and home organization responsibilities.	1

Fuente: El Autor

En el Anexo A. Se podrá encontrar la evaluación SCAMPI C del proceso de desarrollo de software evidenciando el cumplimiento del nivel 3 de CMMI v 1.3.

11. AUDITORIA AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO DE DESARROLLO DE SOFTWARE EN IT STEFANINI COLOMBIA RESPECTO A LA NTC ISO/IEC 27001:2013.

La norma NTC ISO/IEC 27001:2013 contiene los requisitos aplicables a un sistema de gestión de seguridad de la información para poder ser objeto de certificación.

Debido al alcance de este proyecto se busca únicamente auditar el proceso de desarrollo de software de IT Stefanini Colombia, sin embargo, estas mismas normas y procedimientos pueden ser aplicados transversalmente a la organización para lograr la certificación de todas sus áreas.

También puede ser aplicado a cualquier empresa de desarrollo de software con el objetivo de lograr que su sistema de gestión de seguridad de la información cumpla los requisitos de certificación de la norma.

A continuación, se revisa la documentación de auditoria generada para este trabajo lo que permitirá generar las conclusiones del informe final de auditoria que será entregado a la dirección de la organización.

11.1 EL PROGRAMA DE AUDITORÍAS

El programa de auditorías es un documento del área de control interno y auditoría en una organización en el cual se describe las fechas, en las cuales se realizarán auditorias y respecto a que normas o requisitos se auditara, en él se definen el objetivo y los alcances de las auditorías a realizar.

Es común que en las organizaciones se diseñe un programa de auditorías anual en el cual se pueden planificar las actividades sobre un calendario o programador.

El programa de auditorías puede incluir auditorías que tengan una o más normas de gestión en diferentes frentes, calidad, seguridad de la información, gestión de riesgos, gestión ambiental, gestión humana, etc.

El alcance deberá cubrir el tamaño de la organización, establecer prioridades como por ejemplo requisitos legales, y además tener en cuenta su naturaleza, así como la complejidad y madurez de los sistemas de gestión existentes.

Por medio de cada programa de auditoría, el auditor adquiere control sobre el desarrollo del examen, pues estos además de ser una guía para los asistentes sirven para efectuar una adecuada supervisión sobre los mismos, permitiendo también determinar el tiempo real de ejecución de cada procedimiento para compararlo con el estimado y así servir de pauta para la planeación de las próximas auditorías, así mismo, permite conocer en cualquier momento el estado de adelanto del trabajo, ayudando a la toma de decisiones sobre la labor pendiente por realizar.[3]

En el Anexo B se puede encontrar el programa de auditorías utilizado para este proyecto.

11.2 EL CRONOGRAMA DE AUDITORIA

El cronograma de auditoria es un documento del área de control interno y auditoria en una organización, en el cronograma se describen de forma precisa los procedimientos a auditar con fecha, hora y lugar donde se realizará la auditoria, menciona los auditados y el auditor que realizará la auditoria.

Comúnmente es confundido con el programa, sin embargo, como se verá en los anexos tienen características, objetivos y alcances diferentes y su creación siempre dependerá de la metodología y documentación generada para la auditoria por el auditor líder.

En el Anexo C se puede encontrar el cronograma de auditorías utilizado para este proyecto.

11.3 EL PLAN DE AUDITORÍA

El plan de auditoría es un documento del área de control interno y auditoría en una organización, en el plan de auditoria se especifica el proceso auditado, objetivo y alcance de la auditoria, criterios que se tendrán en cuenta en la auditoria, el método incluyendo el grado de muestreo requerido para obtener la suficiente evidencia de auditoria, expone que otra información puede ser necesaria para la realización de la auditoría identificando cualquier otra documentación que previamente deba estar a disposición del equipo auditor, se identifica el equipo auditor y los auditados así como se establece un registro de las actividades de la auditoria, es un documento que se diligencia en el inicio y curso de la auditoria con los eventos que se presentan y debe estar acordado y aprobado entre las partes involucradas.

En el Anexo D se puede encontrar el plan de auditoría utilizado para este proyecto.

[3] http://fccea.unicauca.edu.co/old/tgarf/tgarfse67.html

11.4 LISTADOS DE AUDITORÍA.

Hacen parte de la documentación del área de control interno y auditoría de la organización, sin embargo, para cada auditoría las listas de auditoria o check list se cambian y deben ser nuevamente diseñadas por el auditor líder, se pueden definir como herramientas para la ejecución controlada de la auditoria, para el registro de hallazgos y conclusiones de la misma, se recomienda la creación de una lista de auditoria por cada proceso auditado, sin embargo, es criterio del auditor que tan amplio y que alcance tiene cada listado; aunque existe la recomendación general de no pasar de 20 preguntas o controles por cada listado para evitar saturar al auditado y crear entropía que dificulte la extensión de las actividades de la auditoria la cual puede cambiar como resultado de la información recopilada durante la misma auditoria.

También se debe tener en cuenta que los listados se realizan después de estar creado el plan y el cronograma de la auditoria cuando se tiene definido el objetivo y alcance de la misma.

Si se realizan preguntas estas deben apuntar a la verificación del cumplimiento de un requisito, sin embargo, para algunos casos se puede especificar el control a ser evaluado y de esta manera dar claridad al concepto.

La lista puede ser utilizada para realizar una autoevaluación por parte de los funcionarios de auditoria interna, o puede ser revisada previa evaluación de un ente externo, las listas de auditoria no pretenden abarcar todas las situaciones, es necesario que el auditor o el equipo evaluador realicen su análisis previo y determinen las mejores prácticas[4].

En el Anexo E se encuentran los listados de controles y su evaluación para este proyecto.

11.5 HOJA DE HALLAZGOS DE AUDITORIA.

La hoja de hallazgos de auditoria es un documento del área de control interno y auditoría en una organización, en ella se especifican los hallazgos encontrados detallando sus atributos, es un soporte vital a la hora de realizar las conclusiones y recomendaciones en el informe final de auditoria por lo que es un paso previo a la realización del informe final de auditoria.

[4] http://www.auditool.org/auditoria-interna/25-markets/505-lista-de-chequeo-de-mejores-practicas-en-la-funcion-de-auditoria-interna

Con la hoja de hallazgos se puede profundizar más en los puntos que se describen en la misma, catalogándolos como no conformidades u opciones de mejora y entregando una predefinición del análisis que llevaría a la acción preventiva o correctiva si estas también se tienen catalogadas previamente.

Se debe anotar en este punto que el auditor no es quien establece la acción correctiva o preventiva, esta es una tarea del dueño del proceso o dominio auditado, sin embargo, posterior a la auditoria y a la entrega del informe el auditor encargado o el área de control interno puede hacer el seguimiento de las acciones implementadas para mitigar una no conformidad con esta herramienta.

En el Anexo F se puede encontrar el formato de hoja de hallazgos que se utiliza en este proyecto.

11.6 INFORME FINAL DE AUDITORIA.

El informe final de auditoria es el documento final y objeto de la actividad de auditoria, en él se debe reflejar el estado de la organización respecto a los criterios de auditoria definidos al inicio de la auditoria.

También se deben detallar las recomendaciones y conclusiones del equipo auditor y en el caso de la auditoria interna se establecen los plazos para el levantamiento de las no conformidades encontradas.

Debido a que este documento está dirigido a los directivos de la organización y gerentes de procesos no debe ser muy técnico por lo que en general se recomienda la presentación del mismo en diapositivas con gráficos dinámicos, tablas y cuadros que concluyan los datos encontrados en el reporte.

Por otra parte, y como soporte de este informe en presentaciones se debe dejar documentado de manera técnica el desarrollo de la auditoria, para esto se puede usar la hoja de hallazgos y el reporte final de cumplimiento de la auditoria que puede presentarse en texto u hoja de cálculo.

En el Anexo G se puede encontrar el formato de informe final técnico que se utiliza en este proyecto.

12. EJECUCIÓN DE LA AUDITORIA

12.1 Fase 1 Revisión Documental

12.1.1 Política de Seguridad de la Información

En IT Stefanini existe previamente un documento denominado política de seguridad de la información en el cual se exponen las normas y artículos que rigen los comportamientos frente a la manipulación y gestión de documentación y aplicaciones en la organización.

- Generalidades

El avance tecnológico ha permitido a las organizaciones tener más y mejores maneras de interconectarse, esto ha permitido un mayor aprovechamiento de los recursos de todo tipo al tiempo que ha aumentado el alcance de los negocios convirtiéndose en una gran ventaja competitiva.

Sin embargo, algunos riesgos que se enfrentan han llevado a unas directrices que orientan en el uso adecuado de estas destrezas tecnológicas y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de Informática y Tecnología Stefanini S.A

La finalidad de la política de seguridad de la información en I&T Stefanini es generar conciencia sobre la importancia de los activos informáticos y de información que permiten a la empresa crecer y mantenerse en el mercado.

- Alcance

La política se seguridad de la información se estructura de acuerdo al análisis de riesgos y vulnerabilidades en las actividades de negocio desarrolladas por Informática y Tecnología Stefanini, por consiguiente, su alcance se extiende a toda la organización.

- Detalle

ISO 27001:2013 establece que un Sistema de Gestión de Seguridad de la Información se ocupa de garantizar la integridad física de los activos informáticos y de la información. Para ello se vale del ciclo PHVA, el cual significa “planear” la seguridad de la información observando los puntos débiles y fortalezas de los activos de la organización, “hacer” tomar las medidas necesarias para proteger los activos identificados, “verificar” cerciorarse de que las medidas tomadas sirven para proteger los activos y que se están cumpliendo no solo para los activos sino

para los recursos, para ello se establecen métricas y evaluaciones que permiten conocer el estado de la seguridad de la información y de los activos informáticos en un momento dado, y “Actuar” que se refiere a que cuando se detecta que no se está cumpliendo alguna medida, contramedida o control sobre los activos y recursos o que por la evolución las medidas tomadas ya no son suficientes, se tomen nuevas medidas que permitan garantizar la seguridad de la información y los activos informáticos, entre ellos los recursos, en este punto el ciclo vuelve a iniciar ejecutando y evaluando nuevamente cada fase de PHVA.

Los objetivos en el sistema de gestión de seguridad de la información en I&T stefanini son:

- Implementar un esquema de seguridad de la información y los activos informáticos, que sea transparente para las partes interesadas y este bajo la responsabilidad de la alta dirección quien es la encargada de las decisiones sobre la evaluación del riesgo.
- Comunicar al personal de la organización los controles y decisiones de la dirección para minimizar los riesgos generando conciencia para la aplicación de los mismos con dinamismo, armonía y calidad.

Análisis de razones que impiden la correcta aplicación de la política de seguridad de la información

El día a día en las organizaciones exige un fuerte compromiso de las áreas de IT, este compromiso se dificulta ya que a diario la tecnología evoluciona exigiendo al tiempo la evolución de los negocios y en ocasiones el afán de cumplir un indicador, una meta o un compromiso provoca brechas de seguridad que posteriormente no son atendidas y se dejan acumular haciendo vulnerable una infraestructura tecnológica y la información que sobre ella se transporta.

Las organizaciones no son conscientes de estas vulnerabilidades hasta que son expuestas al público muchas veces acarreando un daño reputacional o financiero muy alto.

La existencia de una política de seguridad de la información no constituye en sí misma una garantía o seguridad de que la información y la infraestructura que soporta se encuentran a salvo, la política es un compendio de direcciones y controles de seguridad emanados de la alta dirección, sin embargo, para garantizar su efectividad debe tener un seguimiento y evaluación constante por la misma dirección o las estructuras organizativas que se deleguen y adaptar en cada momento esta política a las nuevas necesidades de negocios y entorno regulatorio existente.

- Disposiciones Generales acerca de la Información

La información de I&T STEFANINI se clasifica como pública, privada o confidencial, esta clasificación se encuentra contempladas en LI-RD-08 Responsables y Autoridades

- **Clasificación de la información**

Información Pública: esta información tiene las siguientes características y recomendaciones:

Acceso permitido a: todos los empleados de la organización, contratistas por prestación de servicios, clientes.

Distribución a través de: Correo electrónico corporativo, página web, red de datos de I&T STEFANINI o carpetas compartidas y/o servidor de archivos que solicite previamente la identificación de usuario y password.

Distribución por fuera de I&T STEFANINI: Correo electrónico dirigido a cuentas corporativas.

Restricciones para la distribución electrónica: las contenidas en la guía para el buen uso del correo electrónico que se encuentra publicado en el boletín.

Almacenamiento y archivado: El almacenamiento y archivado de la información debe realizarse según lo indica el LI-DC-01 Maestro de Documentos y Registros.

Información Privada: Dentro de esta información se encuentra todos los documentos relacionados con proyectos, la información financiera, información de recursos humanos. Esta información tiene las siguientes características y recomendaciones:

Distribución a través de: Correo electrónico corporativo, red de datos de I&T STEFANINI, carpetas compartidas y/o servidor de archivos que solicite previamente la identificación de usuario y password.

Distribución por fuera de I&T STEFANINI: Correo electrónico dirigido a cuentas corporativas.

Restricciones para la distribución electrónica: las contenidas en la guía para el buen uso del correo electrónico que se encuentra publicado en el boletín.

Almacenamiento y archivado: El almacenamiento y archivado de la información debe realizarse según lo indica el LI-DC-01 Maestro de Documentos y Registros.

Información Confidencial: Este tipo de información no debe ser conocida por terceros que pertenezcan o no al área y/o proyectos si así no lo determina la Gerencia de I&T STEFANINI.

Acceso permitido a: Solo las personas que autorice la Gerencia

Distribución a través de: No se permite la distribución de esta información de manera electrónica, todo manejo se realizará a través del servidor de archivos previa autenticación con usuario y password de red.

Distribución por fuera de I&T STEFANINI: No se permite la distribución de esta información fuera de las instalaciones de I&T STEFANINI.

Almacenamiento y archivado: El almacenamiento y archivado de la información debe realizarse según lo indica el LI-DC-01 Maestro de Documentos y Registros.

Lineamientos y Artículos

79 Artículos catalogados como confidenciales.

12.1.2 Plan de Continuidad

Catalogado como confidencial.

12.2 FASE 2 AUDITORIA DE CAMPO

12.2.1 Programa de Auditoria

Fig. 6 cronogramas de auditoria

Calendario Annual de Auditorias

Norma ISO 27001: 2013	27k
Norma ISO 9001:2008	9k
CMMI Apraisal	CM

Objetivo:	Verificar el cumplimiento de los requisitos de la norma enunciada ssegun la auditoria programada.
Alcance:	Horizontal transversal a toda la organizacion para ISO 9001:2008, Vertical Fabrica de Software Para ISO 27001:2013 y CMMI

CRONOGRAMA ANUAL DE AUDITORIAS

	Enero				Febrero				Marzo				Abril				Mayo				Junio				Julio				Agosto				Septiembre				Octubre				Noviembre				Diciembre			
	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4
Lunes															27k	27k					9k	9k	9k								CM	CM							9k	9k	9k					
Martes															27k	27k					9k	9k	9k								CM	CM							9k	9k	9k					
Miercoles															27k	27k					9k	9k	9k								CM	CM							9k	9k	9k					
Jueves															27k	27k					9k	9k	9k								CM	CM							9k	9k	9k					
Viernes															27k	27k					9k	9k	9k								CM	CM							9k	9k	9k					

Fuente: I&T Stefanini.

12.2.2 Plan de Auditoria

Figura 7. Plan de auditoria

PLAN DE AUDITORIA				
Fecha	11/03/2016	No. Auditoria	1	
Proceso Auditado		Desarrollo de Software		
Objetivo de Auditoria		Establecer el estado actual del SGSI en el proceso de desarrollo de software		
Alcance de auditoria		Evaluacion de la seguridad de la informacion en todos los subprocesos del proceso de desarrollo de software y fabricas continuas.		
Criterios de Auditoria		Norma NTC ISO-IEC 27001:2013. Areas de proceso CMMI V 1.3.		
Personal Auditado		Gerente Fabrica de Software. Gerente de Infraestructura. Gerente de RRHH. Coordinador de Fabrica de software.		
Equipo Auditor		Auditor Lider. Auditor Interno: Ing. Javier Olivo Garcia A.		
Hora	Actividad	Auditor	Auditado	Requisitos
08:00	Reunion del personal auditor	Auditor Lider. Auditor Interno. Gerente de Calidad y Operaciones		Documentacion del proceso de auditoria, cronogramas y listados de auditoria.
09:00	Reunion de apertura de la auditoria	Auditor Lider. Auditor Interno. Gerente de Calidad y Operaciones	Gerente Fabrica de Software. Gerente de Infraestructura. Gerente de RRHH. Coordinador de Fabrica de software.	Presencia de lideres de los procesos implicados en la auditoria.

Continúa...

Fig. 7. Plan de auditoria (Continuación)

Hora	Actividad	Auditor	Auditado	Requisitos
10:00	verificacion de requisitos	Auditor Lider. Auditor Interno. Gerente de Calidad y Operaciones	Gerente Fabrica de Software. Gerente de Infraestructura. Gerente de RRHH. Coordinador de Fabrica de software.	Norma NTC ISO-IEC 27001:2013. Areas de proceso CMMI V 1.3
18-04-16 10:00 am	Inicio de la auditoria Seguridad de los recursos humanos	Javier Olivo Garcia A	Gerente de RRHH	Listados de auditoria. Cronograma de auditoria.
18-04-16 14:00	Revision de las politicas de seguridad de la organizacion.	Javier Olivo Garcia A	Gerente de Fabrica	Listados de auditoria. Cronograma de auditoria.
19-04-16 14:00	Aspectos Organizativos de la seguridad de la organizacion	Javier Olivo Garcia A	Gerente de Fabrica	Listados de auditoria. Cronograma de auditoria.
20-04-16 14:00	Procedimiento cifrado	Javier Olivo Garcia A	Gerente de Fabrica	Listados de auditoria. Cronograma de auditoria.
21-04-16 9:00	Procedimiento gestion de activos	Javier Olivo Garcia A	Coordinador de Fab	Listados de auditoria. Cronograma de auditoria.
21-04-16 14:00	Procedimiento gestion de accesos	Javier Olivo Garcia A	Gerente de Fabrica	Listados de auditoria. Cronograma de auditoria.
22-04-16 14:00	Procedimiento seguridad fisica y ambiental	Javier Olivo Garcia A	Gerente de Fabrica	Listados de auditoria. Cronograma de auditoria.
25-04-16 14:00	Procedimiento seguridad de las operaciones	Javier Olivo Garcia A	Gerente de Fabrica	Listados de auditoria. Cronograma de auditoria.
26-04-16 9:00	Aspectos de la seguridad de la Informacion en la gestion de la continuidad del negocio	Javier Olivo Garcia A	Gerente de Infraest	Listados de auditoria. Cronograma de auditoria.

Continúa...

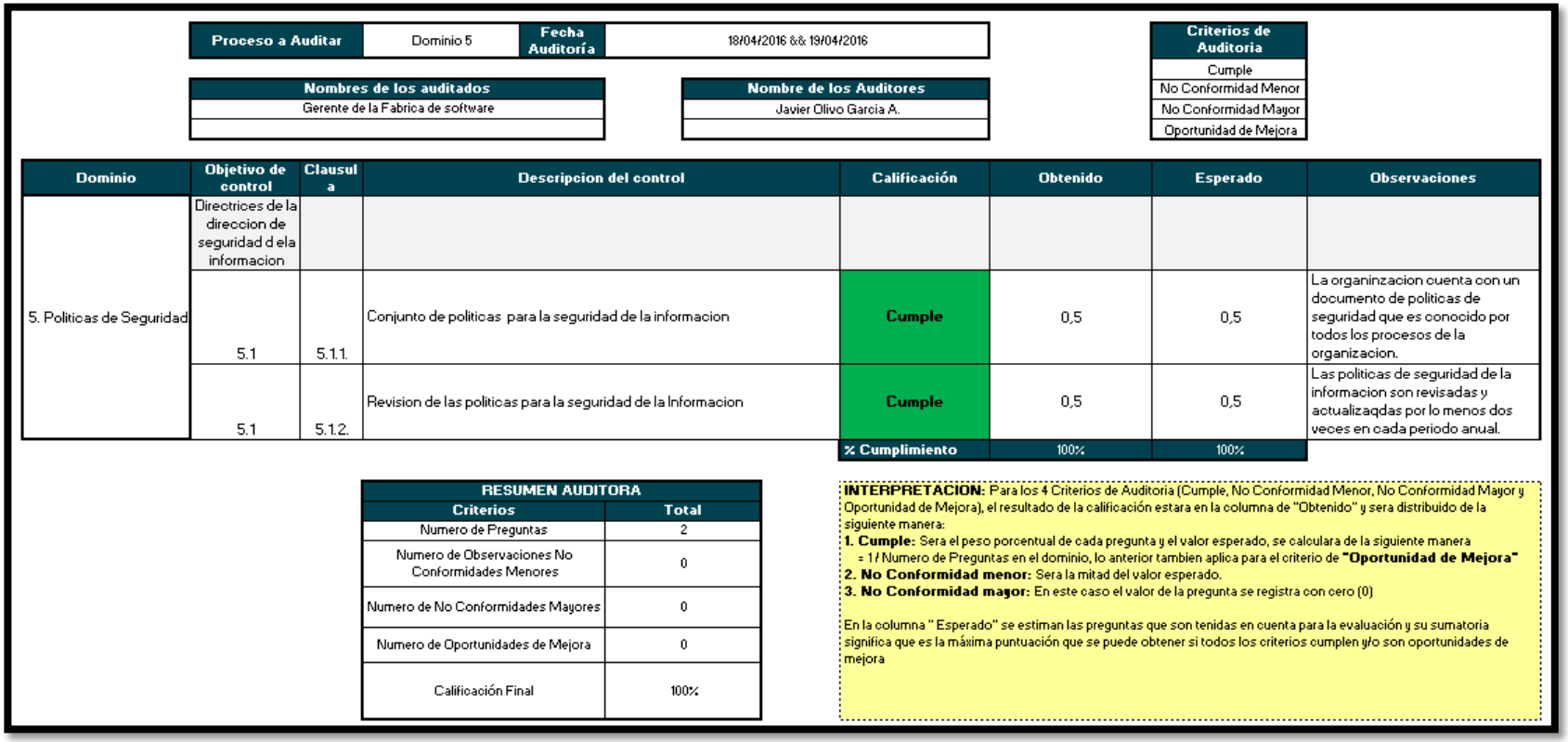
Fig 7. Plan de auditoria (Continuación)

Hora	Actividad	Auditor	Auditado	Requisitos
26-04-16 14:00	Procedimiento seguridad de las telecomunicaciones	Javier Olivo Garcia /	Gerente de Fabrica	Listados de auditoria. Cronograma de auditoria.
27-04-16 14:00	Adquisicion, desarrollo y mantenimiento de los sitemas de informacion	Javier Olivo Garcia /	Gerente de Fabrica	Listados de auditoria. Cronograma de auditoria.
28-04-16 09:00	Relacion con proveedores	Javier Olivo Garcia /	Coordinador de Fab	Listados de auditoria. Cronograma de auditoria.
29-04-16 09:00	Gestion de los incidentes de seguridad de la informacion	Javier Olivo Garcia /	ente de Infraestruct	Listados de auditoria. Cronograma de auditoria.
29-04-16 14:00	Cumplimiento	Javier Olivo Garcia /	Gerente de Fabrica	Listados de auditoria. Cronograma de auditoria.
2-05-16 9:00	Reunion de enlace de auditoria	Auditor Lider. Auditor Interno. Gerente de Calidad y Operaciones		Documentacion de auditoria
2-05-16 14:00	Cierre de auditoria	Auditor Lider. Auditor Interno. Gerente de Calidad y Operaciones	Gerente Fabrica de Software. Gerente de Infraestructura. Gerente de RRHH. Coordinador de Fabrica de software.	Presencia de lideres de los procesos implicados en la auditoria.

Fuente: I&T Stefanini.

12.2.3 Listados de auditoria

Fig. 8. Listados de auditoria, Dominio 5



Proceso a Auditar	Dominio 5	Fecha Auditoría	18/04/2016 && 19/04/2016

Nombres de los auditados
Gerente de la Fabrica de software

Nombre de los Auditores
Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
5. Politicas de Seguridad	Directrices de la direccion de seguridad d ela informacion						
	5.1	5.1.1.	Conjunto de politicas para la seguridad de la informacion	Cumple	0,5	0,5	La organinzacion cuenta con un documento de politicas de seguridad que es conocido por todos los procesos de la organizacion.
	5.1	5.1.2.	Revision de las politicas para la seguridad de la Informacion	Cumple	0,5	0,5	Las politicas de seguridad de la informacion son revisadas y actualizaqdas por lo menos dos veces en cada periodo anual.
				% Cumplimiento	100%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	2
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	100%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Fuente: I&T Stefanini

Fig 9. Listados de auditoria, Dominio 6

Proceso a Auditar	Dominio 6	Fecha Auditoria	18/04/2016 && 19/04/2016

Nombres de los auditados	Nombre de los Auditores
Gerente de la Fabrica de software	Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
6. Aspectos Organizativos de la seguridad de la informacion	Organizacion interna						
	6.1	6.1.1	Asignacion de responsabilidades para la seguridad de la informacion.	Oportunidad de Mejora	0,142857143	0,142857143	La responsabilidad sobre la seguridad de la informacion es delegada en el gerente de cada proyecto quien junto con el area de infraestructura y control interno monitorea el acceso y uso de la informacion segun los privilegios asignados
	6.1	6.1.2	Segregacion de tareas	Oportunidad de Mejora	0,142857143	0,142857143	Las tareas de seguridad de la informacion se asignan a los gerentes y coordinadores de cada proyecto, adicionalmente el area de infraestructura asigna y monitorea el acceso y uso de los recursos, y el area de control de operaciones ejerce vigilancia; no existe la figura de CIO o responsible de seguridad de la informacion en la organizacion a nivel Colombia
	6.1	6.1.3	Contacto con autoridades	Cumple	0,142857143	0,142857143	Existe un contacto directo con las autoridades del area metropolitana y nacional a nivel de recursos tecnologicos como son la SIJIN y DIJIN.
	6.1	6.1.4	Contacto con grupos de interes especial	Cumple	0,142857143	0,142857143	Existe contacto con algubnos grupos de profesionales y expertos en seguridad de la informacion, adicionalmente se hace parte de redes de conocimiento como Microsoft Defense Proyect, Symantec y Mcafee quienes son aliados estrategicos.
	6.1	6.1.5	Seguridad de la informacion en la gestion de proyectos.	No Conformidad Menor	0,071428571	0,142857143	Se pueden apreciar debilidades en los controles de seguridad de la informacion debido a que la gestion de la misma en cada proyecto solamente es realizada ocasionalmente por el gerente de proyecto quien se fundamenta que los controles de seguridad los ejerce de manera logica el area de infraestructura, no existe evidencia de los controles realizados de manera periodica o constante ya que muchas veces depende del cliente del proyecto
	Movilidad y teletrabajo						

Continúa…

Fig 9. Listados de auditoria, Dominio 6 (Continuación)

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
	6.2	6.2.1	Politica de seguridad para dispositivos moviles.	Cumple	0,142857143	0,142857143	Se evidencia la existencia de una politica de seguridad de la informacion para dispositivos moviles y su revision y actualizacion dos veces al año.
	6.2	6.2.2	Teletrabajo	Oportunidad de Mejora	0,142857143	0,142857143	Existe una politica de teletrabajo y trabajo flexible, sin embargo no se implementa ya que actualmemnte no se realiza teletrabajo en ningun proyecto.
				% Cumplimiento	93%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	7
Numero de Observaciones No Conformidades Menores	1
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	3
Calificación Final	93%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera
   = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen ylo son oportunidades de mejora

Fuente: I&T Stefanini

Fig 10. Listado de auditoria, Domino 7.

Proceso a Auditar	Dominio 7	Fecha Auditoria	18/04/2016 && 19/04/2016

Nombres de los auditados	Nombre de los Auditores
Gerente de la Fabrica de software	Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
7. Seguridad de los recursos humanos	Antes de la Contratacion						
	7.1	7.1.1	Investigacion de antecedentes antes de la contratacion.	Oportunidad de Mejora	0,166666667	0,166666667	En la organizacion existe un protocolo de reclutamiento y seleccion del personal, sin embargo solo se llevan a cabo estudios de seguridad cuando el proyecto del cliente asi lo requiere o cuando existe solicitud expresa del cliente.
	7.1	7.1.2	Terminos y condiciones de la contratacion	Cumple	0,166666667	0,166666667	Se evidencia la existencia de clausulas de restriccion y seguridad de la informacion en los contratos laborales del personal que representa la organizacion.
	Durante la contratacion						
	7.2	7.2.1	Responsabilidades de la gestion	Cumple	0,166666667	0,166666667	Se evidencia una division de responsabilidadesx en el proceso de contratacion de personal, asegurando la confirmacion de referencias, experiencias, formacion profesional y antecedentes de los aspirantes a cargos dentro de la organizacion.
	7.2	7.2.2	Concienciacion, educacion y capacitacion en la seguridad de la informacion.	No Conformidad Mayor	0	0,166666667	NO se evidencia la existencia de programas o campañas de promocion de la seguridad de la informacion en la organización
	7.2	7.2.3	Proceso disciplinario	Oportunidad de Mejora	0,166666667	0,166666667	Existe un area Juridica quien se encuentra alineada con el area de control de operaciones e infraestructura preparadis para tomar las acciones necesarias en caso de algun fraude o delito, sin embargo no se evidencian casos de acciones tomadas en ningun periodo.
	Terminacion o cambio de contratacion						

Continúa…

Fig 10 Listado de auditoria, Domino 7 (Continuación)

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
	7.3	7.3.1	Cese o cambio de puesto de trabajo	No Conformidad Menor	0,083333333	0,166666667	Existe un procedimiento de informe al area de infraestructura , sin embargo se evidencian periodos prolongados en la inactivacion de cuentas por retiros y el cambio de permisos y privilegios por movimientos de personal, este tiempo muerto se presenta por demoras en la notificacion de RRHH a Infraestructura.
				% Cumplimiento	75%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	6
Numero de Observaciones No Conformidades Menores	1
Numero de No Conformidades Mayores	1
Numero de Oportunidades de Mejora	2
Calificación Final	75%

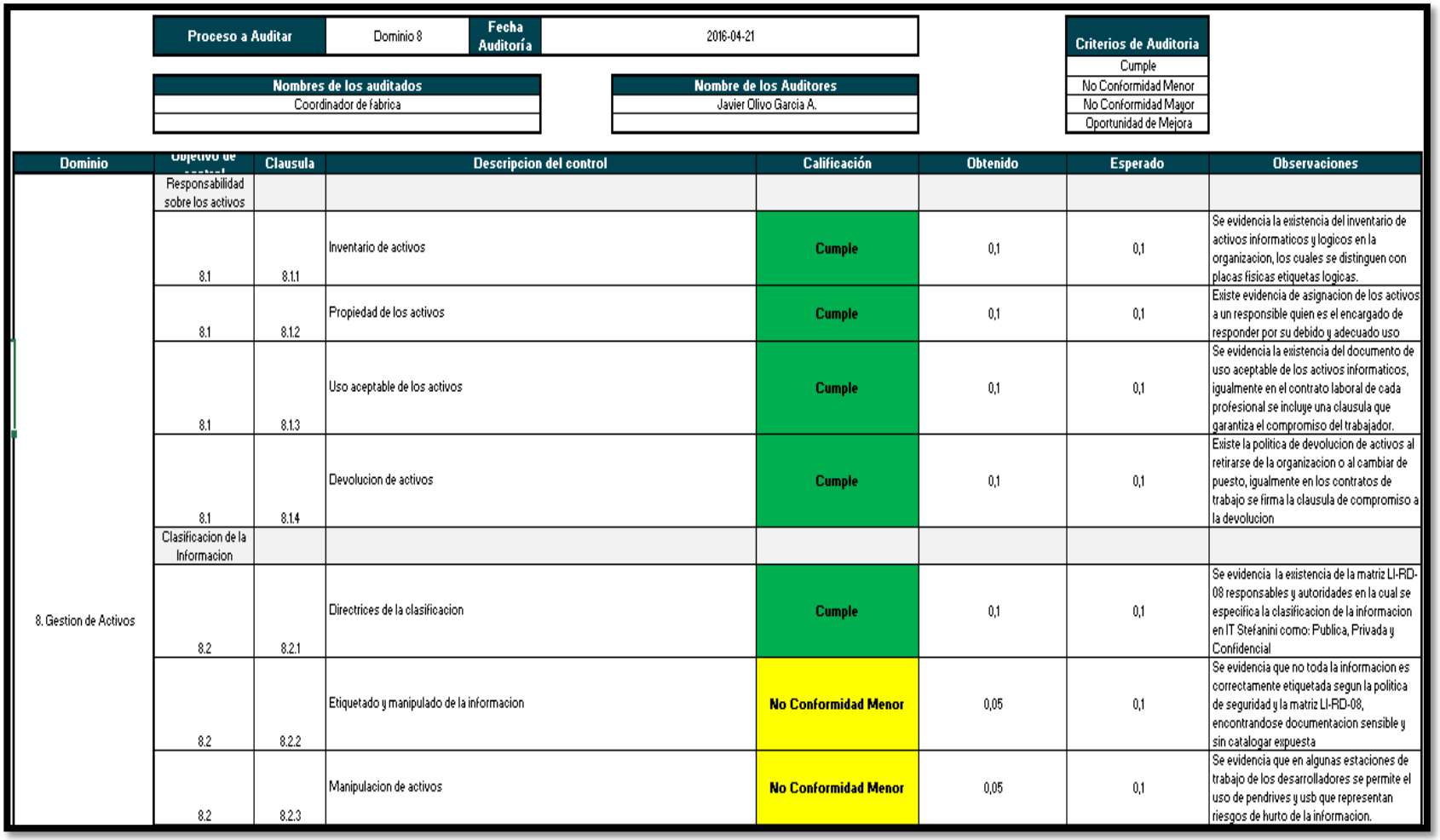
INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera
   = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Fuente: I&T Stefanini

Fig 11. Listado de Auditoria Dominio 8.



Proceso a Auditar	Dominio 8	Fecha Auditoría	2016-04-21

Nombres de los auditados	Nombre de los Auditores
Coordinador de fabrica	Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
8. Gestion de Activos	Responsabilidad sobre los activos						
	8.1	8.1.1	Inventario de activos	Cumple	0,1	0,1	Se evidencia la existencia del inventario de activos informaticos y logicos en la organizacion, los cuales se distinguen con placas fisicas etiquetas logicas.
	8.1	8.1.2	Propiedad de los activos	Cumple	0,1	0,1	Existe evidencia de asignacion de los activos a un responsible quien es el encargado de responder por su debido y adecuado uso
	8.1	8.1.3	Uso aceptable de los activos	Cumple	0,1	0,1	Se evidencia la existencia del documento de uso aceptable de los activos informaticos, igualmente en el contrato laboral de cada profesional se incluye una clausula que garantiza el compromiso del trabajador.
	8.1	8.1.4	Devolucion de activos	Cumple	0,1	0,1	Existe la politica de devolucion de activos al retirarse de la organizacion o al cambiar de puesto, igualmente en los contratos de trabajo se firma la clausula de compromiso a la devolucion
	Clasificacion de la Informacion						
	8.2	8.2.1	Directrices de la clasificacion	Cumple	0,1	0,1	Se evidencia la existencia de la matriz LI-RD-08 responsables y autoridades en la cual se especifica la clasificacion de la informacion en IT Stefanini como: Publica, Privada y Confidencial
	8.2	8.2.2	Etiquetado y manipulado de la informacion	No Conformidad Menor	0,05	0,1	Se evidencia que no toda la informacion es correctamente etiquetada segun la politica de seguridad y la matriz LI-RD-08, encontrandose documentacion sensible y sin catalogar expuesta
	8.2	8.2.3	Manipulacion de activos	No Conformidad Menor	0,05	0,1	Se evidencia que en algunas estaciones de trabajo de los desarrolladores se permite el uso de pendrives y usb que representan riesgos de hurto de la informacion.

Continúa…

Fig 11. Listado de Auditoria Dominio 8 (Continuación)

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
	Manejo de los soportes de almacenamiento						
	8.3	8.3.1	Gestion de los soportes extraibles	Cumple	0,1	0,1	Se evidencia la existencia de una politica de almacenamiento en medios extraibles identificada como IN-RF-99
	8.3	8.3.2	Eliminacion de soportes	No Conformidad Mayor	0	0,1	No se evidencia un procedimiento seguro de eliminacion de la informacion en soportes logicos.
	8.3	8.3.3	Soportes fisicos en transito	No Conformidad Mayor	0	0,1	No se evidencia un procedimeinto para el manejo seguro de los soportes fisicos hardware cuando son movilizados de mun area a otra.
				% Cumplimiento	70%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	10
Numero de Observaciones No Conformidades Menores	2
Numero de No Conformidades Mayores	2
Numero de Oportunidades de Mejora	0
Calificación Final	70%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera
   = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor**: Sera la mitad del valor esperado.
3. **No Conformidad mayor**: En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Fuente: I&T Stefanini

Fig 12. Listados de Auditoria, Dominio 9.

Proceso a Auditar	Dominio 9	Fecha Auditoría	20/04/2016 && 21/04/2016

Nombres de los auditados
Gerente de Fabrica
Gerente de Infraestructura

Nombre de los Auditores
Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
	Requisitos del negocio para el control de accesos						
	9.1	9.1.1	Politica de control de accesos	Cumple	0,071428571	0,071428571	Se evidencia la existencia de la politica de control de accesos la cual es gestionada por el area de infraestructura segun el LI-RD-08 matriz de responsables y autoridades donde se especifican accesos y aplicaciones para los usuarios.
	9.1	9.1.2	Control de acceso a las redes y servicios asociados	Cumple	0,071428571	0,071428571	Se evidencia la existencia de configuraciones seguras a nivel de directorio activo para los usuarios y en los access point que conectan las estaciones de trabajo a las redes de la organizacion, basandose en tecnologias Cisco y gestores de conexion instalados en la configuracion de las estaciones como check point security
	Gestion de acceso de usuario						
	9.2	9.2.1	Gestion de Altas y Bajas en el registro de usuarios	No Conformidad Menor	0,035714286	0,071428571	Se encuentra una politica clara para la gestion de altas y bajas de usuarios que se retiran de la organizacion y los traslados o movimientos de personal, sin embargo se puede evidenciar que los tiempos de respuesta para la baja y modificacion de los privilegios de un usuario no son inmediatos a su notificacion
	9.2	9.2.2	Gestion de derechos de acceso asignados a los usuarios	Cumple	0,071428571	0,071428571	Se evidencia cumplimiento se los lineamientos en la matriz de responsables y autoridades LI-RD-08
	9.2	9.2.3	Gestion de los derechos de acceso con privilegios especiales	Cumple	0,071428571	0,071428571	Se evidencia cumplimiento se los lineamientos en la matriz de responsables y autoridades LI-RD-08
	9.2	9.2.4	Gestion de informacion confidencial de autenticacion de usuarios	Cumple	0,071428571	0,071428571	Se evidencia el seguro almacenamiento de las bases de datos de usuarios dentro del directorio activo cumpliendo requisitos de encriptamiento nivel SHA1 de 4096 bits diponible por la plataforma Microsoft WinServer

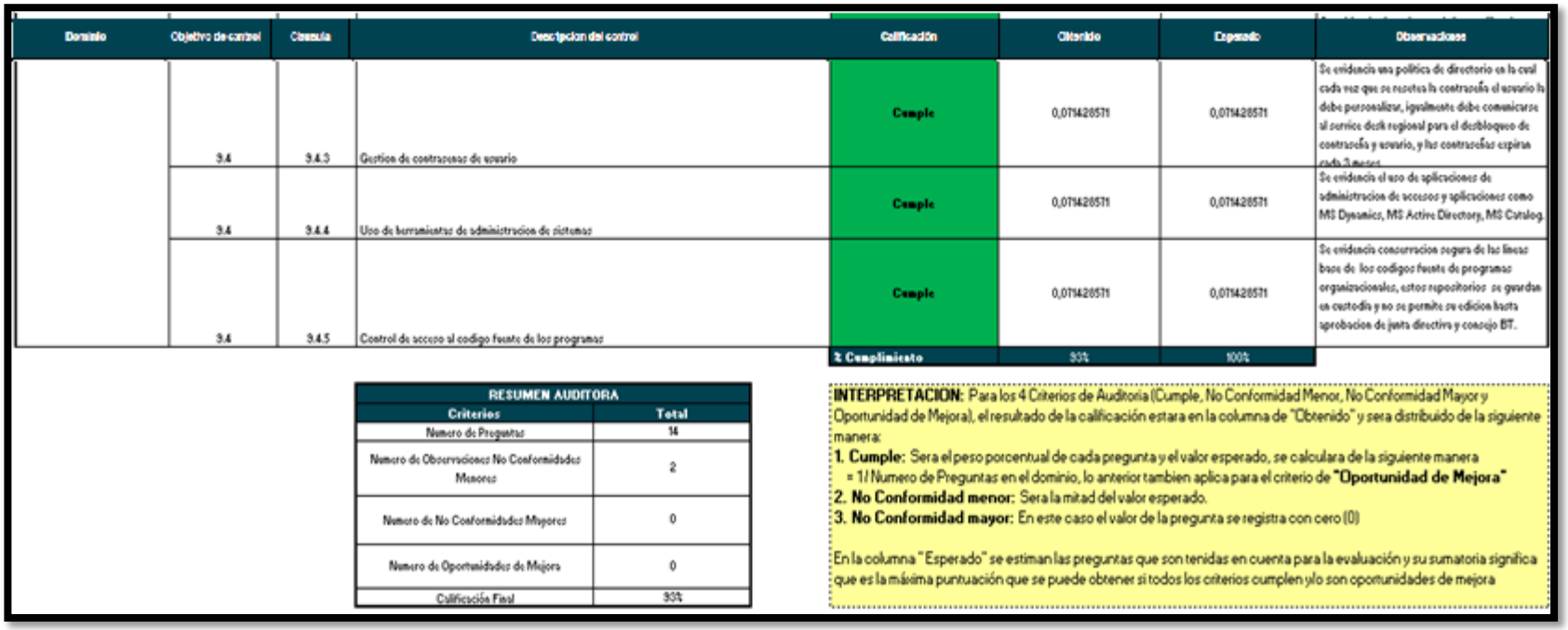
Continúa…

Fig 12. Listados de Auditoria, Dominio 9 (Continuación)

Dominio	Objetivo de control	Cláusula	Descripción del control	Calificación	Obtenido	Esperado	Observaciones
9. Control de accesos	9.2	9.2.5	Revisión de los derechos de acceso de los usuarios	cumple	0,071428571	0,071428571	Se evidencia el monitoreo de los perfiles de acceso de los diferentes usuarios segun el area y cargo que desempeñan almacenado estos privilegios con la matriz LI-PID-01
	9.2	9.2.6	Retirada o adaptacion de los derechos de acceso	No Conformidad Menor	0,035714286	0,071428571	Se evidenci la existencia de la politica de cambio d eprivilegios y control de accesos para los traslados o movimientos de personal, se evidencia la gestion correcta por el area de infraestructura, sin embargo el retiro y adaptacion de privilegios no se realiza inmediatamente se informa por parte d ela gerencia a cargo.
	Responsabilidad de usuario						
	9.3	9.3.1	Uso de información confidencial para la autenticacion	Cumple	0,071428571	0,071428571	Se evidencia una cultura de confidencialidad en los usuarios de los sistemas de la organización en la cual no se permite el uso de contraseñas grupales o prestamo de usuarios y contraseñas.
	Control de acceso a sistemas y aplicaciones						
	9.4	9.4.1	Restriccion del acceso a la información	Cumple	0,071428571	0,071428571	Se evidencia la existencia de privilegios y restricciones de acceso a sitios, carpetas y grupos dacuerdo al los asignados al cargo y rol del funcionario en la organización según la matriz LI-PID-08
	9.4	9.4.2	Procedimientos seguros de inicio de sesion	Cumple	0,071428571	0,071428571	Se evidencia la existencia de una configuracion de autenticacion segura en el dominio de la organización bazada en el directorio activo de windows.

Continúa…

Fig 12. Listados de Auditoria, Dominio 9 (Continuación)



Dominio	Objetivo de control	Cláusula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
	9.4	9.4.3	Gestion de contraseñas de usuario	Cumple	0,071428571	0,071428571	Se evidencia una política de directorio en la cual cada vez que se restablece la contraseña el usuario la debe personalizar, igualmente debe comunicarse al service desk regional para el desbloqueo de contraseña y usuario, y las contraseñas expiran cada 3 meses
	9.4	9.4.4	Uso de herramientas de administracion de sistemas	Cumple	0,071428571	0,071428571	Se evidencia el uso de aplicaciones de administracion de accesos y aplicaciones como MS Dynamics, MS Active Directory, MS Catalog
	9.4	9.4.5	Control de acceso al codigo fuente de los programas	Cumple	0,071428571	0,071428571	Se evidencia concurrencia segura de las líneas base de los codigos fuente de programas organizacionales, estos repositorios se guardan en custodia y no se permite su edición hasta aprobacion de junta directiva y consejo BT.
				% Cumplimiento	93%	100%	

RESUMEN AUDITORIA	
Criterios	Total
Numero de Preguntas	14
Numero de Observaciones No Conformidades Menores	2
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	93%

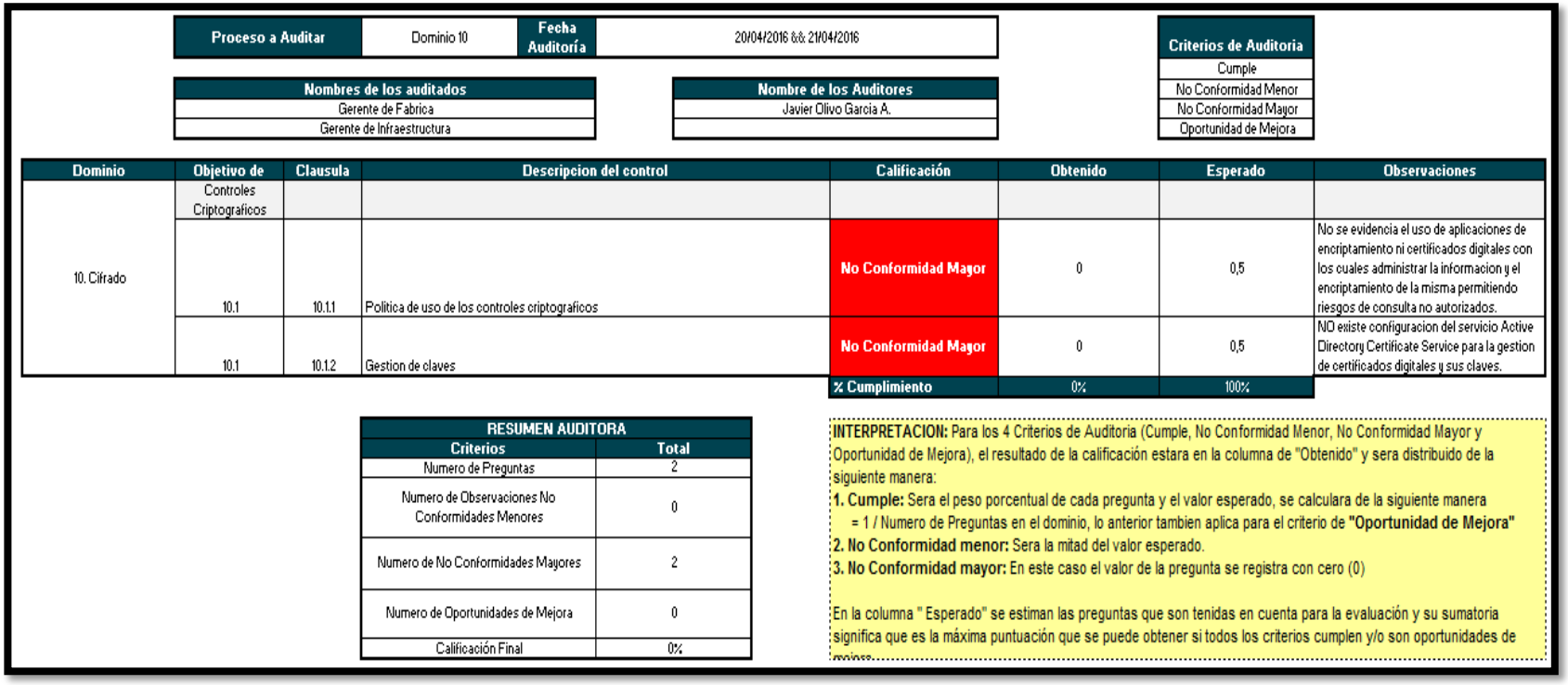
INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera
   = 1/ Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna "Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen ylo son oportunidades de mejora

Fuente: I&T Stefanini

Fig. 13 Listados de Auditoria Dominio 10.



Proceso a Auditar	Dominio 10	Fecha Auditoría	20/04/2016 && 21/04/2016

Nombres de los auditados
Gerente de Fabrica
Gerente de Infraestructura

Nombre de los Auditores
Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
10. Cifrado	Controles Criptograficos						
	10.1	10.1.1	Politica de uso de los controles criptograficos	No Conformidad Mayor	0	0,5	No se evidencia el uso de aplicaciones de encriptamiento ni certificados digitales con los cuales administrar la informacion y el encriptamiento de la misma permitiendo riesgos de consulta no autorizados.
	10.1	10.1.2	Gestion de claves	No Conformidad Mayor	0	0,5	NO existe configuracion del servicio Active Directory Certificate Service para la gestion de certificados digitales y sus claves.
				% Cumplimiento	0%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	2
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	2
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora.

Fuente: I&T Stefanini

Fig 14. Listados de Auditoria Dominio 11.

Proceso a Auditar	Dominio 11	Fecha Auditoría	2016-04-22

Nombres de los auditados
Gerente de Fabrica
Gerente de infraestructura

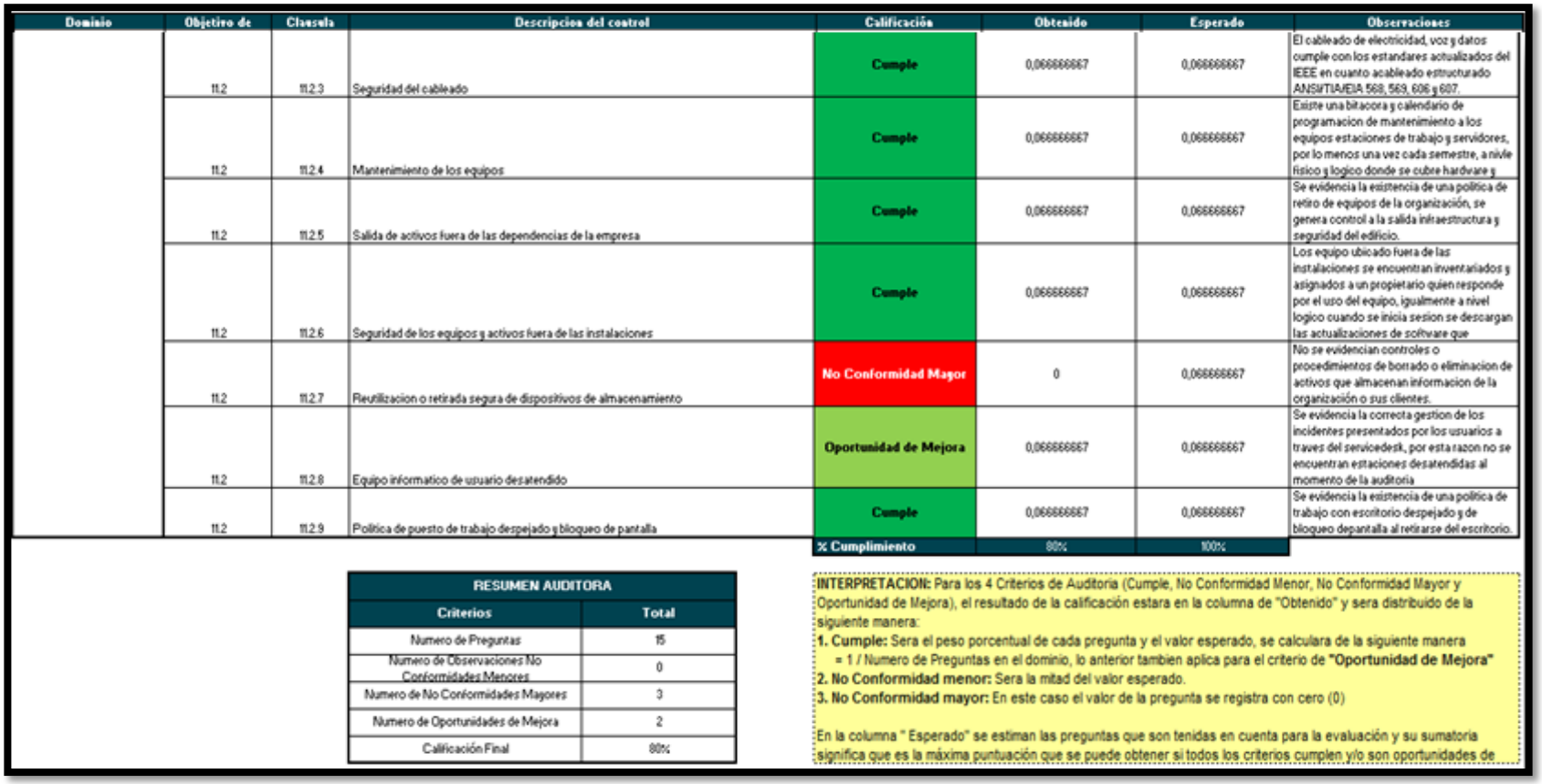
Nombre de los Auditores
Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
	Areas Seguras						
	11.1	11.1.1	Perimetro de seguridad Fisica	No Conformidad Mayor	0	0,066666667	Se evidencia que la fabrica de software ubicada en la sede principal calle 122 no dispone de aislamiento del resto de areas operativas y administrativas.
	11.1	11.1.2	Controles fisicos a la entrada	No Conformidad Mayor	0	0,066666667	No se evidencian controles fisicol o logicos para el acceso a la fabrica de software
	11.1	11.1.3	Seguridad de oficinas, despachos y recursos	Oportunidad de Mejora	0,066666667	0,066666667	Se evidencia que en las instalaciones en las que funciona la fabrica de sofware se dispone de CCTV conectados al area de seguridad del edificio, sin embargo esta vigilancia deberia ser propia de la
	11.1	11.1.4	proteccion contra las amenazas externas y ambientales	Cumple	0,066666667	0,066666667	Se evidencia la existencia y actualizacion de los sistemas de control de incendios y sistemas de proteccion a tierra.
	11.1	11.1.5	Trabajo en areas Seguras	Cumple	0,066666667	0,066666667	El area de trabajo de la fabrica de software no es accesible para personal ajeno a la organización, adicionalmente dispone de CCTV y vigilancia ocasional a cargo del
	11.1	11.1.6	Areas de acceso publico, carga y descarga	Cumple	0,066666667	0,066666667	El area no es accesible al publico, y por la naturaleza del area no se realizan trabajos de cargue y descargue en el area.
	Seguridad de los equipos						
	11.2	11.2.1	Emplazamiento y proteccion de equipos	Cumple	0,066666667	0,066666667	Las estaciones de trabajo en la organización son portatiles y disponen de los materiales de aseguramiento a los escritorios por medio de dockings ajustables, existe un SPT y adicional las estaciones portatiles se protejen con su propia bateria.
11. Seguridad Fisica y ambiental	11.2	11.2.2	Instalaciones de suministro	Cumple	0,066666667	0,066666667	El suministro electrico esta a cargo del edificio el cual dispone de plantas electricas diesel de 100 KVA ubicadas en la terraza aisladas de personal ajeno a la administrcion

Continúa…

Fig 14. Listados de Auditoria Dominio 11 (Continuación)



Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
	11.2	11.2.3	Seguridad del cableado	Cumple	0,066666667	0,066666667	El cableado de electricidad, voz y datos cumple con los estandares actualizados del IEEE en cuanto acableado estructurado ANSI/TIA/EIA 568, 569, 606 y 607.
	11.2	11.2.4	Mantenimiento de los equipos	Cumple	0,066666667	0,066666667	Existe una bitacora y calendario de programacion de mantenimiento a los equipos estaciones de trabajo y servidores, por lo menos una vez cada semestre, a nivle fisico y logico donde se cubre hardware y
	11.2	11.2.5	Salida de activos fuera de las dependencias de la empresa	Cumple	0,066666667	0,066666667	Se evidencia la existencia de una politica de retiro de equipos de la organización, se genera control a la salida infraestructura y seguridad del edificio.
	11.2	11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Cumple	0,066666667	0,066666667	Los equipo ubicado fuera de las instalaciones se encuentran inventariados y asignados a un propietario quien responde por el uso del equipo, igualmente a nivel logico cuando se inicia sesion se descargan las actualizaciones de software que
	11.2	11.2.7	Reutilizacion o retirada segura de dispositivos de almacenamiento	No Conformidad Mayor	0	0,066666667	No se evidencian controles o procedimientos de borrado o eliminacion de activos que almacenan informacion de la organización o sus clientes.
	11.2	11.2.8	Equipo informatico de usuario desatendido	Oportunidad de Mejora	0,066666667	0,066666667	Se evidencia la correcta gestion de los incidentes presentados por los usuarios a traves del servicedesk, por esta razon no se encuentran estaciones desatendidas al momento de la auditoria
	11.2	11.2.9	Politica de puesto de trabajo despejado y bloqueo de pantalla	Cumple	0,066666667	0,066666667	Se evidencia la existencia de una politica de trabajo con escritorio despejado y de bloqueo depantalla al retirarse del escritorio.
				% Cumplimiento	80%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	15
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	3
Numero de Oportunidades de Mejora	2
Calificación Final	80%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de

Fuente: I&T Stefanini

Fig 15. Listados de Auditoria Dominio 12.

Proceso a Auditar	Dominio 12	Fecha Auditoría	25/04/2016 && 26/04/2016

Nombres de los auditados
Gerente de Fabrica
Gerente de Infraestructura

Nombre de los Auditores
Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
	Responsabilidad y porcedimeintos de operacion						
	12.1	12.1.1	Documentacion de procedimientos de operacion	Cumple	0,071428571	0,071428571	Se evidencia la existencia de manuales, cursos, presentaciones y procesos de operación sujetos al manual de calidad organizacional.
	12.1	12.1.2	Gestion de activos	Cumple	0,071428571	0,071428571	Se evidencia la existencia de procedimientos de gestion de activos organizacionales fisiocos y logicos, estos procedimientos se encuentran publicos en la intranet y estan sujetos al manual de calidad de la organización.
	12.1	12.1.3	Gestion de capacidades	Cumple	0,071428571	0,071428571	Se evidencia la existencia de evaluaciones de capacidad de manera continua las cuales se sujetan a los procedimientos y metodoslogias observadas por la gerencia y la politica de calidad.
	12.1	12.1.4	Separacion de entornos de desarrollo, prueba y produccion	No Conformidad Mayor	0	0,071428571	En la sede principal de la organización no se encuentran diferenciados los entornos de desarrollo, prueba y produccion.
	Proteccion contra codigo malicioso						
	12.2	12.2.1	Controles contra el codigo malicioso	Cumple	0,071428571	0,071428571	Existe una politica de auditoria mediante el directorio activo la cual se ejecuta en periodos semanales, adicionalmente existen restricciones para la instalacion de software por parte de los usuarios y se utiliza la suite MS Security essentials.
	Copias de seguridad						
	12.3	12.3.1	Copias de seguridad de la informacion	Cumple	0,071428571	0,071428571	Existe una politica de backups de la organización la cual se cumple y actualiza de manera permanente y continua.

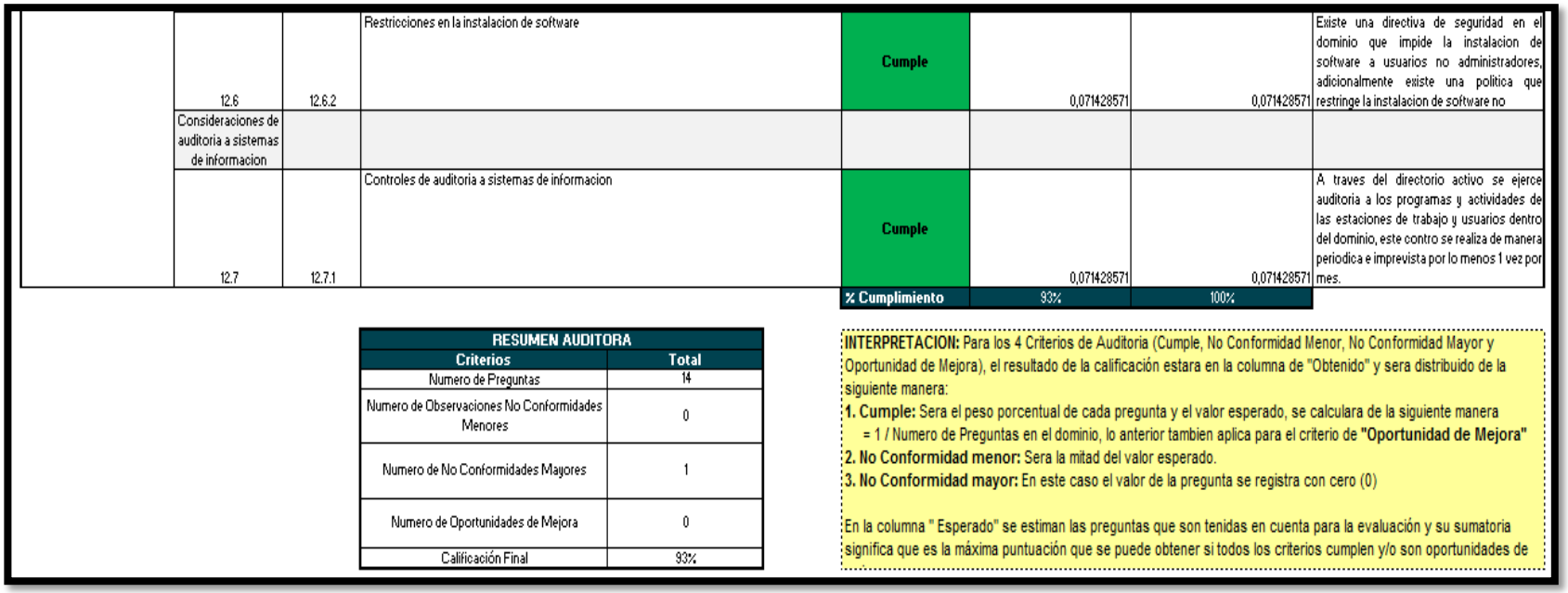
Continúa…

Fig 15. Listados de Auditoria Dominio 12 (Continuación)

12. Seguridad en las operaciones	Registro de actividad y						
	12.4	12.4.1	Registro y gestion de eventos de actividad	Cumple	0,071428571	0,071428571	Se evidencia la existencia de logs de eventos y la supervision sobre estos garantizando la seguridad en las operaciones.
	12.4	12.4.2	Proteccion de los registros de la informacion	Cumple	0,071428571	0,071428571	Los registros y logs de eventos se encuentran respaldados y protegidos en los servidores, adicionalmente se guarda un backup en cintas de almacenamiento que se cambianb cada semana.
	12.4	12.4.3	Registros de actividad del operador y administrador del sistema	Cumple	0,071428571	0,071428571	A traves del AD de micrososft se controla y monitorea las horas de inicio de sesion en los sistemas organizacionales segun la politica de seguridad y el cargo desempenado, igualmente se ejece supervision sobre los logs de aplicaciones
	12.4	12.4.4	Sincronizacion de relojes	Cumple	0,071428571	0,071428571	Los relojes de sistemas, personal y organizacion se encuentran sincronizados con la hora legal colombiana y GMT indicados por el Instituto Nacional de
	Control del software en explotacion						
	12.5	12.5.1	Instalacion de software en sistemas en produccion	Cumple	0,071428571	0,071428571	Solamente el area de infraestructura puede realizar instalacion de programas sobre las estaciones y para ello debe realziar una solicitud al servicedesk quien instala el programa del catalogo interno de la organizacion.
	Gestion de la vulnerabilidad						
	12.6	12.6.1	Gestion de las vulnerabilidades tecnicas	Cumple	0,071428571	0,071428571	Existe una politica de seguridad que actualiza a diario los mecanismos de segurtidad en el dominio, igualmente se dispone de un equipo tecnico que ejerce control preventivo y correctivo a las vulnerabilidades que se presentan en la infraestructura de la organizacion

Continúa…

Fig 15. Listados de Auditoria Dominio 12 (Continuación)



	12.6	12.6.2	Restricciones en la instalacion de software	Cumple	0,071428571	0,071428571	Existe una directiva de seguridad en el dominio que impide la instalacion de software a usuarios no administradores, adicionalmente existe una politica que restringe la instalacion de software no
	Consideraciones de auditoria a sistemas de informacion						
	12.7	12.7.1	Controles de auditoria a sistemas de informacion	Cumple	0,071428571	0,071428571	A traves del directorio activo se ejerce auditoria a los programas y actividades de las estaciones de trabajo y usuarios dentro del dominio, este contro se realiza de manera periodica e imprevista por lo menos 1 vez por mes.
				% Cumplimiento	93%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	14
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	1
Numero de Oportunidades de Mejora	0
Calificación Final	93%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de

Fuente: I&T Stefanini

Figura 16. Listados de Auditoria Dominio 13.

Proceso a Auditar	Dominio 13	Fecha Auditoría	25/04/2016 && 26/04/2016

Nombres de los auditados
Gerente de Fabrica
Gerente de Infraestructura

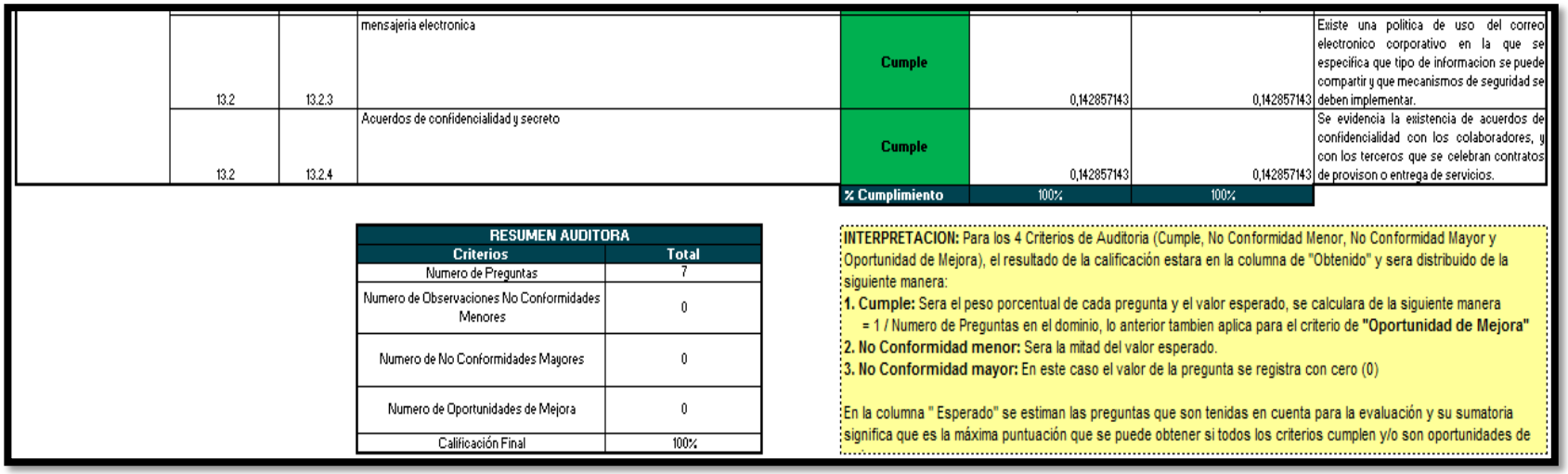
Nombre de los Auditores
Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
13. Seguridad en las telecomunicaciones	Gestion de la seguridad en las redes						
	13.1	13.1.1	Controles de red	Cumple	0,142857143	0,142857143	Se tienen implementados y funcionales los firewall de la organizacion, sistemas IDS/IDP, proxies y balanceadores de carga que ejercen control sobre el trafico y actividades en la red
	13.1	13.1.2	Mecanismos de seguridad asociados con servicios en red	Cumple	0,142857143	0,142857143	A nivel de enrutadores y switches se encuentran configurados de manera correcta los protocolos de encriptacion y el protocolo IPSEC de Cisco.
	13.1	13.1.3	Segregacion de redes	Cumple	0,142857143	0,142857143	La red de la organizacion se encuentra subneteada por areas optimizando los anchos de banda y seguridad operativa, se tienen en cuenta una configuracion de red categoria B, con mascara sub 24.
	Intercambio de informacion con partes externas						
	13.2	13.2.1	Politicas y procesimientos de intercambio de informacion	Cumple	0,142857143	0,142857143	Existe una politica de intercambio de informacion entre areas internas y externas de la organizacion, esta politica se revisa 1 vez por semestre.
	13.2	13.2.2	Acuerdos de intercambio	Cumple	0,142857143	0,142857143	Se evidenan acuerdos de intercambio y porpiedad intelectual en la contratacion con terceros.

Continúa…

Fig 16. Listados de Auditoria Dominio 13 (Continuación)



	13.2	13.2.3	mensajeria electronica	Cumple	0,142857143	0,142857143	Existe una politica de uso del correo electronico corporativo en la que se especifica que tipo de informacion se puede compartir y que mecanismos de seguridad se deben implementar.
	13.2	13.2.4	Acuerdos de confidencialidad y secreto	Cumple	0,142857143	0,142857143	Se evidencia la existencia de acuerdos de confidencialidad con los colaboradores, y con los terceros que se celebran contratos de provison o entrega de servicios.
				% Cumplimiento	100%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	7
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	100%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de

Fuente: I&T Stefanini

Fig 17. Listados de auditoria, Dominio 14.

Proceso a Auditar	Dominio 14	Fecha Auditoría	2016-04-27

Nombres de los auditados
Gerente de Fabrica

Nombre de los Auditores
Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
	Requisitos de seguridad de los sistemas de informacion						
	14.1	14.1.1	Analisis y especificacion de los requisitos de seguridad	Cumple	0,076923077	0,076923077	Se evidencia una politica de seguridad de la informacion, donde se especifican los requistos de seguridad dentro de la organizacion.
	14.1	14.1.2	Seguridad en las comunicaciones en servicios accesibles por redes publicas	Cumple	0,076923077	0,076923077	La organizacion solamente dispone de un servicio de contacto externo a traves de su pagina web que se encuentra abierta al publico, este servicio se reside en un equipo blinadado con antivirus y un firewall con una base de conocimientos sobre ataque frecuentes, adicional las comunicaciones se realizan a traves de puertos seguros.
	14.1	14.1.3	Proteccion de las transacciones realizadas por redes telematicas	Cumple	0,076923077	0,076923077	La informacion en la red viaja encriptada adicionalmente las aplicaciones transaccionales usan capas de3 seguridad que impiden la interceptacion de los datos, capas como: certificados de seguridad, uso de puertos seguros, encriptacion a nivel de red con IPSEC.
	Seguridad en los procesos de desarrollo y soporte						
	14.2	14.2.1	Politica de desarrollo seguro de software	Cumple	0,076923077	0,076923077	Se evidencia una politica de desarrollo de software sujeta a los mas altos estandares de seguridad como se solicita en CMMI y en las metodologias agiles.
	14.2	14.2.2	Procedimientos de control de cambios de los sistemas	Cumple	0,076923077	0,076923077	Existe una politica, procedimientos , y capaciotaciones internas sobre el controm de cambios en el software como se solicita en el estandar CMMI.

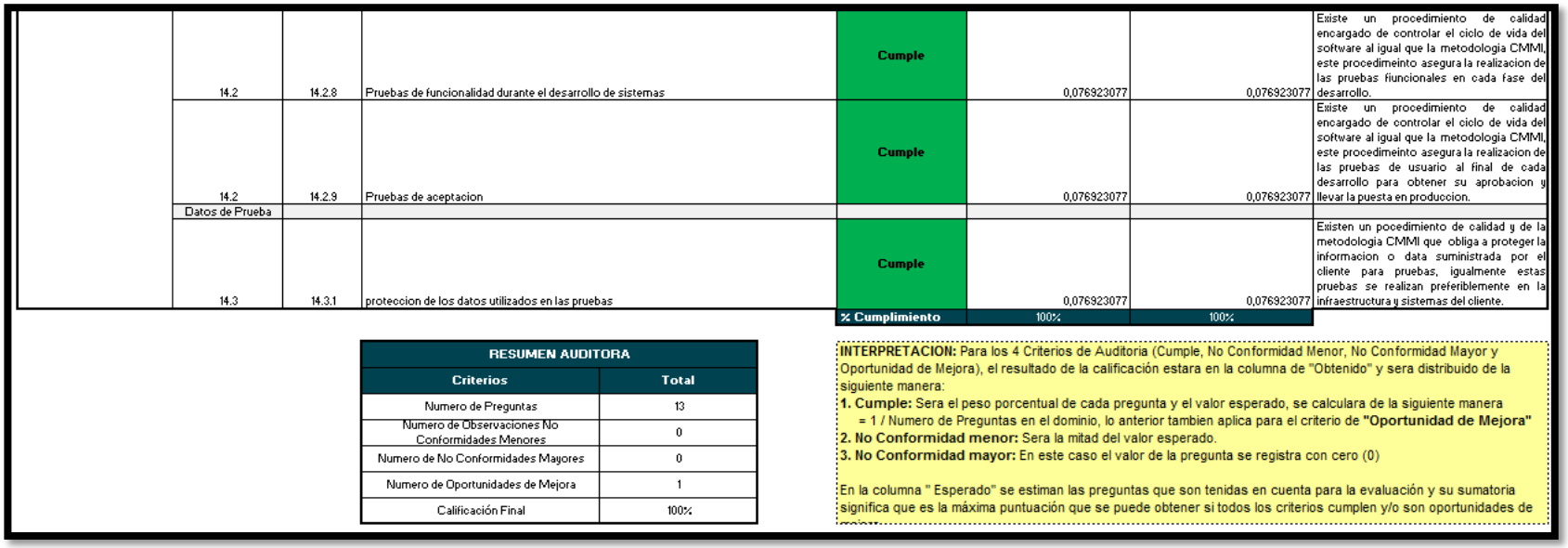
Continúa…

Fig 17. Listados de auditoria, Dominio 14 (Continuación)

14. Adquisicion, desarrollo y mantenimiento de los sistemas de informacion	14.2	14.2.3	Revision tecnica de las aplicaciones tras efectuar cambios en el sistema operativo	Cumple	0,076923077	0,076923077	Existe una politica de desarrollo y revision la cual establece un procedimiento en el cual el desarrollador es la primera capa, se realiza revision de pares con el lider tecnico o gerente de proyecto, adicionalmente se hace otra revision por el area QA..
	14.2	14.2.4	Restricciones a los cambios en los paquetes de software	Cumple	0,076923077	0,076923077	Existen procedimientos de modificacion de Lineas Base, este procedimeinto establece la revision de pares y aprobacion del oficial de seguridad o gerente de operaciones de la organizacion, igualmente siempre se respalda la linea base con el objetivo de poder realizar un rollback en caso fortuito.
	14.2	14.2.5	Uso de principios de ingenieria en proteccion de sistemas	Cumple	0,076923077	0,076923077	Las lineas base se almacenan en repositorios segurosy solo se puede acceder a una copia de la linea base para realizar una modifdicacion, para aprobar esta modificacion debe existir revision de pares y aprobacion de la direccion.
	14.2	14.2.6	Seguridad en entornos de desarrollo	Cumple	0,076923077	0,076923077	
	14.2	14.2.7	Externalizacion del desarrollo de software	Oportunidad de Mejora	0,076923077	0,076923077	Se omite ya que la organizacion no externaliza el desarrollo de software, este se realiza inhouse por las fabricas internas, sin embargo se debe generar una politica de desarrollo con externos.

Continúa…

Fig 17. Listados de auditoria, Dominio 14 (Continuación)



	14.2	14.2.8	Pruebas de funcionalidad durante el desarrollo de sistemas	Cumple	0,076923077	0,076923077	Existe un procedimiento de calidad encargado de controlar el ciclo de vida del software al igual que la metodologia CMMI, este procedimeinto asegura la realizacion de las pruebas fiuncionales en cada fase del desarrollo.
	14.2	14.2.9	Pruebas de aceptacion	Cumple	0,076923077	0,076923077	Existe un procedimiento de calidad encargado de controlar el ciclo de vida del software al igual que la metodologia CMMI, este procedimeinto asegura la realizacion de las pruebas de usuario al final de cada desarrollo para obtener su aprobacion y llevar la puesta en produccion.
	Datos de Prueba						
	14.3	14.3.1	proteccion de los datos utilizados en las pruebas	Cumple	0,076923077	0,076923077	Existen un pocedimiento de calidad y de la metodologia CMMI que obliga a proteger la informacion o data suministrada por el cliente para pruebas, igualmente estas pruebas se realizan preferiblemente en la infraestructura y sistemas del cliente.
				% Cumplimiento	100%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	13
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	1
Calificación Final	100%

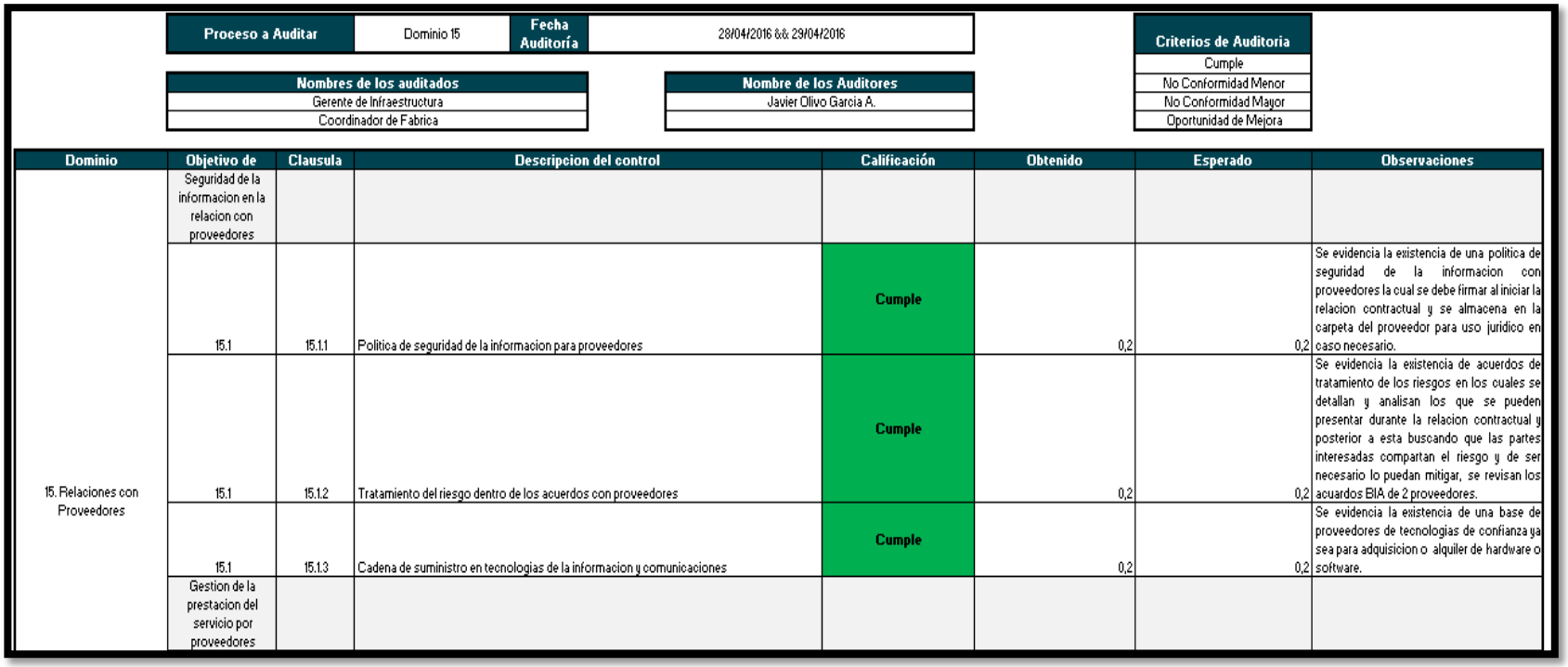
INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera
   = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de

Fuente: I&T Stefanini

Fig 18. Listados de auditoria, Dominio 15.



Proceso a Auditar	Dominio 15	Fecha Auditoría	28/04/2016 && 29/04/2016

Nombres de los auditados
Gerente de Infraestructura
Coordinador de Fabrica

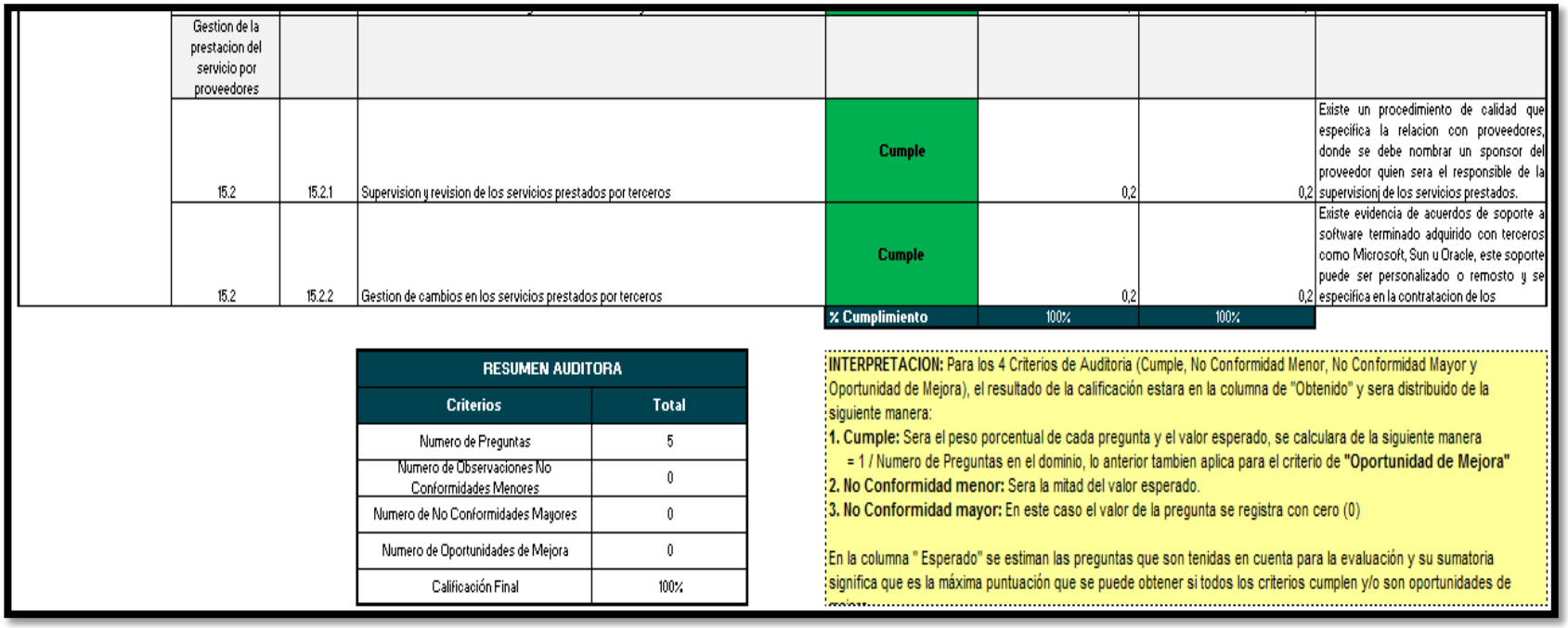
Nombre de los Auditores
Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
15. Relaciones con Proveedores	Seguridad de la informacion en la relacion con proveedores						
	15.1	15.1.1	Politica de seguridad de la informacion para proveedores	Cumple	0,2	0,2	Se evidencia la existencia de una politica de seguridad de la informacion con proveedores la cual se debe firmar al iniciar la relacion contractual y se almacena en la carpeta del proveedor para uso juridico en caso necesario.
	15.1	15.1.2	Tratamiento del riesgo dentro de los acuerdos con proveedores	Cumple	0,2	0,2	Se evidencia la existencia de acuerdos de tratamiento de los riesgos en los cuales se detallan y analisan los que se pueden presentar durante la relacion contractual y posterior a esta buscando que las partes interesadas compartan el riesgo y de ser necesario lo puedan mitigar, se revisan los acuardos BIA de 2 proveedores.
	15.1	15.1.3	Cadena de suministro en tecnologias de la informacion y comunicaciones	Cumple	0,2	0,2	Se evidencia la existencia de una base de proveedores de tecnologias de confianza ya sea para adquisicion o alquiler de hardware o software.
	Gestion de la prestacion del servicio por proveedores						

Continúa…

Fig 18. Listados de auditoria, Dominio 15 (Continuación)



	Gestion de la prestacion del servicio por proveedores						
	15.2	15.2.1	Supervision y revision de los servicios prestados por terceros	Cumple	0,2	0,2	Existe un procedimiento de calidad que especifica la relacion con proveedores, donde se debe nombrar un sponsor del proveedor quien sera el responsible de la supervisionj de los servicios prestados.
	15.2	15.2.2	Gestion de cambios en los servicios prestados por terceros	Cumple	0,2	0,2	Existe evidencia de acuerdos de soporte a software terminado adquirido con terceros como Microsoft, Sun u Oracle, este soporte puede ser personalizado o remosto y se especifica en la contratacion de los
				% Cumplimiento	100%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	5
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	100%

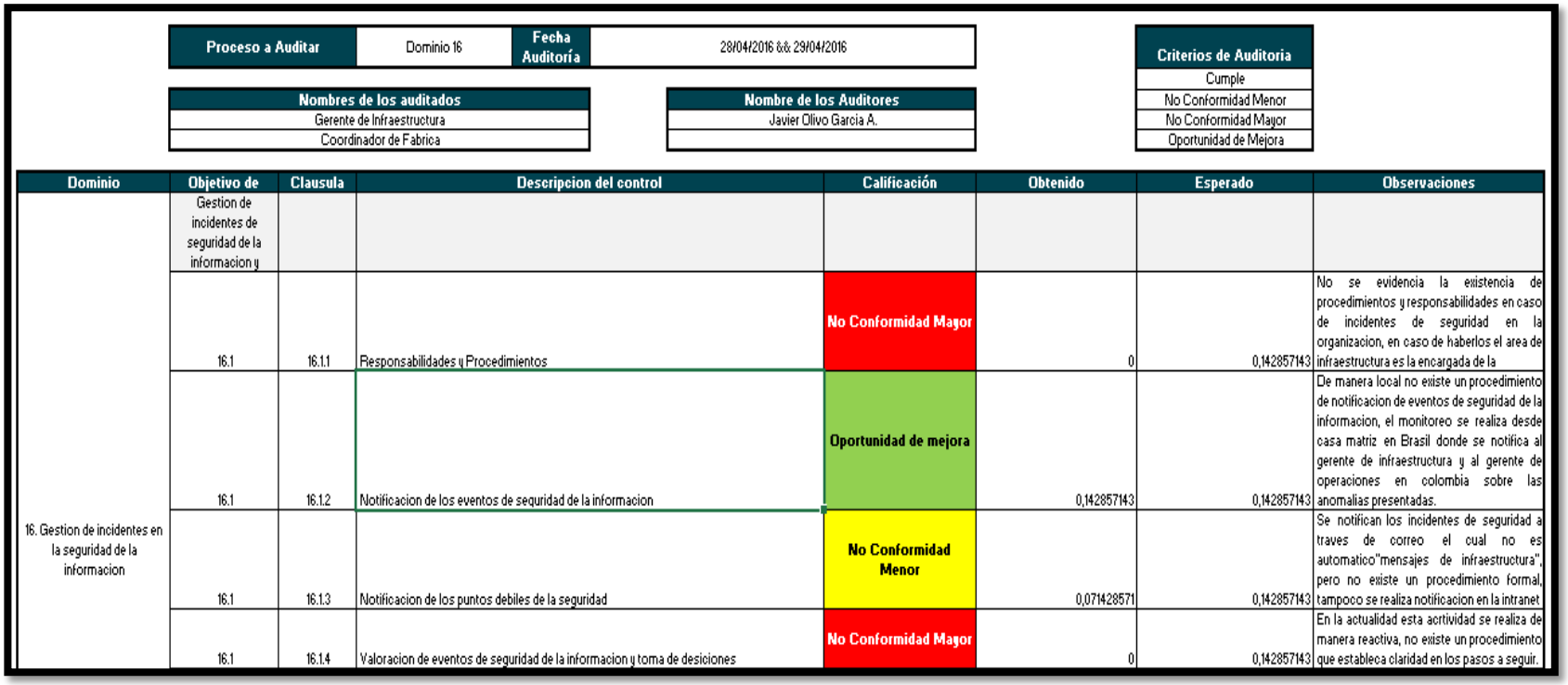
INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de

Fuente: I&T Stefanini

Fig 19. Listados de auditoria, Dominio 16.



Proceso a Auditar	Dominio 16	Fecha Auditoría	28/04/2016 && 29/04/2016

Nombres de los auditados
Gerente de Infraestructura
Coordinador de Fabrica

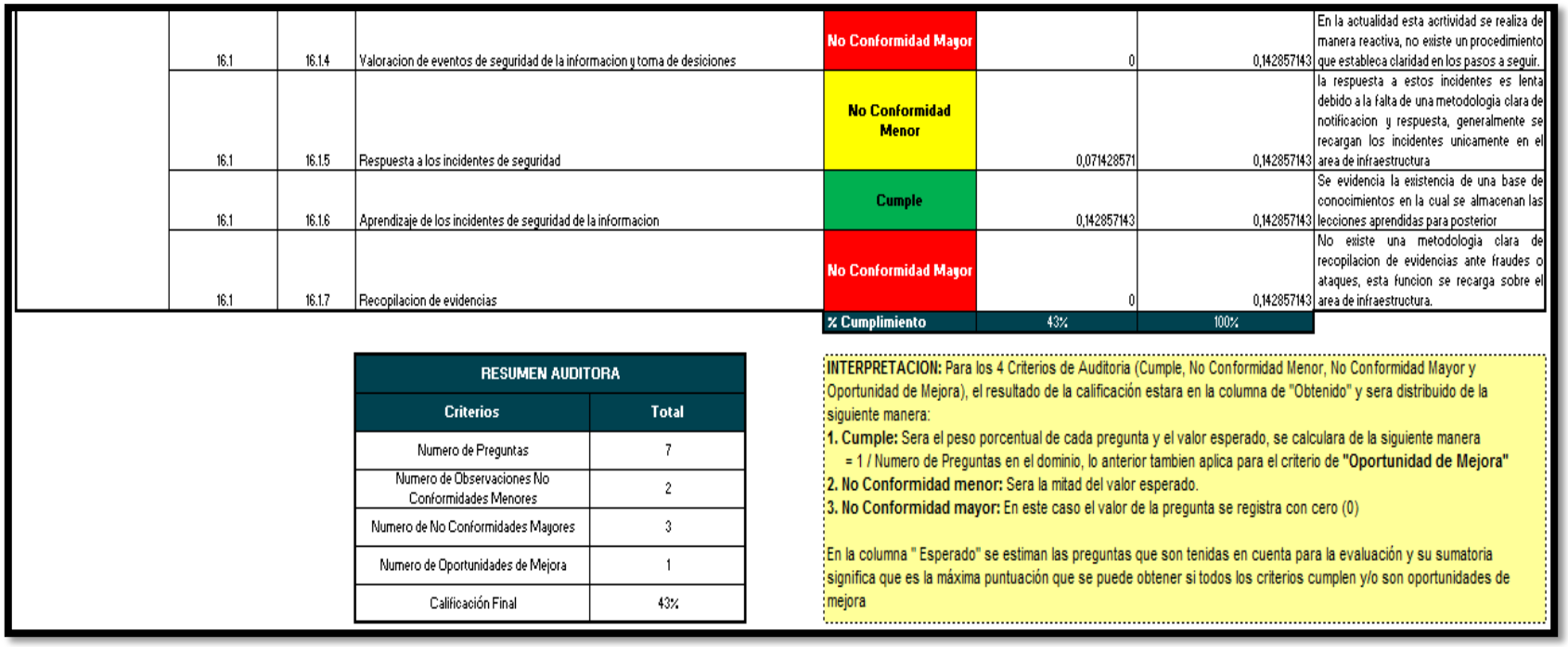
Nombre de los Auditores
Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
	Gestion de incidentes de seguridad de la informacion y						
	16.1	16.1.1	Responsabilidades y Procedimientos	No Conformidad Mayor	0	0,142857143	No se evidencia la existencia de procedimientos y responsabilidades en caso de incidentes de seguridad en la organizacion, en caso de haberlos el area de infraestructura es la encargada de la
	16.1	16.1.2	Notificacion de los eventos de seguridad de la informacion	Oportunidad de mejora	0,142857143	0,142857143	De manera local no existe un procedimiento de notificacion de eventos de seguridad de la informacion, el monitoreo se realiza desde casa matriz en Brasil donde se notifica al gerente de infraestructura y al gerente de operaciones en colombia sobre las anomalias presentadas.
16. Gestion de incidentes en la seguridad de la informacion	16.1	16.1.3	Notificacion de los puntos debiles de la seguridad	No Conformidad Menor	0,071428571	0,142857143	Se notifican los incidentes de seguridad a traves de correo el cual no es automatico"mensajes de infraestructura", pero no existe un procedimiento formal, tampoco se realiza notificacion en la intranet
	16.1	16.1.4	Valoracion de eventos de seguridad de la informacion y toma de desiciones	No Conformidad Mayor	0	0,142857143	En la actualidad esta acrtividad se realiza de manera reactiva, no existe un procedimiento que estableca claridad en los pasos a seguir.

Continúa…

Fig 19. Listados de auditoria, Dominio 16 (Continuación)



	16.1	16.1.4	Valoracion de eventos de seguridad de la informacion y toma de desiciones	No Conformidad Mayor	0	0,142857143	En la actualidad esta acrtividad se realiza de manera reactiva, no existe un procedimiento que estableca claridad en los pasos a seguir.
	16.1	16.1.5	Respuesta a los incidentes de seguridad	No Conformidad Menor	0,071428571	0,142857143	la respuesta a estos incidentes es lenta debido a la falta de una metodologia clara de notificacion y respuesta, generalmente se recargan los incidentes unicamente en el area de infraestructura
	16.1	16.1.6	Aprendizaje de los incidentes de seguridad de la informacion	Cumple	0,142857143	0,142857143	Se evidencia la existencia de una base de conocimientos en la cual se almacenan las lecciones aprendidas para posterior
	16.1	16.1.7	Recopilacion de evidencias	No Conformidad Mayor	0	0,142857143	No existe una metodologia clara de recopilacion de evidencias ante fraudes o ataques, esta funcion se recarga sobre el area de infraestructura.
				% Cumplimiento	43%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	7
Numero de Observaciones No Conformidades Menores	2
Numero de No Conformidades Mayores	3
Numero de Oportunidades de Mejora	1
Calificación Final	43%

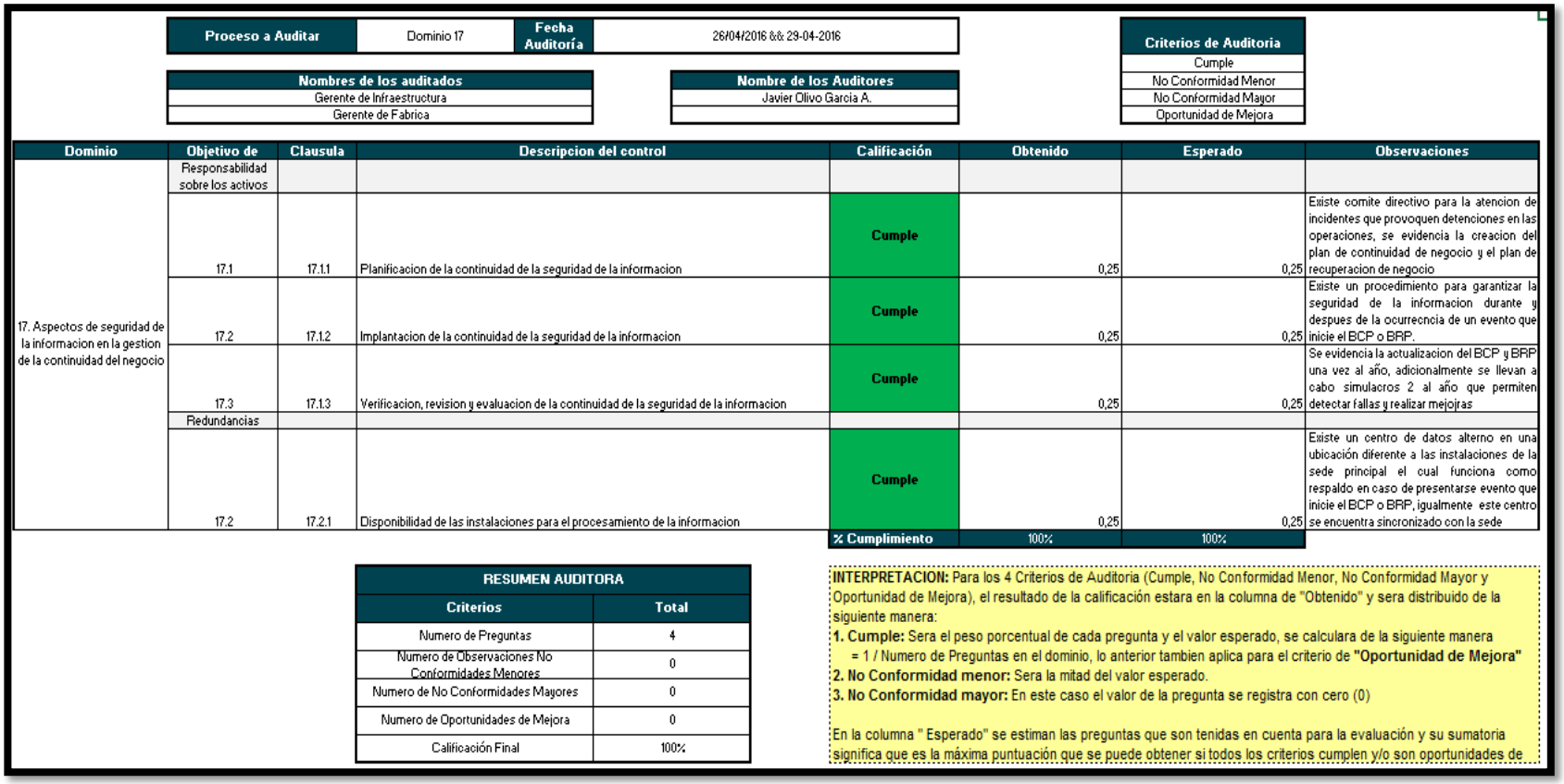
INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Fuente: I&T Stefanini

Fig. 20. Listados de auditoria, Dominio 17.



Proceso a Auditar	Dominio 17	Fecha Auditoría	26/04/2016 && 29-04-2016

Nombres de los auditados
Gerente de Infraestructura
Gerente de Fabrica

Nombre de los Auditores
Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
17. Aspectos de seguridad de la informacion en la gestion de la continuidad del negocio	Responsabilidad sobre los activos						
	17.1	17.1.1	Planificacion de la continuidad de la seguridad de la informacion	Cumple	0,25	0,25	Existe comite directivo para la atencion de incidentes que provoquen detenciones en las operaciones, se evidencia la creacion del plan de continuidad de negocio y el plan de recuperacion de negocio
	17.2	17.1.2	Implantacion de la continuidad de la seguridad de la informacion	Cumple	0,25	0,25	Existe un procedimiento para garantizar la seguridad de la informacion durante y despues de la ocurreccnia de un evento que inicie el BCP o BRP.
	17.3	17.1.3	Verificacion, revision y evaluacion de la continuidad de la seguridad de la informacion	Cumple	0,25	0,25	Se evidencia la actualizacion del BCP y BRP una vez al año, adicionalmente se llevan a cabo simulacros 2 al año que permiten detectar fallas y realizar mejoras
	Redundancias						
	17.2	17.2.1	Disponibilidad de las instalaciones para el procesamiento de la informacion	Cumple	0,25	0,25	Existe un centro de datos alterno en una ubicación diferente a las instalaciones de la sede principal el cual funciona como respaldo en caso de presentarse evento que inicie el BCP o BRP, igualmente este centro se encuentra sincronizado con la sede
				% Cumplimiento	100%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	4
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	100%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. Cumple: Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera
= 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**

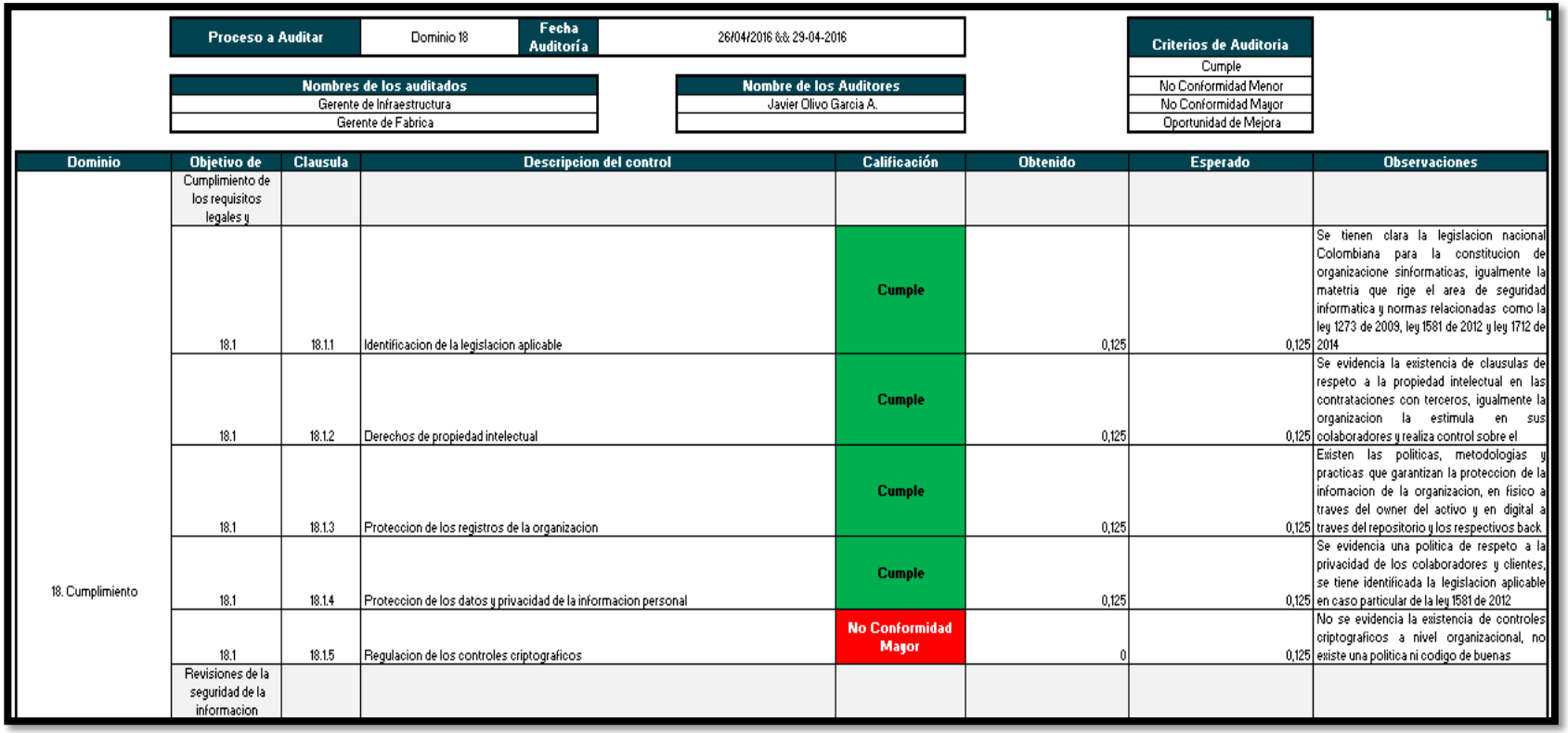
2. No Conformidad menor: Sera la mitad del valor esperado.

3. No Conformidad mayor: En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de

Fuente: I&T Stefanini

Fig. 21. Listados de auditoria, Dominio 18.



Proceso a Auditar	Dominio 18	Fecha Auditoría	26/04/2016 && 29-04-2016

Nombres de los auditados
Gerente de Infraestructura
Gerente de Fabrica

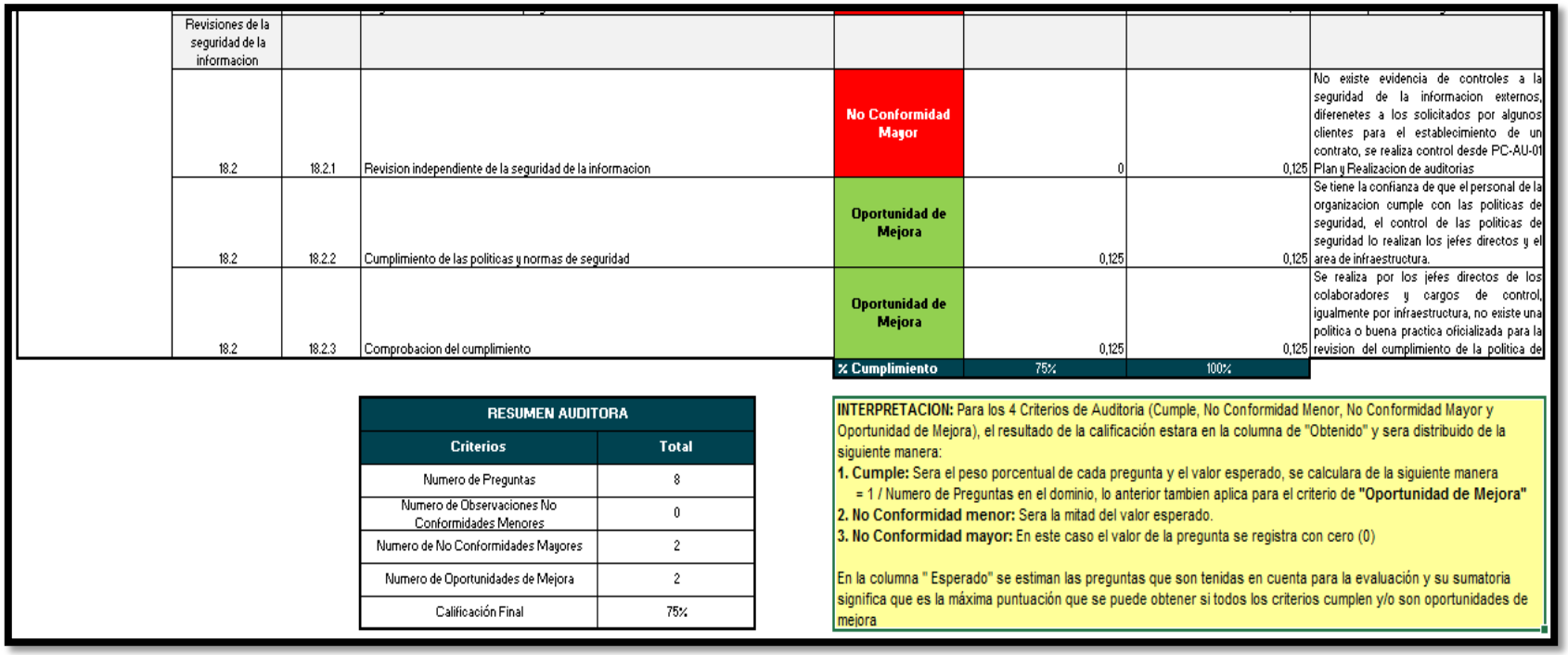
Nombre de los Auditores
Javier Olivo Garcia A.

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
18. Cumplimiento	Cumplimiento de los requisitos legales y						
	18.1	18.1.1	Identificacion de la legislacion aplicable	Cumple	0,125	0,125	Se tienen clara la legislacion nacional Colombiana para la constitucion de organizacione sinformaticas, igualmente la matetria que rige el area de seguridad informatica y normas relacionadas como la ley 1273 de 2009, ley 1581 de 2012 y ley 1712 de 2014
	18.1	18.1.2	Derechos de propiedad intelectual	Cumple	0,125	0,125	Se evidencia la existencia de clausulas de respeto a la propiedad intelectual en las contrataciones con terceros, igualmente la organizacion la estimula en sus colaboradores y realiza control sobre el
	18.1	18.1.3	Proteccion de los registros de la organizacion	Cumple	0,125	0,125	Existen las politicas, metodologias y practicas que garantizan la proteccion de la infomacion de la organizacion, en fisico a traves del owner del activo y en digital a traves del repositorio y los respectivos back
	18.1	18.1.4	Proteccion de los datos y privacidad de la informacion personal	Cumple	0,125	0,125	Se evidencia una politica de respeto a la privacidad de los colaboradores y clientes, se tiene identificada la legislacion aplicable en caso particular de la ley 1581 de 2012
	18.1	18.1.5	Regulacion de los controles criptograficos	No Conformidad Mayor	0	0,125	No se evidencia la existencia de controles criptograficos a nivel organizacional, no existe una politica ni codigo de buenas
	Revisiones de la seguridad de la informacion						

Continúa…

Fig 21. Listados de auditoria, Dominio 18 (Continuación)



	Revisiones de la seguridad de la informacion					
	18.2	18.2.1	Revision independiente de la seguridad de la informacion	No Conformidad Mayor	0	0,125	No existe evidencia de controles a la seguridad de la informacion externos, diferenetes a los solicitados por algunos clientes para el establecimiento de un contrato, se realiza control desde PC-AU-01 Plan y Realizacion de auditorias
	18.2	18.2.2	Cumplimiento de las politicas y normas de seguridad	Oportunidad de Mejora	0,125	0,125	Se tiene la confianza de que el personal de la organizacion cumple con las politicas de seguridad, el control de las politicas de seguridad lo realizan los jefes directos y el area de infraestructura.
	18.2	18.2.3	Comprobacion del cumplimiento	Oportunidad de Mejora	0,125	0,125	Se realiza por los jefes directos de los colaboradores y cargos de control, igualmente por infraestructura, no existe una politica o buena practica oficializada para la revision del cumplimiento de la politica de
				% Cumplimiento	75%	100%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	8
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	2
Numero de Oportunidades de Mejora	2
Calificación Final	75%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Fuente: I&T Stefanini.

12.2.4 Hoja de Hallazgos

Fig 22. Hoja de Hallazgos

HOJA DE HALLAZGOS									
FECHA AUDITORIA:	18 Abril 2016 al 19 de Abril 2016								
Nro.	Código	Proceso Auditado	Clausula 27001:2013	Descripción del control	Responsable	Clasificación	Detalle	Tipo No Conformidad U-No usa M-Mal uso O-Oportunidad de mejora	Auditor
1	6.1	Desarrollo de software	6.1.1	Conjunto de politicas para la seguridad de la informacion	Gerente de Fabricas Continuas	**Oportunidad de Mejora**	La organinzacion cuenta con un documento de politicas de seguridad que es conocido por todos los procesos de la organizacion.	O	Javier Garcia
2	6.1	Desarrollo de software	6.1.2	Segregacion de tareas	Gerente de Fabricas Continuas	**Oportunidad de Mejora**	Las tareas de seguridad de la informacion se asignan a los gerentes y coordinadores de cada proyecto, adicionalmente el area de infraestructura asigna y monitorea el acceso y uso de los recursos, y el area de control de operaciones ejerce vigilancia; no existe la figura de CIO o responsible de seguridad de la informacion en la organizacion a nivel Colombia	O	Javier Garcia
3	6.1	Desarrollo de software	6.1.5	Seguridad de la informacion en la gestion de proyectos.	Gerente de Fabricas Continuas	**No Conformidad Menor**	Se pueden apreciar debilidades en los controles de seguridad de la informacion debido a que la gestion de la misma en cada proyecto solamente es realizada ocasionalmente por el gerente de proyecto quien se fundamenta que los controles de seguridad los ejerce de manera logica el area de infraestructura, no existe evidencia de los controles realizados de manera periodica o constante ya que muchas veces depende del cliente del proyecto.	M	Javier Garcia
4	6.2	Desarrollo de software	6.2.2	Teletrabajo	Gerente de Fabricas Continuas	**Oportunidad de Mejora**	Existe una politica de teletrabajo y trabajo flexible, sin embargo no se implementa ya que actualmemnte no se realiza teletrabajo en ningun proyecto.	O	Javier Garcia
5	7.1	Desarrollo de software	7.1.1	Investigacion de antecedentes antes de la contratacion.	Gerente de Fabricas Continuas	**Oportunidad de Mejora**	En la organizacion existe un protocolo de reclutamiento y seleccion del personal, sin embargo solo se llevan a cabo estudios de seguridad cuando el proyecto del cliente asi lo requiere o cuando existe solicitud expresa del cliente.	O	Javier Garcia
6	7.2	Desarrollo de software	7.2.2	Concienciacion, educacion y capacitacion en la seguridad de la inforormacion	Gerente de Fabricas Continuas	**No Conformidad Mayor**	NO se evidencia la existencia de programas o campañas de promocion de la seguridad de la informacion en la organización	U	Javier Garcia

Continúa…

Fig 22. Hoja de Hallazgos (Continuación)

HOJA DE HALLAZGOS

FECHA AUDITORIA:	18 Abril 2016 al 19 de Abril 2016

Nro.	Código	Proceso Auditado	Clausula 27001:2013	Descripción del control	Responsable	Clasificación	Detalle	Tipo No Conformidad U-No usa M-Mal uso O-Oportunidad de mejora	Auditor
7	7.3	Desarrollo de software	7.3.1	Cese o Cambio de puesto de trabajo	Gerente de Fabricas Continuas	**No Conformidad Menor**	Existe un procedimiento de informe al area de infraestructura , sin embargo se evidencian periodos prolongados en la inactivacion de cuentas por retiros y el cambio de permisos y privilegios por movimientos de personal, este tiempo muerto se presenta por demoras en la notificacion de RRHH a Infraestructura	M	Javier Garcia
8	8.2	Desarrollo de software	8.2.2	Etiquetado y Manipulado de la Informacion	Coordinador de fabricas continuas	**No Conformidad Menor**	Se evidencia que no toda la informacion es correctamente etiquetada segun la politica de seguridad y la matriz LI-RD-08, encontrandose documentacion sensible y sin catalogar expuesta	M	Javier Garcia
9	8.2	Desarrollo de software	8.2.3	Manipulacion de Activos	Coordinador de fabricas continuas	**No Conformidad Menor**	Se evidencia que en algunas estaciones de trabajo de los desarrolladores se permite el uso de pendrives y usb que representan riesgos de hurto de la informacion.	M	Javier Garcia
10	8.3	Desarrollo de software	8.3.2	Eliminacion de Soportes	Coordinador de fabricas continuas	**No Conformidad Mayor**	No se evidencia un procedimiento seguro de eliminacion de la informacion en soportes logicos.	U	Javier Garcia
11	8.3	Desarrollo de software	8.3.3	Soportes Fisicos en transito	Coordinador de fabricas continuas	**No Conformidad Mayor**	No se evidencia un procedimeinto para el manejo seguro de los soportes fisicos hardware cuando son movilizados de mun area a otra.	U	Javier Garcia
12	9.2	Desarrollo de software	9.2.1	Gestion de altas y Bajas en el registro de usuarios	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Menor**	Se encuentra una politica clara para la gestion de altas y bajas de usuarios que se retiran de la organizacion y los traslados o movimientos de personal, sin embargo se puede evidenciar que los tiempos de respuesta para la baja y modificacion de los privilegios de un usuario no son inmediatos a su notificacion.	M	Javier Garcia
13	9.2	Desarrollo de software	9.2.6	Retirada o adaptacion de los derechos de acceso	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Menor**	Se evidenci la existencia de la politica de cambio d eprivilegios y control de accesos para los traslados o movimientyos de personal, se evidencia la gestion correcta por el area de infraestructura, sin embargo el retiro y adaptacion de privilegios no se realiza inmediatamente se sinforma por parte d ela gerencia a cargo.	M	Javier Garcia

Continúa…

Fig 22. Hoja de Hallazgos (Continuación)

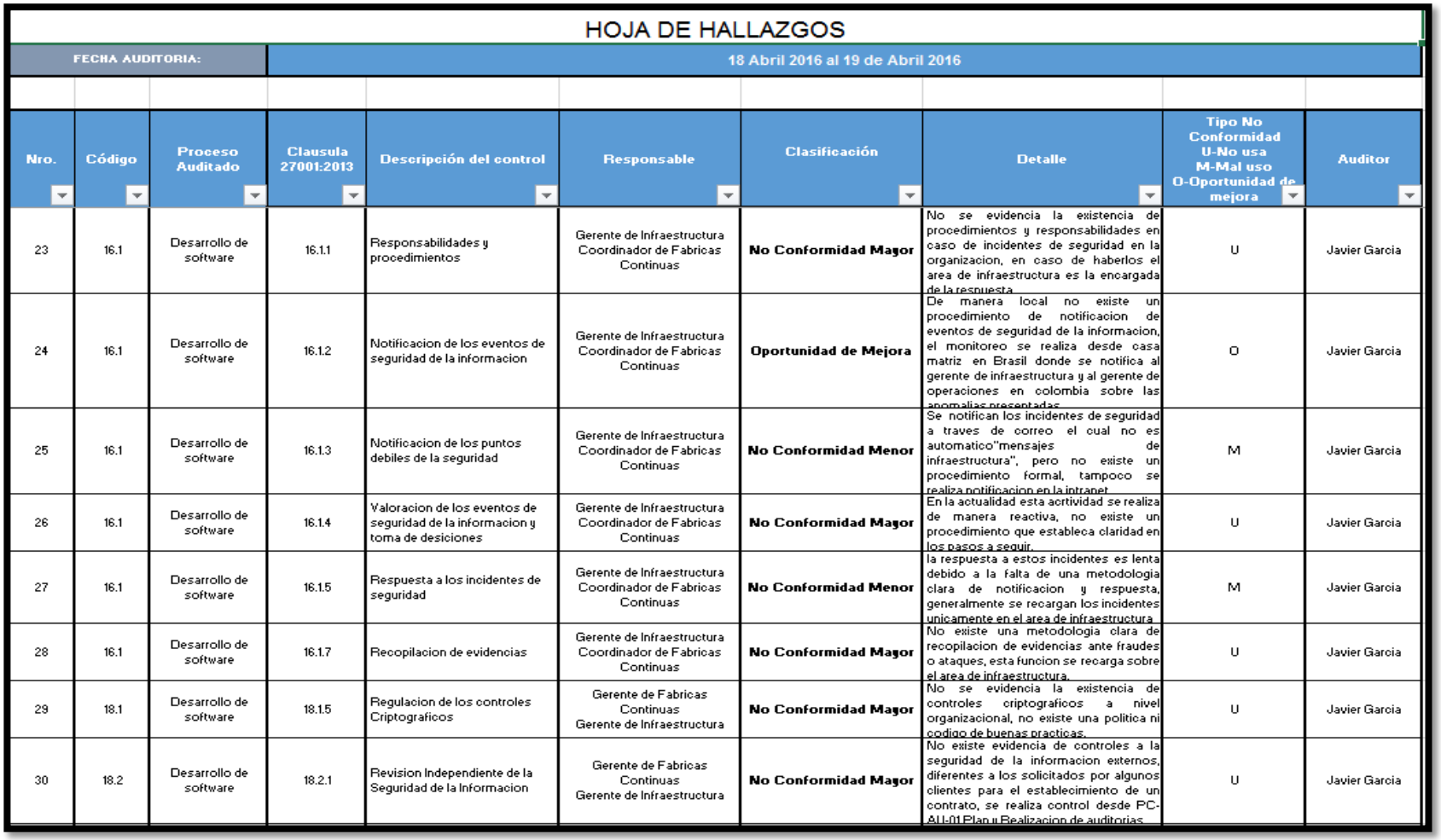
HOJA DE HALLAZGOS

FECHA AUDITORIA:	18 Abril 2016 al 19 de Abril 2016

Nro.	Código	Proceso Auditado	Clausula 27001:2013	Descripción del control	Responsable	Clasificación	Detalle	Tipo No Conformidad U-No usa M-Mal uso O-Oportunidad de mejora	Auditor
14	10.1	Desarrollo de software	10.1.1	Politica de uso de controles criptograficos	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No se evidencia el uso de aplicaciones de encriptamiento ni certificados digitales con los cuales administrar la informacion y el encriptamiento de la misma permitiendo riesgos de consulta no autorizados.	U	Javier Garcia
15	10.1	Desarrollo de software	10.1.2	Gestion de claves	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	NO existe configuracion del servicio Active Directory Certificate Service para la gestion de certificados digitales y sus claves.	U	Javier Garcia
16	11.1	Desarrollo de software	11.1.1	Perimetro de Seguridad Fisica	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	Se evidencia que la fabrica de software ubicada en la sede principal calle 122 no dispone de aislamiento del resto de areas operativas u administrativas.	U	Javier Garcia
17	11.1	Desarrollo de software	11.1.2	Controles Fisicos en la entrada	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No se evidencian controles fisicol o logicos para el acceso a la fabrica de software	U	Javier Garcia
18	11.1	Desarrollo de software	11.1.3	Seguridad de Oficinas, despachos y recursos	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se evidencia que en las instalaciones en las que funciona la fabrica de sofware se dispone de CCTV conectados al area de seguridad del edificio, sin embargo esta vigilancia deberia ser propia de la organizacion	O	Javier Garcia
19	11.2	Desarrollo de software	11.2.7	Reutilizacion o retirada segura de dispositivos de almacenamiento	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No se evidencian controles o procedimientos de borrado o eliminacion de activos que almacenan informacion de la organización o sus	U	Javier Garcia
20	11.2	Desarrollo de software	11,2,8	Equipo informatico de usuario desatendido	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se evidencia la correcta gestion de los incidentes presentados por los usuarios a traves del servicedesk, por esta razon no se encuentran estaciones desatendidas al momento de la auditoria	O	Javier Garcia
21	12.1	Desarrollo de software	12.1.4	Separacion de entornos de desarrollo, prueba y produccion	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	En la sede principal de la organización no se encuentran diferenciados los entornos de desarrollo, prueba y	U	Javier Garcia
22	14.2	Desarrollo de software	14.2.7	Externanilzacion del desarrollo de Software	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se omite ya que la organizacion no externaliza el desarrollo de software, este se realiza inhouse por las fabricas internas, sin embargo se debe generar una politica de desarrollo con externos.	O	Javier Garcia

Continúa…

Fig 22. Hoja de Hallazgos (Continuación)



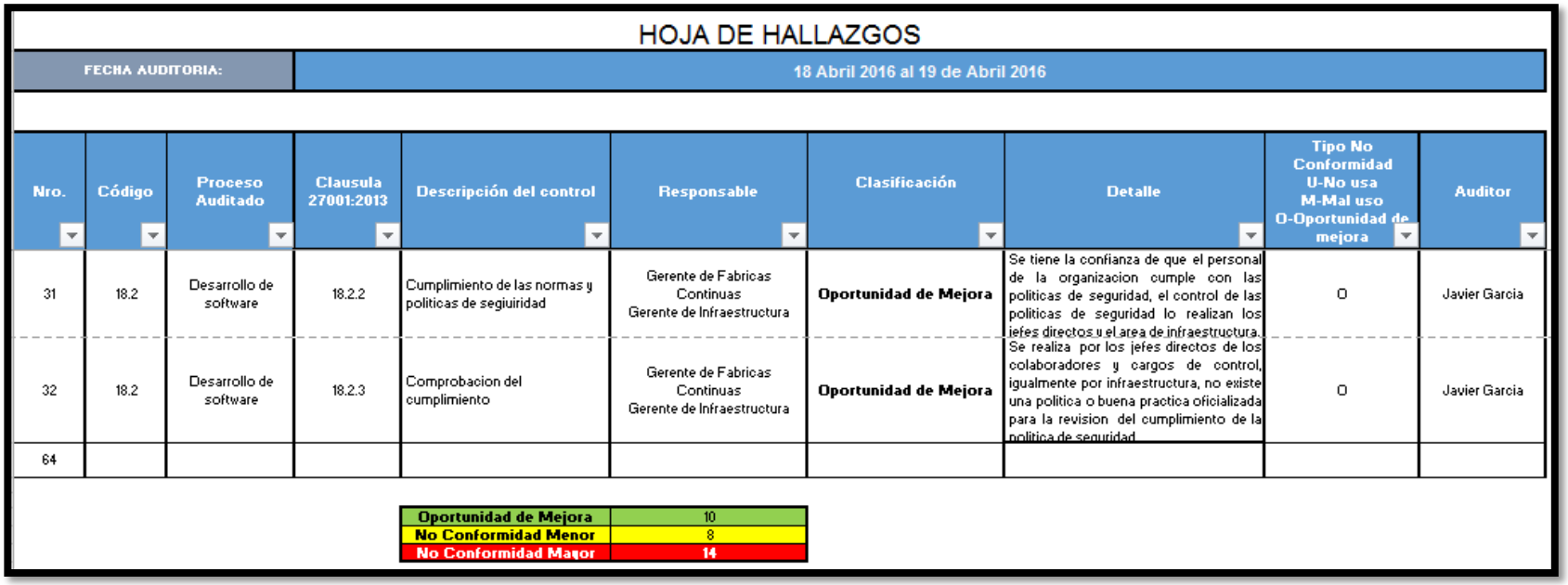
HOJA DE HALLAZGOS

FECHA AUDITORIA:	18 Abril 2016 al 19 de Abril 2016

Nro.	Código	Proceso Auditado	Clausula 27001:2013	Descripción del control	Responsable	Clasificación	Detalle	Tipo No Conformidad U-No usa M-Mal uso O-Oportunidad de mejora	Auditor
23	16.1	Desarrollo de software	16.1.1	Responsabilidades y procedimientos	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Mayor**	No se evidencia la existencia de procedimientos y responsabilidades en caso de incidentes de seguridad en la organizacion, en caso de haberlos el area de infraestructura es la encargada de la respuesta	U	Javier Garcia
24	16.1	Desarrollo de software	16.1.2	Notificacion de los eventos de seguridad de la informacion	Gerente de Infraestructura Coordinador de Fabricas Continuas	**Oportunidad de Mejora**	De manera local no existe un procedimiento de notificacion de eventos de seguridad de la informacion, el monitoreo se realiza desde casa matriz en Brasil donde se notifica al gerente de infraestructura y al gerente de operaciones en colombia sobre las anomalias presentadas	O	Javier Garcia
25	16.1	Desarrollo de software	16.1.3	Notificacion de los puntos debiles de la seguridad	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Menor**	Se notifican los incidentes de seguridad a traves de correo el cual no es automatico"mensajes de infraestructura", pero no existe un procedimiento formal, tampoco se realiza notificacion en la intranet	M	Javier Garcia
26	16.1	Desarrollo de software	16.1.4	Valoracion de los eventos de seguridad de la informacion y toma de desiciones	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Mayor**	En la actualidad esta acrtividad se realiza de manera reactiva, no existe un procedimiento que estableca claridad en los pasos a seguir.	U	Javier Garcia
27	16.1	Desarrollo de software	16.1.5	Respuesta a los incidentes de seguridad	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Menor**	la respuesta a estos incidentes es lenta debido a la falta de una metodologia clara de notificacion y respuesta, generalmente se recargan los incidentes unicamente en el area de infraestructura	M	Javier Garcia
28	16.1	Desarrollo de software	16.1.7	Recopilacion de evidencias	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Mayor**	No existe una metodologia clara de recopilacion de evidencias ante fraudes o ataques, esta funcion se recarga sobre el area de infraestructura.	U	Javier Garcia
29	18.1	Desarrollo de software	18.1.5	Regulacion de los controles Criptograficos	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No se evidencia la existencia de controles criptograficos a nivel organizacional, no existe una politica ni codigo de buenas practicas.	U	Javier Garcia
30	18.2	Desarrollo de software	18.2.1	Revision Independiente de la Seguridad de la Informacion	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No existe evidencia de controles a la seguridad de la informacion externos, diferentes a los solicitados por algunos clientes para el establecimiento de un contrato, se realiza control desde PC-AU-01 Plan y Realizacion de auditorias	U	Javier Garcia

Continúa…

Fig 22. Hoja de Hallazgos (Continuación)



HOJA DE HALLAZGOS

FECHA AUDITORIA:	18 Abril 2016 al 19 de Abril 2016

Nro.	Código	Proceso Auditado	Clausula 27001:2013	Descripción del control	Responsable	Clasificación	Detalle	Tipo No Conformidad U-No usa M-Mal uso O-Oportunidad de mejora	Auditor
31	18.2	Desarrollo de software	18.2.2	Cumplimiento de las normas y politicas de segiuridad	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se tiene la confianza de que el personal de la organizacion cumple con las politicas de seguridad, el control de las politicas de seguridad lo realizan los jefes directos u el area de infraestructura.	O	Javier Garcia
32	18.2	Desarrollo de software	18.2.3	Comprobacion del cumplimiento	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se realiza por los jefes directos de los colaboradores y cargos de control, igualmente por infraestructura, no existe una politica o buena practica oficializada para la revision del cumplimiento de la politica de seguridad	O	Javier Garcia
64									

Oportunidad de Mejora	10
No Conformidad Menor	8
No Conformidad Mayor	14

Fuente: I&T Stefanini

12.2.5 Informe De Auditoria

06 DE MAYO DE 2016

Gerencia de Calidad y operaciones Colombia

Calle 122 No 23-46 piso 5, Bogotá D.C- Colombia.

Sres. Directivos:

En el presente documento encontraran el Informe final de la auditoría realizada al proceso Desarrollo de Software que tuvo lugar desde el 18 de abril de 2016 al 29 de abril de 2016, contando con el apoyo de las gerencias de Calidad y Operaciones, Recursos Humanos, Infraestructura y Fábrica de Software. Esta auditoria había sido anunciada desde el mes de octubre de 2015 y autorizada por la Gerencia de Calidad y Operaciones en nombre de la Ing. Luz Marina Motta Beltrán mediante carta de aprobación dirigida al Ing. Javier Olivo Garcia Araque con registro Profesional 25255-308521 CND quien desarrolla su proyecto de grado para la Universidad Nacional Abierta y a Distancia – UNAD Como especialista en seguridad informática.

Datos generales

Fechas de la auditoria:

18 al 29 de abril 2016.

Tipo de Auditoria:

Interna

Criterios Aplicados:

Norma NTC ISO-IEC 27001:2013

CMMI® V1.3 2011

Cliente de Auditoria:

Fábrica de software I&T Stefanini Colombia.

Objetivo de la Auditoria:

Verificar el cumplimiento de los objetivos de control de la norma ISO 27002:2013

Alcance de la Auditoria:

Proceso de Desarrollo de Software.

Metodología

Para llevar a cabo la auditoria de seguridad de la información 2016-I y con el objetivo de evidenciar los controles que se cumplen, los que presentan fallas y los que no se están cumpliendo de acuerdo a la norma NTC ISO-IEC 27001:2013, el auditor tuvo en cuenta la siguiente metodología.

- **Visita in Situ**

El auditor realizo varias visitas a la Fábrica de Software ubicada en la calle 122 con autopista, piso 6 donde funciona la sede principal en Colombia con el objetivo de verificar los procedimientos de operación del área respecto al sistema de gestión de seguridad actual.

- **Revisión de la documentación de seguridad de la información**

El auditor solicito y reviso la documentación existente en la organización respecto a la gestión de la seguridad de la información verificando el manual de políticas de seguridad de la información, el plan de continuidad y el plan de recuperación de desastres, entre otros planes de seguridad relacionados con aplicaciones y equipos especiales que no se incluyen de manera precisa en los 79 artículos del manual de seguridad de la información, de la misma manera reviso los estándares que se cumplen en el proceso de desarrollo de software para analizar su relación con la seguridad de la información

- **Entrevistas con desarrolladores de algunas fábricas de software**

El Auditor realizo entrevistas específicas a algunos de los desarrolladores para explorar la conciencia de seguridad de la información en la operación diaria, igualmente en estas entrevistas se busca el conocimiento de los desarrolladores acerca de los estándares y normas que gobiernan el área.

- **Cuestionarios con líderes del proceso**

El auditor diseño una lista de cuestionarios que diligencio en compañía de los líderes del proceso y procesos relacionados, estos listados serán los que arrojen una imagen cuantitativa del estado de la seguridad de la información respecto a la norma NTC ISO-IEC 27001:2013.

También se validó el último resultado de evaluación SCAMPI relacionada con las 22 áreas de proceso de CMMI V1.3 2011 que certifican en nivel 3 el desarrollo de software.

- **Resultados**

Los resultados de las actividades anteriores se plasman en los listados de auditoria los cuales se anexan a este documento y se detallan en el presente informe final de auditoria, destacando de los 114 controles evaluados correspondientes a la norma NTC ISO-IEC 27002:2013 los siguientes detalles.

Tabla 2. Controles evaluados, norma NTC ISO-IEC 27002:2013

Controles Conformes	82
Oportunidad de Mejora	10
No Conformidad Menor	8
No Conformidad Mayor	**14**
Controles Evaluados	**114**

Fuente: El Autor

El porcentaje de cumplimiento por cada uno de los 14 dominios de la norma NTC ISO-IEC 27001:2013 es el siguiente:

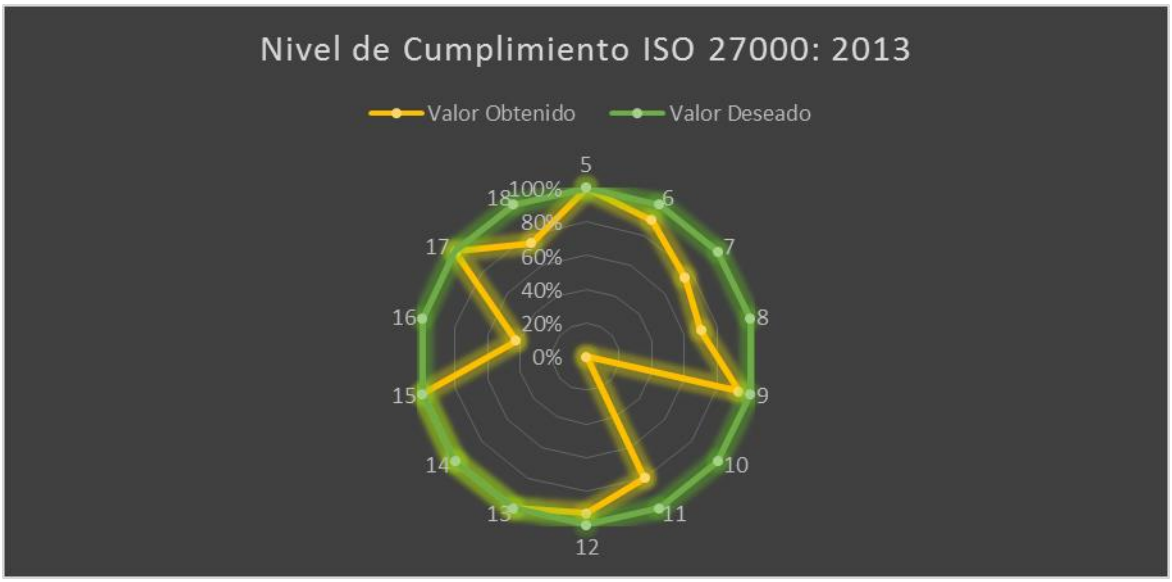
Tabla 3. Cumplimiento porcentual ISO 27001:2013

DOMINIO	VALOR OBTENIDO	VALOR DESEADO
5	100%	100%
6	90%	100%
7	75%	100%
8	70%	100%
9	93%	100%
10	0%	100%
11	80%	100%
12	93%	100%
13	100%	100%
14	100%	100%
15	100%	100%
16	43%	100%
17	100%	100%
18	75%	100%
Average	80%	

Fuente: el autor.

Que en la gráfica se representa de la siguiente manera:

Fig. 23. Nivel de cumplimiento ISO 27001:2013.



Fuente: El Autor

Teniendo como un promedio general el 80% del cumplimiento de los controles en el proceso auditado.

Se comentan detalladamente en este informe los controles que de una u otra manera no se encuentran conformes por considerar que se debe enfatizar en llevarlos al área de conformidad.

No conformidad Mayores

Fig. 24. no conformidades Mayores.

Nro.	Código	Proceso Auditado	Clausula 27001:2013	Descripción del control	Responsable	Clasificación	Detalle	Tipo No Conformidad U-No usa M-Mal uso O-Oportunidad de mejora	Auditor
6	7.2	Desarrollo de software	7.2.2	Concienciacion, educacion y capacitacion en la seguridad de la inforormacion	Gerente de Fabricas Continuas	**No Conformidad Mayor**	NO se evidencia la existencia de programas o campañas de promocion de la seguridad de la informacion en la organización	U	Javier Garcia
10	8.3	Desarrollo de software	8.3.2	Eliminacion de Soportes	Coordinador de fabricas continuas	**No Conformidad Mayor**	No se evidencia un procedimiento seguro de eliminacion de la informacion en soportes logicos.	U	Javier Garcia
11	8.3	Desarrollo de software	8.3.3	Soportes Fisicos en transito	Coordinador de fabricas continuas	**No Conformidad Mayor**	No se evidencia un procedimeinto para el manejo seguro de los soportes fisicos hardware cuando son movilizados de mun area a otra.	U	Javier Garcia
14	10.1	Desarrollo de software	10.1.1	Politica de uso de controles criptograficos	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No se evidencia el uso de aplicaciones de encriptamiento ni certificados digitales con los cuales administrar la informacion y el encriptamiento de la misma permitiendo riesgos de consulta no autorizados.	U	Javier Garcia
15	10.1	Desarrollo de software	10.1.2	Gestion de claves	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	NO existe configuracion del servicio Active Directory Certificate Service para la gestion de certificados digitales y sus claves.	U	Javier Garcia
16	11.1	Desarrollo de software	11.1.1	Perimetro de Seguridad Fisica	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	Se evidencia que la fabrica de software ubicada en la sede principal calle 122 no dispone de aislamiento del resto de areas operativas y administrativas.	U	Javier Garcia
17	11.1	Desarrollo de software	11.1.2	Controles Fisicos en la entrada	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No se evidencian controles fisicol o logicos para el acceso a la fabrica de software	U	Javier Garcia
21	12.1	Desarrollo de software	12.1.4	Separacion de entornos de desarrollo, prueba y produccion	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	En la sede principal de la organización no se encuentran diferenciados los entornos de desarrollo, prueba y produccion.	U	Javier Garcia
23	16.1	Desarrollo de software	16.1.1	Responsabilidades y procedimientos	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Mayor**	No se evidencia la existencia de procedimientos y responsabilidades en caso de incidentes de seguridad en la organizacion, en caso de haberlos el area de infraestructura es la encargada de la respuesta.	U	Javier Garcia
26	16.1	Desarrollo de software	16.1.4	Valoracion de los eventos de seguridad de la informacion y toma de desiciones	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Mayor**	En la actualidad esta acrtividad se realiza de manera reactiva, no existe un procedimiento que estableca claridad en los pasos a seguir.	U	Javier Garcia
28	16.1	Desarrollo de software	16.1.7	Recopilacion de evidencias	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Mayor**	No existe una metodologia clara de recopilacion de evidencias ante fraudes o ataques, esta funcion se recarga sobre el area de infraestructura.	U	Javier Garcia
29	18.1	Desarrollo de software	18.1.5	Regulacion de los controles Criptograficos	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No se evidencia la existencia de controles criptograficos a nivel organizacional, no existe una politica ni codigo de buenas practicas.	U	Javier Garcia
30	18.2	Desarrollo de software	18.2.1	Revision Independiente de la Seguridad de la Informacion	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No existe evidencia de controles a la seguridad de la informacion externos, diferentes a los solicitados por algunos clientes para el establecimiento de un contrato, se realiza control desde PC-AU-01 Plan y Realizacion de auditorias	U	Javier Garcia

Fuente: I&T Stefanini

No Conformidad Menores

Fig. 25. no Conformidades Menores.

Nro.	Código	Proceso Auditado	Clausula 27001:2013	Descripción del control	Responsable	Clasificación	Detalle	Tipo No Conformidad U-No usa M-Mal uso O-Oportunidad de mejora	Auditor
3	6.1	Desarrollo de software	6.1.5	Seguridad de la informacion en la gestion de proyectos.	Gerente de Fabricas Continuas	**No Conformidad Menor**	Se pueden apreciar debilidades en los controles de seguridad de la informacion debido a que la gestion de la misma en cada proyecto solamente es realizada ocasionalmente por el gerente de proyecto quien se fundamenta que los controles de seguridad los ejerce de manera logica el area de infraestructura, no existe evidencia de los controles realizados de manera periodica o constante ya que muchas veces depende del cliente del proyecto.	M	Javier Garcia
7	7.3	Desarrollo de software	7.3.1	Cese o Cambio de puesto de trabajo	Gerente de Fabricas Continuas	**No Conformidad Menor**	Existe un procedimiento de informe al area de infraestructura , sin embargo se evidencian periodos prolongados en la inactivacion de cuentas por retiros y el cambio de permisos y privilegios por movimientos de personal, este tiempo muerto se presenta por demoras en la notificacion de RRHH a Infraestructura.	M	Javier Garcia
8	8.2	Desarrollo de software	8.2.2	Etiquetado y Manipulado de la Informacion	Coordinador de fabricas continuas	**No Conformidad Menor**	Se evidencia que no toda la informacion es correctamente etiquetada segun la politica de seguridad y la matriz LI-RD-08, encontrandose documentacion sensible y sin catalogar expuesta	M	Javier Garcia
9	8.2	Desarrollo de software	8.2.3	Manipulacion de Activos	Coordinador de fabricas continuas	**No Conformidad Menor**	Se evidencia que en algunas estaciones de trabajo de los desarrolladores se permite el uso de pendrives y usb que representan riesgos de hurto de la informacion.	M	Javier Garcia
12	9.2	Desarrollo de software	9.2.1	Gestion de altas y Bajas en el registro de usuarios	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Menor**	Se encuentra una politica clara para la gestion de altas y bajas de usuarios que se retiran de la organizacion y los traslados o movimientos de personal, sin embargo se puede evidenciar que los tiempos de respuesta para la baja y modificacion de los privilegios de un usuario no son inmediatos a su notificacion.	M	Javier Garcia
13	9.2	Desarrollo de software	9.2.6	Retirada o adaptacion de los derechos de acceso	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Menor**	Se evidenci la existencia de la politica de cambio d eprivilegios y control de accesos para los traslados o movimientyos de personal, se evidencia la gestion correcta por el area de infraestructura, sin embargo el retiro y adaptacion de privilegios no se realiza inmediatamente se sinforma por parte d ela gerencia a cargo.	M	Javier Garcia
25	16.1	Desarrollo de software	16.1.3	Notificacion de los puntos debiles de la seguridad	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Menor**	Se notifican los incidentes de seguridad a traves de correo el cual no es automatico"mensajes de infraestructura", pero no existe un procedimiento formal, tampoco se realiza notificacion en la intranet corporativa.	M	Javier Garcia

Fuente: I&T Stefanini

Oportunidades de Mejora.

Fig. 26 Oportunidades de mejora.

Nro.	Código	Proceso Auditado	Clausula 27001:2013	Descripción del control	Responsable	Clasificación	Detalle	Tipo No Conformidad U-No usa M-Mal uso O-Oportunidad de mejora	Auditor
1	6.1	Desarrollo de software	6.1.1	Conjunto de politicas para la seguridad de la informacion	Gerente de Fabricas Continuas	**Oportunidad de Mejora**	La organinzacion cuenta con un documento de politicas de seguridad que es conocido por todos los procesos de la organizacion.	O	Javier Garcia
2	6.1	Desarrollo de software	6.1.2	Segregacion de tareas	Gerente de Fabricas Continuas	**Oportunidad de Mejora**	Las tareas de seguridad de la informacion se asignan a los gerentes y coordinadores de cada proyecto, adicionalmente el area de infraestructura asigna y monitorea el acceso y uso de los recursos, y el area de control de operaciones ejerce vigilancia; no existe la figura de CIO o responsible de seguridad de la informacion en la organizacion a nivel Colombia	O	Javier Garcia
4	6.2	Desarrollo de software	6.2.2	Teletrabajo	Gerente de Fabricas Continuas	**Oportunidad de Mejora**	Existe una politica de teletrabajo y trabajo flexible, sin embargo no se implementa ya que actualmemnte no se realiza teletrabajo en ningun proyecto.	O	Javier Garcia
5	7.1	Desarrollo de software	7.1.1	Investigacion de antecedentes antes de la contratacion.	Gerente de Fabricas Continuas	**Oportunidad de Mejora**	En la organizacion existe un protocolo de reclutamiento y seleccion del personal, sin embargo solo se llevan a cabo estudios de seguridad cuando el proyecto del cliente asi lo requiere o cuando existe solicitud expresa del cliente.	O	Javier Garcia
18	11.1	Desarrollo de software	11.1.3	Seguridad de Oficinas, despachos y recursos	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se evidencia que en las instalaciones en las que funciona la fabrica de sofware se dispone de CCTV conectados al area de seguridad del edificio, sin embargo esta vigilancia deberia ser propia de la organizacion.	O	Javier Garcia
20	11.2	Desarrollo de software	11,2,8	Equipo informatico de usuario desatendido	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se evidencia la correcta gestion de los incidentes presentados por los usuarios a traves del servicedesk, por esta razon no se encuentran estaciones desatendidas al momento de la auditoria	O	Javier Garcia
22	14.2	Desarrollo de software	14.2.7	Externanilzacion del desarrollo de Software	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se omite ya que la organizacion no externaliza el desarrollo de software, este se realiza inhouse por las fabricas internas, sin embargo se debe generar una politica de desarrollo con externos.	O	Javier Garcia
24	16.1	Desarrollo de software	16.1.2	Notificacion de los eventos de seguridad de la informacion	Gerente de Infraestructura Coordinador de Fabricas Continuas	**Oportunidad de Mejora**	De manera local no existe un procedimiento de notificacion de eventos de seguridad de la informacion, el monitoreo se realiza desde casa matriz en Brasil donde se notifica al gerente de infraestructura y al gerente de operaciones en colombia sobre las anomalias presentadas.	O	Javier Garcia
31	18.2	Desarrollo de software	18.2.2	Cumplimiento de las normas y politicas de segiuiridad	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se tiene la confianza de que el personal de la organizacion cumple con las politicas de seguridad, el control de las politicas de seguridad lo realizan los jefes directos y el area de infraestructura.	O	Javier Garcia

Fuente: I&T Stefanini

- **Conclusiones**

A nivel general se puede diagnosticar un cumplimiento intermedio de los requisitos de la norma NTC ISO IEC 27001:2013 en la organización, esto debido a que las NO conformidades encontradas pesan bastante sobre el sistema de gestión de seguridad de la información al referirse específicamente a los controles criptográficos, separación de áreas de desarrollo, prueba y producción, valoración de los incidentes de seguridad de la información y la revisión independiente del sistema de gestión de seguridad que garantizan la integridad, confidencialidad y disponibilidad de los sistemas de información.

Aunque la tabla anteriormente expuesta nos muestre un cumplimiento promedio del 80%, la realidad es que esta solamente es la vista cuantitativa, al tener en cuenta la vista cualitativa el porcentaje de cumplimiento desciende alrededor del 50 % y si se tienen en cuenta dominios de seguridad de la información como el 10. Controles Criptográficos y el 16 Gestión de incidentes de la seguridad de la información el porcentaje de cumplimiento desciende incluso por debajo del 50% mereciendo una atención especial por parte de los líderes del área, procesos relacionados y los directivos de la organización.

Actualmente la mayoría de actividades de seguridad de la informática recaen sobre el área de infraestructura que tienen entre otras, la responsabilidad de velar por la seguridad de la información.

El entorno de desarrollo presenta fuertes debilidades respecto a la seguridad de la información que allí se trabaja, al no estar separadas estas áreas y aisladas de otras áreas administrativas de la organización los riesgos de modificación, pérdida o robo de la información tienden a aumentar y si a esto se le suma la confianza de los líderes del proceso en lugar de un control estandarizado los resultados pueden ser catastróficos para la organización y para sus clientes.

La inexistencia de políticas y controles criptográficos que se reflejen en comunicación encriptada, infraestructuras PKI, comunicaciones y enlaces seguros expone la información de la organización a riesgos innecesarios que se convierten en vulnerabilidades de la información.

La falta de normas y políticas que establezcan procedimientos claros de recopilación de evidencias puede dar lugar a que incidentes de seguridad ocasionados por individuos dentro o fuera de la organización no puedan ser correctamente documentados y reseñados para posteriormente ser judicializados por las autoridades en Colombia, dando lugar a que estas conductas queden impunes y la imagen de la organización se desvalorice.

La falta de concienciación y capacitación en seguridad de la información, así como la falta de un procedimiento de revisión independiente de la seguridad de la información entorpece la evolución del sistema de gestión de seguridad de la información ocasionando entropía y haciendo el sistema lento ante posibles amenazas o vulnerabilidades que puedan aparecer en el medio.

Las no conformidades menores detalladas en este reporte tienen menor peso cuantitativo que una no conformidad mayor, sin embargo, también dan lugar a vulnerabilidades que pueden ser explotadas por agentes internos y externos, y de la misma manera califica en sistema como no apto para una certificación por organismo competente.

Las no conformidades solo se catalogan como Mayores o Menores en una auditoria interna, en una auditoria externa de certificación o recertificación una no conformidad tiene en ambos casos la misma importancia inhabilitando el sistema completo para poder ser certificado.

Las no conformidades mayores para este informe se describen como controles reglamentarios para la norma NTC ISO-IEC 27001:2013 que no existen en la organización; las no conformidades menores corresponden a controles establecidos pero que no se están llevando a cabo de manera correcta.

Respecto a las opciones de mejora detalladas estás corresponden a controles de la norma NTC ISO-IEC 27001:2013 que se están llevando a cabo de manera correcta pero que aún se pueden optimizar para mejorar sus resultados.

EL levantamiento de las no conformidades y aplicación de oportunidades de mejora corresponde a los líderes de proceso de cada área quienes serán los responsables de analizar la causa raíz de cada no conformidad y presentar al auditor en un plazo no mayor a 20 días posterior a la detección de la no conformidad un plan de mejora que de origen a la mitigación de la no conformidad y permita aumentar la confiabilidad del sistema de gestión de seguridad de la información, en este caso el auditor interno o auditor líder, o responsable de calidad y operaciones serán los únicos que podrán validar la no conformidad como gestionada y conforme de acuerdo a la norma NTC ISO IEC 27001:2013.

- **Recomendaciones**

Se recomienda la inversión en personal capacitado en Seguridad de la Información de manera Local en Colombia el cual tenga a cargo las actividades de seguridad, apoyo a infraestructura, recursos humanos y el área jurídica las cuales se encuentran estrechamente relacionadas en la operación segura de un Sistema de gestión de seguridad en cualquier organización.

Se recomienda a la dirección establecer una estrategia de promoción de la seguridad de la información, esta estrategia debe abordar todas las áreas de la organización desde el momento de la vinculación de personal, promoción a través de los medios institucionales, cursos virtuales, intranet, correo electrónico y posters ubicados en sitios estratégicos, esto permitirá aumentar la sensibilidad del personal de la organización hacia la seguridad de la información.

La inversión en software de control y gobernabilidad de la información en la organización es una opción que debe considerar, esto permitiría llevar un correcto manejo y trazabilidad de las políticas de seguridad de la información, su correcto cumplimiento y gestionar el SGSI de manera local, a estos sistemas se pueden vincular las estadísticas del IDS, de los incidentes detectados por la consola de antivirus y los incidentes de seguridad registrados de manera general.

El área de seguridad de la información debe ser un área independiente de las demás, incluso infraestructura, no se puede confundir las actividades de esta área con las de seguridad de la información si se quiere implementar un ISMS que permanezca actualizado, bajo control y objeto de certificación.

Es muy importante cumplir con cada uno de los controles detallados en la norma, por ello se debe considerar por parte de la dirección realizar las inversiones necesarias para separar las áreas de levantamiento de requerimientos, desarrollo, pruebas y producción de las fábricas de software.

Al separar las áreas es recomendable que a estas áreas solamente pueda acceder personal autorizado por lo cual se deben implementar mecanismos de control para el acceso físico a las instalaciones de las fábricas de software.

Los equipos de las fábricas de software deben poseer un aislamiento especial de internet a través de los cortafuegos, no es recomendable que desde los mismos equipos de la fábrica los colaboradores se puedan conectar a correos personales, redes sociales y sitios de almacenamiento en la nube, esto claramente ocasiona una vulnerabilidad de seguridad.

Se recomienda a la dirección establecer un cronograma de auditorías de seguridad de la información de manera periódica en la cual se pueda evaluar el alcance y cumplimiento de los requisitos de control de la norma, de esta manera se logra preparar el SGSI para la certificación oficial por organismo competente.

Fin del Informe.

Informe Elaborado por:

El Auditor,

Ing. Javier Olivo Garcia Araque

Est. Especialización en seguridad Informática UNAD.

13. CONCLUSIONES

En cuanto al proceso de auditoria se puede destacar el apoyo de la dirección y la orientación del equipo de calidad y operaciones quienes realizaron acompañamiento durante la auditoria validando que se cumplieran los objetivos propuestos los cuales consistían en la detección de puntos débiles que se deben mejorar para aspirar a la certificación del proceso de desarrollo de software.

Existe un cumplimiento intermedio de los requisitos de la norma NTC ISO IEC 27001:2013 en la organización, esto debido a que las NO conformidades encontradas pesan bastante sobre el sistema de gestión de seguridad de la información al referirse específicamente a los controles criptográficos, separación de áreas de desarrollo, prueba y producción, valoración de los incidentes de seguridad de la información y la revisión independiente del sistema de gestión de seguridad que garantizan la integridad, confidencialidad y disponibilidad de los sistemas de información.

Aunque la tabla expuesta en el informe de auditoría muestra un cumplimiento promedio del 80%, la realidad es que esta solamente es la vista cuantitativa, al tener en cuenta la vista cualitativa el porcentaje de cumplimiento desciende al rededor del 50% y si se tienen en cuenta dominios de seguridad de la información como el 10 Controles Criptográficos y el 16 Gestión de incidentes de la seguridad de la información, el porcentaje de cumplimiento desciende incluso por debajo del 50% mereciendo una atención especial por parte de los líderes del área, procesos relacionados y los directivos de la organización.

Actualmente la mayoría de actividades de seguridad de la información recaen sobre el área de infraestructura que tiene entre otras actividades la responsabilidad de velar por la seguridad de la información reduciendo la importancia que tiene esta área.

El entorno de desarrollo presenta fuertes debilidades respecto a la seguridad de la información que allí se trabaja, al no estar separadas estas áreas y aisladas de otras áreas administrativas de la organización los riesgos de modificación, pérdida o robo de la información tienden a aumentar y si a esto se le suma la confianza de los líderes del proceso en lugar de un control estandarizado los resultados pueden ser catastróficos para la organización y para sus clientes.

La inexistencia de políticas y controles criptográficos que se reflejen en comunicación encriptada, infraestructuras PKI, comunicaciones y enlaces seguros expone la información de la organización a riesgos innecesarios que se convierten en vulnerabilidades de la información.

Existe una ausencia de normas y políticas que establezcan procedimientos claros de recopilación de evidencias, lo cual puede dar lugar a que incidentes de seguridad ocasionados por individuos dentro o fuera de la organización no sean correctamente reseñados y posteriormente sea más difícil su judicialización por las autoridades en Colombia. Lo anterior permite que las conductas delincuenciales con la información queden impunes y que la imagen de la organización se desvalorice.

La falta de concienciación y capacitación en seguridad de la información, así como la falta de un procedimiento de revisión independiente de la seguridad de la información entorpece la evolución del sistema de gestión de seguridad de la información ocasionando entropía y haciendo el sistema lento ante posibles amenazas o vulnerabilidades que puedan aparecer en el medio.

Las no conformidades menores detalladas en el reporte tienen menor peso cuantitativo que una no conformidad mayor, sin embargo, también dan lugar a vulnerabilidades que pueden ser explotadas por agentes internos y externos, y de la misma manera califica el sistema como no apto para una certificación por un organismo competente.

Las no conformidades solo se catalogan como Mayores o Menores en una auditoria interna como la realizada en este trabajo de grado, en una auditoria externa de certificación o recertificación una no conformidad tiene en ambos casos la misma importancia inhabilitando el sistema completo para poder ser certificado.

Las no conformidades mayores para este informe se describen como controles reglamentarios para la norma NTC ISO-IEC 27001:2013 que no existen en la organización; las no conformidades menores corresponden a controles establecidos pero que no se están llevando a cabo de manera correcta.

14. RESULTADOS E IMPACTOS

14.1 RESULTADOS

Como resultado de este trabajo se logra realizar una evaluación al sistema de gestión de seguridad de la información de la organización lo cual se convierte en el primer paso de un proceso de sensibilización para la implementación futura de la norma ISO 27001:2013.

Se obtiene la información documentada que evidencia la aplicación de la auditoria en la cual se observan los controles conformes, los no conformes y las oportunidades de mejora en el Sistema de gestión de seguridad de la información.

Se genera una metodología para la realización de la auditoria periódica al sistema de gestión de seguridad de la información en la organización.

14.2 IMPACTOS

El desarrollo de este proyecto permitió:

Realizar un diagnóstico del estado actual de la seguridad de la información comparando respecto a la norma los controles no conformes y opciones de mejora que pueden ser objeto de análisis para la implementación de las recomendaciones en el plan estratégico del año 2017.

La generación de conciencia a nivel del área de Fábricas de Software sobre la importancia de conservar y optimizar los controles de seguridad de la información.

Se genera una metodología con la cual se puede evaluar la seguridad de la información a nivel transversal en toda la organización.

Se genera también conciencia en la dirección sobre la necesidad de la certificación del Sistema de gestión de seguridad de la información de manera oficial por razones de mercado y competencia.

15. DIVULGACION

Este trabajo no incluye información confidencial de la organización objeto de la auditoria, sin embargo, se incluye información referente a un proceso de auditoria en seguridad de la información en el periodo actual el cual puede diferir de los datos que reposan en la organización, los fines de este trabajo son metodológicos y académicos y solamente buscan ilustrar el procedimiento de realizar una Auditoria a Sistemas de Gestión de Seguridad de la Información a Nivel Organizativo.

Los derechos de propiedad intelectual de este trabajo corresponden a la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD - COLOMBIA quien determinara las formas en las que este documento se puede compartir al público respetando su propiedad.

Sobre este trabajo pueden existir algunas restricciones de publicación que determinara la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD-COLOMBIA, en cualquier momento.

Este documento puede ser publicado en el repositorio institucional de la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD- COLOMBIA, para ser utilizado como referencia para otros trabajos de investigación en la Universidad o público general.

La UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD- COLOMBIA puede determinar en cualquier momento medios diferentes de publicación de este documento, revistas, artículos científicos, periódicos institucionales, libros, internet.

BIBLIOGRAFÍA

ARIZA, Andrea. Elaboración de un plan de implementación de la ISO/IEC 27001:2005. Trabajo Final de Master. Catalunya. Universitat Oberta de Catalunya. 2013. 108 p.

BRITISH STANDARDS INSTITUTION. Evolución de la norma ISO 27001 BS 7799, obtenido [en línea] el 10 de septiembre de 2015 de: http://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/

CORTEZ, Diana Marcela y ARDILA, Alix Victoria. Metodología para la implementación de un sistema integrado de gestión de las normas ISO 9001, ISO 20000, ISO 27001. Trabajo de grado de Especialista en gestión de proyectos y Calidad. Bogotá D.C. Universidad EAN. Facultad de Posgrados, 2012. 72 p.

INFORMATICA Y TECNOLOGIA STEFANINI. Historia de Stefanini Colombia y Stefanini Solutions, obtenido [en línea] el 15 de septiembre de 2015 de: http://www.stefaninicolombia.com/quienes-somos-2/

INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACION. Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos. NTC-ISO/IEC 27001:2005. Bogotá D.C. El instituto 37p.

INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACION. Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos. NTC-ISO/IEC 27001:2013. Bogotá D.C. El instituto 26p.

INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACION. Referencias Bibliográficas. Contenido Forma y Estructura. NTC-ISO/IEC 5613:2008. Bogotá D.C, El Instituto. 38p.

INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACION. Referencias Documentales para fuentes de Información Electrónica. NTC-ISO/IEC 4490:1998. Bogotá D.C, El Instituto. 27p.

INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACION. Documentación. Presentación de Tesis trabajos de grado y otros trabajos de investigación. NTC-ISO/IEC 1486:2008. Bogotá D.C. EL instituto. 42p.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Evolución de empresas certificadas en ISO 27001:2013 en Colombia, obtenido [en línea] el 10 de septiembre de 2015 de: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=CO#countrypick

NIETO, Juan Pablo. Plan de implementación de la ISO/IEC 27001:2005. Trabajo Final de Master. Catalunya. Universitat Oberta de Catalunya. 2013. 136 p.

PEREZ, Carlos. Evaluación SCAMPI para el modelo CMMI del SEI, obtenido, [en línea] el 15 de septiembre de 2015 de: http://suite101.net/article/scampi-a21533#.VgIj5NV_Oko

PIATTINI, Mario G.y PESO, Emilio Del. Auditoria Informática un enfoque práctico, 2 edición. Mexico D.F. editorial Alfaomega. 2001. 649p. ISBN 978-15-0731-2.

SOFTWARE ENGINEERING INSTITUTE. Standard CMMI® Appraisal Method for process Improvement (SCAMPI^{SM}) A, Version 1.3 Method Definition Document. CMU/SEI-2011-HB-001. 2011. United States, 276p.

SOLARTE, Francisco Nicolás. Metodología para realizar una Auditoria, obtenido, [en línea] el 15 de septiembre de 2015 de: http://auditordesistemas.blogspot.com.co/2011/11/metodologia-para-realizar-auditoria.html

UNIVERSIDAD DEL CAUCA. Elaboración de programas de Auditoria, obtenido, [en línea] el 20 de marzo de 2016 de: http://fccea.unicauca.edu.co/old/tgarf/tgarfse67.html

ANEXO A

CMMI-SCAMPI 1.3 STEFANINI

Capability Maturity Model Integration© for Development Version 1.3 (CMMI-DEV-V1.3©)													
Level	**Process**	**Goal**	**Practice**	**Subpractice**	**Work Product**	**Concept**	**Detailed**	**Modular**	**Info Map**	**Usable**	**Evidence**	**Total**
1 - Initial	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2 - Managed	7	15	54	231	231	100%	100%	100%	100%	100%	100%	100%
3 - Defined	11	26	86	411	411	100%	100%	100%	100%	100%	100%	100%
4. Quan. Mgd.	2	3	12	66	66	0%	0%	0%	0%	0%	0%	0%
5- Optimizing	2	5	15	71	71	0%	0%	0%	0%	0%	0%	0%
Total	**22**	**49**	**167**	**779**	**779**	**50%**	**50%**	**50%**	**50%**	**50%**	**50%**	**50%**
1 - Initial	**N/A**	**N/A**	**N/A**	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Requirements Management (REQM)	**Manage Requirements**	**Understand Requirements**	Establish criteria for distinguishing appropriate requirements providers	Lists of criteria for distinguishing appropriate requirements providers	1	2	4	8	16	32	100%
				Establish objective criteria for the evaluation and acceptance of requirements	Criteria for evaluation and acceptance of requirements	1	2	4	8	16	32	100%
				Analyze requirements to ensure that established criteria are met	Results of analyses against criteria	1	2	4	8	16	32	100%
				Reach an understanding of requirements with requirements providers so that project participants can commit to them	A set of approved requirements	1	2	4	8	16	32	100%
			Obtain Commitment to Requirements	Assess the impact of requirements on existing commitments	Requirements impact assessments	1	2	4	8	16	32	100%
				Negotiate and record commitments	Documented commitments to requirements and requirements changes	1	2	4	8	16	32	100%
			Manage Requirements Changes	Document all requirements and requirements changes that are given to or generated by the project	Requirements change requests	1	2	4	8	16	32	100%
				Maintain a requirements change history, including the rationale for changes	Requirements change impact reports	1	2	4	8	16	32	100%
				Evaluate the impact of requirement changes from the standpoint of relevant stakeholders	Requirements status	1	2	4	8	16	32	100%
				Make requirements and change data available to the project	Requirements database	1	2	4	8	16	32	100%
			Maintain Bidirectional Traceability of Requirements	Maintain requirements traceability to ensure that the source of lower level (i.e., derived) requirements is documented	Requirements traceability matrix	1	2	4	8	16	32	100%
				Maintain requirements traceability from a requirement to its derived requirements and allocation to work products	Requirements tracking system	1	2	4	8	16	32	100%
				Generate a requirements traceability matrix	Requirements traceability report	1	2	4	8	16	32	100%

ANEXO B

PROGRAMA DE AUDITORIA.

Calendario Annual de Auditorias

Norma ISO 27001: 2013	
Norma ISO 9001:2008	
CMMI Apraisal	

Objetivo:	Verificar el cumplimiento de los requisitos de la norma enunciada ssegun la auditoria programada.
Alcance:	Horizontal transversal a toda la organizacion para ISO 9001:2008, Vertical Fabrica de Software Para ISO 27001:2013 y CMMI

CRONOGRAMA ANUAL DE AUDITORIAS

	Enero				Febrero				Marzo				Abril				Mayo				Junio				Julio				Agosto				Septiembre				Octubre				Noviembre				Diciembre			
	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4	s1	s2	s3	s4
Lunes																																																
Martes																																																
Miercoles																																																
Jueves																																																
Viernes																																																

ANEXO C

CRONOGRAMA DE AUDITORIA.

CRONOGRAMA DE AUDITORIA ISO 27001:2013							
Dominio	Procedimiento/Instructivo	Auditado	Auditor	Fecha	Hora	Lugar	Dedicacio
5	Politicas de seguridad						
7	Seguridad de los recursos humanos						
6	Aspectos organizativos de la seguridad de la informacion						
10	Cifrado						
8	Gestion de Activos						
9	Control de Accesos						
11	Seguridad fisica y ambiental						
12	Seguridad de las operaciones						
13	Seguridad de las telecomunicaciones						
17	Aspectos de la seguridad de la Informacion en la gestion de la continuidad del negocio						
14	Adquisicion, desarrollo y mantenimiento de los sitemas de informacion						
15	Relacion con proveedores						
16	Gestion de los incidentes de seguridad de la informacion						
18	Cumplimiento						

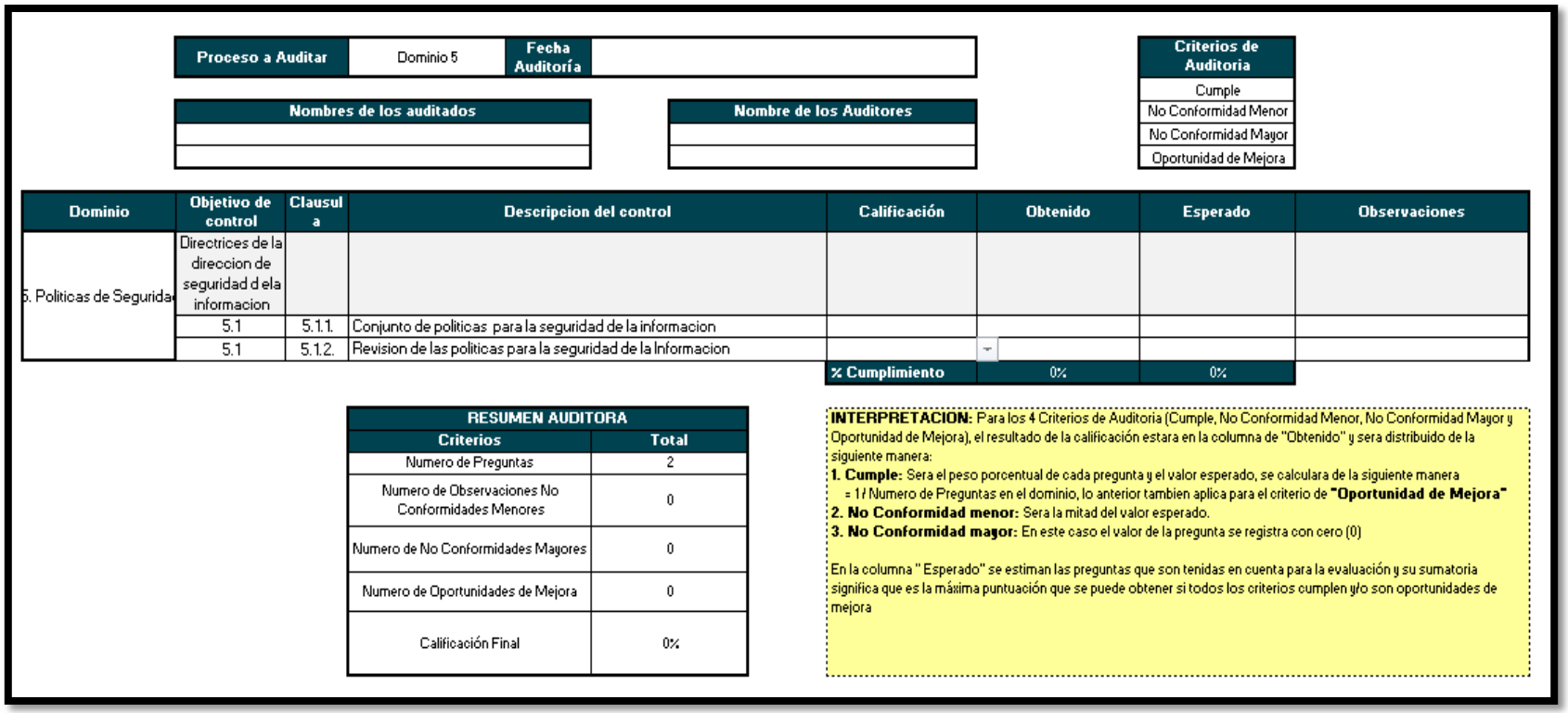
ANEXO D

PLAN DE AUDITORIA.

PLAN DE AUDITORIA				
Fecha		No. Auditoria		
Proceso Auditado				
Objetivo de Auditoria				
Alcance de auditoria				
Criterios de Auditoria				
Personal Auditado				
Equipo Auditor				
Hora	Actividad	Auditor	Auditado	Requisitos
	Revision controles numeral 5			

ANEXO E

LISTADOS DE AUDITORIA.



Proceso a Auditar	Dominio 5	Fecha Auditoría	

Nombres de los auditados	Nombre de los Auditores

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
5. Politicas de Seguridad	Directrices de la direccion de seguridad d ela informacion						
	5.1	5.1.1.	Conjunto de politicas para la seguridad de la informacion				
	5.1	5.1.2.	Revision de las politicas para la seguridad de la Informacion				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	2
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. Cumple: Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera
= 1/ Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**

2. No Conformidad menor: Sera la mitad del valor esperado.

3. No Conformidad mayor: En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Proceso a Auditar	Dominio 6	Fecha Auditoría	

Nombres de los auditados	Nombre de los Auditores

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
6. Aspectos Organizativos de la seguridad de la informacion	Organizacion interna						
	6.1	6.1.1	Asignacion de responsabilidades para la seguridad de la informacion.				
	6.1	6.1.2	Segregacion de tareas				
	6.1	6.1.3	Contacto con autoridades				
	6.1	6.1.4	Contacto con grupos de interes especial				
	6.1	6.1.5	Seguridad de la informacion en la gestion de proyectos.				
	Movilidad y teletrabajo						
	6.2	6.2.1	Politica de seguridad para dispositivos moviles.				
	6.2	6.2.2	Teletrabajo				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	7
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. Cumple: Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**

2. No Conformidad menor: Sera la mitad del valor esperado.

3. No Conformidad mayor: En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Proceso a Auditar	Dominio 7	Fecha Auditoría	

Nombres de los auditados	Nombre de los Auditores

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
7. Seguridad de los recursos humanos	Antes de la Contratacion						
	7.1	7.1.1	Investigacion de antecedentes antes de la contratacion.				
	7.1	7.1.2	Terminos y condiciones de la contratacion				
	Durante la contratacion						
	7.2	7.2.1	Responsabilidades de la gestion				
	7.2	7.2.2	Concienciacion, educacion y capacitacion en la seguridad de la informa				
	7.2	7.2.3	Proceso disciplinario				
	Terminacion o cambio de contratacion						
	7.3	7.3.1	Cese o cambio de puesto de trabajo				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	6
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Proceso a Auditar	Dominio 8	Fecha Auditoría	

Nombres de los auditados

Nombre de los Auditores

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
8. Gestion de Activos	Responsabilidad sobre los activos						
	8.1	8.1.1	Inventario de activos				
	8.1	8.1.2	Propiedad de los activos				
	8.1	8.1.3	Uso aceptable de los activos				
	8.1	8.1.4	Devolucion de activos				
	Clasificacion de la Informacion						
	8.2	8.2.1	Directrices de la clasificacion				
	8.2	8.2.2	Etiquetado y manipulado de la informacion				
	8.2	8.2.3	Manipulacion de activos				
	Manejo de los soportes de almacenamiento						
	8.3	8.3.1	Gestion de los soportes extraibles				
	8.3	8.3.2	Eliminacion de soportes				
	8.3	8.3.3	Soportes fisicos en transito				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	10
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. Cumple: Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera
= 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**

2. No Conformidad menor: Sera la mitad del valor esperado.

3. No Conformidad mayor: En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Proceso a Auditar	Dominio 9	Fecha Auditoría	

Nombres de los auditados	Nombre de los Auditores

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
9. Control de accesos	Requisitos del negocio para el control de accesos						
	9.1	9.1.1	Politica de control de accesos				
	9.1	9.1.2	Control de acceso a las redes y servicios asociados				
	Gestion de acceso de usuario						
	9.2	9.2.1	Gestion de Altas y Bajas en el registro de usuarios				
	9.2	9.2.2	Gestion de derechos de acceso asignados a los usuarios				
	9.2	9.2.3	Gestion de los derechos de acceso con privilegios especiales				
	9.2	9.2.4	Gestion de informacion confidencial de autenticacion de usuarios				
	9.2	9.2.5	Revision de los derechos de acceso de los usuarios				
	9.2	9.2.6	Retirada o adaptacion de los derechos de acceso				
	Responsabilidad de usuario						
	9.3	9.3.1	Uso de informacion confidencial para la autenticacion				
	Control de acceso a sistemas y aplicaciones						
	9.4	9.4.1	Restriccion del acceso a la informacion				
	9.4	9.4.2	Procedimientos seguros de inicio de sesion				
	9.4	9.4.3	Gestion de contrasenas de usuario				
	9.4	9.4.4	Uso de herramientas de administracion de sistemas				
	9.4	9.4.5	Control de acceso al codigo fuente de los programas				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	14
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1/ Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna "Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Proceso a Auditar	Dominio 10	Fecha Auditoría	

Nombres de los auditados

Nombre de los Auditores

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
10. Cifrado	Controles Criptograficos						
	10.1	10.1.1	Politica de uso de los controles criptograficos				
	10.1	10.1.2	Gestion de claves				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	2
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora.

Proceso a Auditar	Dominio 11	Fecha Auditoría	

Nombres de los auditados	Nombre de los Auditores

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de control	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
11. Seguridad Fisica y ambiental	Areas Seguras						
	11.1	11.1.1	Perimetro de seguridad Fisica				
	11.1	11.1.2	Controles fisicos a la entrada				
	11.1	11.1.3	Seguridad de oficinas, despachos y recursos				
	11.1	11.1.4	proteccion contra las amenazas externas y ambientales				
	11.1	11.1.5	Trabajo en areas Seguras				
	11.1	11.1.6	Areas de acceso publico, carga y descarga				
	Seguridad de los equipos						
	11.2	11.2.1	Emplazamiento y proteccion de equipos				
	11.2	11.2.2	Instalaciones de suministro				
	11.2	11.2.3	Seguridad del cableado				
	11.2	11.2.4	Mantenimiento de los equipos				
	11.2	11.2.5	Salida de activos fuera de las dependencias de la empresa				
	11.2	11.2.6	Seguridad de los equipos y activos fuera de las instalaciones				
	11.2	11.2.7	Reutilizacion o retirada segura de dispositivos de almacenamiento				
	11.2	11.2.8	Equipo informatico de usuario desatendido				
	11.2	11.2.9	Politica de puesto de trabajo despejado y bloqueo de pantalla				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	15
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de

Proceso a Auditar	Dominio 12	Fecha Auditoría	

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Nombres de los auditados	Nombre de los Auditores

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
	Responsabilidad y procedimientos de operacion						
	12.1	12.1.1	Documentacion de procedimientos de operacion				
	12.1	12.1.2	Gestion de cambios				
	12.1	12.1.3	Gestion de capacidades				
	12.1	12.1.4	Separacion de entornos de desarrollo, prueba y produccion				
	Proteccion contra codigos maliciosos						
	12.2	12.2.1	Controles contra el codigo malicioso				
	Copias de seguridad						
	12.3	12.3.1	Copias de seguridad de la informacion				
	Registros de actividad y supervision						
12. Seguridad en las operaciones	12.4	12.4.1	Registro y gestion de eventos de actividad				
	12.4	12.4.2	Proteccion de los registros de la informacion				
	12.4	12.4.3	Registros de actividad del operador y administrador del sistema				
	12.4	12.4.4	Sincronizacion de relojes				
	Control del software en explotacion						
	12.5	12.5.1	Instalacion de software en sistemas en produccion				
	Gestion de la vulnerabilidad tecnica						
	12.6	12.6.1	Gestion de las vulnerabilidades tecnicas				
	12.6	12.6.2	Restricciones en la instalacion de software				
	Consideraciones de auditorias a sistemas de informacion						
	12.7	12.7.1	Controles de auditorias a sistemas de informacion				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORIA	
Criterios	Total
Numero de Preguntas	14
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera
   = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Proceso a Auditar	Dominio 13	Fecha Auditoría	

Nombres de los auditados	Nombre de los Auditores

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
13. Seguridad en las telecomunicaciones	Gestion de la seguridad en las redes						
	13.1	13.1.1	Controles de red				
	13.1	13.1.2	Mecanismos de seguridad asociados con servicios en red				
	13.1	13.1.3	Segregacion de redes				
	Intercambio de informacion con partes externas						
	13.2	13.2.1	Politicas y procesimientos de intercambio de informacion				
	13.2	13.2.2	Acuerdos de intercambio				
	13.2	13.2.3	mensajeria electronica				
	13.2	13.2.4	Acuerdos de confidencialidad y secreto				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	7
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de

Proceso a Auditar	Dominio 14	Fecha Auditoría	

Nombres de los auditados	Nombre de los Auditores

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
14. Adquisicion, desarrollo y mantenimiento de los sistemas de informacion	Requisitos de seguridad de los sistemas de informacion						
	14.1	14.1.1	Analisis y especificacion de los requisitos de seguridad				
	14.1	14.1.2	Seguridad en las comunicaciones en servicios accesibles por redes publicas				
	14.1	14.1.3	Proteccion de las transacciones realizadas por redes telematicas				
	Seguridad en los procesos de desarrollo y soporte						
	14.2	14.2.1	Politica de desarrollo seguro de software				
	14.2	14.2.2	Procedimientos de control de cambios de los sistemas				
	14.2	14.2.3	Revision tecnica de las aplicaciones tras efectuar cambios en el sistema operativo				
	14.2	14.2.4	Restricciones a los cambios en los paquetes de software				
	14.2	14.2.5	Uso de principios de ingenieria en proteccion de sistemas				
	14.2	14.2.6	Seguridad en entornos de desarrollo				
	14.2	14.2.7	Externalizacion del desarrollo de software				
	14.2	14.2.8	Pruebas de funcionalidad durante el desarrollo de sistemas				
	14.2	14.2.9	Pruebas de aceptacion				
	Datos de Prueba						
	14.3	14.3.1	proteccion de los datos utilizados en las pruebas				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	13
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de

Proceso a Auditar	Dominio 15	Fecha Auditoría	

Nombres de los auditados	Nombre de los Auditores

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
15. Relaciones con Proveedores	Seguridad de la informacion en la relacion con proveedores						
	15.1	15.1.1	Politica de seguridad de la informacion para proveedores				
	15.1	15.1.2	Tratamiento del riesgo dentro de los acuerdos con proveedores				
	15.1	15.1.3	Cadena de suministro en tecnologias de la informacion y comunicaciones				
	Gestion de la prestacion del servicio por proveedores						
	15.2	15.2.1	Supervision y revision de los servicios prestados por terceros				
	15.2	15.2.2	Gestion de cambios en los servicios prestados por terceros				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	5
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. Cumple: Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera
= 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**

2. No Conformidad menor: Sera la mitad del valor esperado.

3. No Conformidad mayor: En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora.

Proceso a Auditar	Dominio 16	Fecha Auditoría	

Nombres de los auditados

Nombre de los Auditores

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
	Gestion de incidentes de seguridad de la informacion y						
16. Gestion de incidentes en la seguridad de la informacion	16.1	16.1.1	Responsabilidades y Procedimientos				
	16.1	16.1.2	Notificacion de los eventos de seguridad de la informacion				
	16.1	16.1.3	Notificacion de los puntos debiles de la seguridad				
	16.1	16.1.4	Valoracion de eventos de seguridad de la informacion y toma de desiciones				
	16.1	16.1.5	Respuesta a los incidentes de seguridad				
	16.1	16.1.6	Aprendizaje de los incidentes de seguridad de la informacion				
	16.1	16.1.7	Recopilacion de evidencias				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	7
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. Cumple: Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera
= 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**

2. No Conformidad menor: Sera la mitad del valor esperado.

3. No Conformidad mayor: En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Proceso a Auditar	Dominio 17	Fecha Auditoría	

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Nombres de los auditados

Nombre de los Auditores

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
17. Aspectos de seguridad de la informacion en la gestion de la continuidad del negocio	Responsabilidad sobre los activos						
	17.1	17.1.1	Planificacion de la continuidad de la seguridad de la informacion				
	17.2	17.1.2	Implantacion de la continuidad de la seguridad de la informacion				
	17.3	17.1.3	Verificacion, revision y evaluacion de la continuidad de la seguridad de la informacion				
	Redundancias						
	17.2	17.2.1	Disponibilidad de las instalaciones para el procesamiento de la informacion				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	4
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

Proceso a Auditar	Dominio 18	Fecha Auditoría	

Nombres de los auditados

Nombre de los Auditores

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de	Clausula	Descripcion del control	Calificación	Obtenido	Esperado	Observaciones
18. Cumplimiento	Cumplimiento de los requisitos legales y						
	18.1	18.1.1	Identificacion de la legislacion aplicable				
	18.1	18.1.2	Derechos de propiedad intelectual				
	18.1	18.1.3	Proteccion de los registros de la organizacion				
	18.1	18.1.4	Proteccion de los datos y privacidad de la informacion personal				
	18.1	18.1.5	Regulacion de los controles criptograficos				
	Revisiones de la seguridad de la informacion						
	18.2	18.2.1	Revision independiente de la seguridad de la informacion				
	18.2	18.2.2	Cumplimiento de las politicas y normas de seguridad				
	18.2	18.2.3	Comprobacion del cumplimiento				
				% Cumplimiento	0%	0%	

RESUMEN AUDITORA	
Criterios	Total
Numero de Preguntas	8
Numero de Observaciones No Conformidades Menores	0
Numero de No Conformidades Mayores	0
Numero de Oportunidades de Mejora	0
Calificación Final	0%

INTERPRETACION: Para los 4 Criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estara en la columna de "Obtenido" y sera distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera
   = 1 / Numero de Preguntas en el dominio, lo anterior tambien aplica para el criterio de **"Oportunidad de Mejora"**
2. **No Conformidad menor:** Sera la mitad del valor esperado.
3. **No Conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna " Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora

ANEXO F

HOJA DE HALLAZGOS.

HOJA DE HALLAZGOS									
FECHA AUDITORIA:									
Nro.	Código	Proceso Auditado	Clausula 27001:2013	Descripción de la No Conformidad u Oportunidad de Mejora	Responsable	Clasificación	Acción correctiva o preventiva relacionada	Tipo No Conformidad U-No usa M-Mal uso	Auditor
		Desarrollo de software			Gerente de fabricas continuas				Javier Garcia

ANEXO G

INFORME FINAL DE AUDITORIA.

Informática & Tecnología Stefanini S.A
Calle 122 No 23-46 Piso 5
Tel. 7454777 Fax 7454777 Ext 117
www.StefaniniColombia.com

stefanini
Informática
& Tecnología

06 DE MAYO DE 2016

Gerencia de Calidad y operaciones Colombia
Calle 122 No 23-46 piso 5, Bogotá D.C- Colombia.

Sres. Directivos:

En el presente documento encontraran el Informe final de la auditoría realizada al proceso Desarrollo de Software que tuvo lugar desde el 18 de abril de 2016 al 29 de abril de 2016, contando con el apoyo de las gerencias de Calidad y Operaciones, Recursos Humanos, Infraestructura y Fábrica de Software. Esta auditoria había sido anunciada desde el mes de Octubre de 2015 y autorizada por la Gerencia de Calidad y Operaciones en nombre de la Ing. Luz Marina Motta Beltran mediante carta de aprobación dirigida al Ing. Javier Olivo Garcia Araque con registro Profesional 25255-308521 CND quien desarrolla su proyecto de grado para la Universidad Nacional Abierta y a Distancia – UNAD Como especialista en seguridad informática.

Informe Final de Auditoria Interna ISO 27001:2013 al proceso de Desarrollo de Software

Contenido

Informe Final de Auditoria Interna ISO 27001:2013 al proceso de Desarrollo de Software

1. Datos generales

Fechas de la auditoria:

18 al 29 de Abril 2016.

Tipo de Auditoria:

Interna

Criterios Aplicados:

Norma NTC ISO-IEC 27001:2013

CMMI® V1.3 2011

Cliente de Auditoria:

Fábrica de software I&T Stefanini Colombia.

Objetivo de la Auditoria:

Verificar el cumplimiento de los objetivos de control de la norma ISO 27002:2013

Alcance de la Auditoria:

Proceso de Desarrollo de Software.

2. Metodología

Para llevar a cabo la auditoria de seguridad de la información 2016-I y con el objetivo de evidenciar los controles que se cumplen, los que presentan fallas y los que no se están cumpliendo de acuerdo a la norma NTC ISO-IEC 27001:2013, el auditor tuvo en cuenta las siguiente metodología.

2.1 Visita in Situ

El auditor realizo varias visitas a la Fábrica de Software ubicada en la calle 122 con autopista, piso 6 donde funciona la sede principal en Colombia con el objetivo de verificar los procedimientos de operación del área respecto al sistema de gestión de seguridad actual.

2.2 Revisión de la documentación de seguridad de la información.

El auditor solicito y reviso la documentación existente en la organización respecto a la gestión de la seguridad de la información verificando el manual de políticas de seguridad de la información, el plan de continuidad y el plan de recuperación de desastres, entre otros planes de seguridad relacionados con aplicaciones y equipos especiales que no se incluyen de manera precisa en los 79 artículos del manual de seguridad de la información, de la misma manera reviso los estándares que se cumplen en el proceso de desarrollo de software para analizar su relación con la seguridad de la información

2.3 Entrevistas con desarrolladores de algunas fábricas de software.

El Auditor realizo entrevistas específicas a algunos de los desarrolladores para explorar la conciencia de seguridad de la información en la operación diaria, igualmente en estas entrevistas se busca el conocimiento de los desarrolladores acerca de los estándares y normas que gobiernan el área.

2.4 Cuestionarios con líderes del proceso

El auditor diseño una lista de cuestionarios que diligencio en compañía de los líderes del proceso y procesos relacionados, estos listados serán los que arrojen una imagen cuantitativa del estado de la seguridad de la información respecto a la norma NTC ISO-IEC 27001:2013.

También se validó el último resultado de evaluación SCAMPI relacionada con las 22 áreas de proceso de CMMI V1.3 2011 que certifican en nivel 3 el desarrollo de software.

3 Resultados.

Los resultados de las actividades anteriores se plasman en los listados de auditoria los cuales se anexan a este documento y se detallan en el presente informe final de auditoria, destacando de los 114 controles evaluados correspondientes a la norma NTC ISO-IEC 27002:2013 los siguientes detalles.

Controles Conformes	82
Oportunidad de Mejora	10
No Conformidad Menor	8
No Conformidad Mayor	14
Controles Evaluados	114

El porcentaje de cumplimiento por cada uno de los 14 dominios de la norma NTC ISO-IEC 27001:2013 es el siguiente:

DOMINIO	VALOR OBTENIDO	VALOR DESEADO
5	100%	100%
6	90%	100%
7	75%	100%
8	70%	100%
9	93%	100%
10	0%	100%
11	80%	100%
12	93%	100%
13	100%	100%
14	100%	100%
15	100%	100%
16	43%	100%
17	100%	100%
18	75%	100%
Average	80%	

Que en la gráfica se representa de la siguiente manera:

Teniendo como un promedio general el 80% del cumplimiento de los controles en el proceso auditado.

Se comentan detalladamente en este informe los controles que de una u otra manera no se encuentran conformes por considerar que se debe enfatizar en llevarlos al área de conformidad.

3.1 No conformidad Mayores

Nro.	Código	Proceso Auditado	Clausula 27001:2013	Descripción del control	Responsable	Clasificación	Detalle	Tipo No Conformidad U-No usa M-Mal uso O-Oportunidad de mejora	Auditor
6	7.2	Desarrollo de software	7.2.2	Corcienciacion, educacion y capacitacion en la seguridad de la informacion	Gerente de Fabricas Continuas	**No Conformidad Mayor**	NO se evidencia la existencia de programas o campañas de promocion de la seguridad de la informacion en la organización	U	Javier Garcia
10	8.3	Desarrollo de software	8.3.2	Eliminacion de Soportes	Coordinador de fabricas continuas	**No Conformidad Mayor**	No se evidencia un procedimiento seguro de eliminacion de la informacion en soportes logicos.	U	Javier Garcia
11	8.3	Desarrollo de software	8.3.3	Soportes Fisicos en transito	Coordinador de fabricas continuas	**No Conformidad Mayor**	No se evidencia un procedimeinto para el manejo seguro de los soportes fisicos hardware cuando son movilizados de mun area a otra.	U	Javier Garcia
14	10.1	Desarrollo de software	10.1.1	Politica de uso de controles criptograficos	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No se evidencia el uso de aplicaciones de encriptamiento ni certificados digitales con los cuales administrar la informacion y el encriptamiento de la misma permitiendo riesgos de consulta no autorizados.	U	Javier Garcia
15	10.1	Desarrollo de software	10.1.2	Gestion de claves	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	NO existe configuracion del servicio Active Directory Certificate Service para la gestion de certificados digitales y sus claves.	U	Javier Garcia
16	11.1	Desarrollo de software	11.1.1	Permetro de Seguridad Fisica	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	Se evidencia que la fabrica de software ubicada en la sede principal calle 122 no dispone de aislamiento del resto de areas operativas y administrativas.	U	Javier Garcia
17	11.1	Desarrollo de software	11.1.2	Controles Fisicos en la entrada	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No se evidencian conroles fisicol o logicos para el acceso a la fabrica de software	U	Javier Garcia
21	12.1	Desarrollo de software	12.1.4	Separacion de entornos de desarrollo, prueba y produccion	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	En la sede principal de la organización no se encuentran diferenciados los entornos de desarrollo, prueba y produccion.	U	Javier Garcia
23	16.1	Desarrollo de software	16.1.1	Responsabilidades y procedimientos	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Mayor**	No se evidencia la existencia de procedimientos y responsabilidades en caso de incidentes de seguridad en la organizacion, en caso de haberlos el area de infraestructura es la encargada de la respuesta.	U	Javier Garcia
26	16.1	Desarrollo de software	16.1.4	Valoracion de los eventos de seguridad de la informacion y toma de desiciones	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Mayor**	En la actualidad esta acrtividad se realiza de manera reactiva, no existe un procedimiento que estableca claridad en los pasos a seguir.	U	Javier Garcia
28	10.1	Desarrollo de software	10.1.7	Recopilacion de evidencias	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Mayor**	No existe una metodologia clara de recopilacion de evidencias ante fraudes o ataques, esta funcion se recarga sobre el area de infraestructura.	U	Javier Garcia
29	18.1	Desarrollo de software	18.1.5	Regulacion de los controles Criptograficos	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No se evidencia la existencia de controles criptograficos a nivel organizacional, no existe una politica ni codigo de buenas practicas.	U	Javier Garcia
30	18.2	Desarrollo de software	18.2.1	Revision Independiente de la Seguridad de la Informacion	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Mayor**	No existe evidencia de controles a la seguridad de la informacion externos, diferentes a los solicitados por algunos clientes para el establecimiento de un contrato, se realiza control desde PC-AU-01 Plan y Realizacion de auditorias	U	Javier Garcia

3.2 No Conformidad Menores

Nro.	Código	Proceso Auditado	Clausula 27001:2013	Descripción del control	Responsable	Clasificación	Detalle	Tipo No Conformidad U-No usa M-Mal uso O-Oportunidad de mejora	Auditor
3	6.1	Desarrollo de software	6.1.5	Seguridad de la informacion en la gestion de proyectos.	Gerente de Fabricas Continuas	**No Conformidad Menor**	Se pueden apreciar debilidades en los controles de seguridad de la informacion debido a que la gestion de la misma en cada proyecto solamente es realizada ocasionalmente por el gerente de proyecto quien se fundamenta que los controles de seguridad los ejerce de manera logica el area de infraestructura, no existe evidencia de los controles realizados de manera periodica o constante ya que muchas veces depende del cliente del proyecto.	M	Javier Garcia
7	7.3	Desarrollo de software	7.3.1	Cese o Cambio de puesto de trabajo	Gerente de Fabricas Continuas	**No Conformidad Menor**	Existe un procedimiento de informe al area de infraestructura , sin embargo se evidencian periodos prolongados en la inactivacion de cuentas por retiros y el cambio de permisos y privilegios por movimientos de personal, este tiempo muerto se presenta por demoras en la notificacion de RRHH a Infraestructura.	M	Javier Garcia
8	8.2	Desarrollo de software	8.2.2	Etiquetado y Manipulado de la Informacion	Coordinador de fabricas continuas	**No Conformidad Menor**	Se evidencia que no toda la informacion es correctamente etiquetada segun la politica de seguridad y la matriz LI-RD-08, encontrandose documentacion sensible y sin catalogar expuesta	M	Javier Garcia
9	8.2	Desarrollo de software	8.2.3	Manipulacion de Activos	Coordinador de fabricas continuas	**No Conformidad Menor**	Se evidencia que en algunas estaciones de trabajo de los desarrolladores se permite el uso de pendrives y usb que representan riesgos de hurto de la informacion.	M	Javier Garcia
12	9.2	Desarrollo de software	9.2.1	Gestion de altas y Bajas en el registro de usuarios	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Menor**	Se encuentra una politica clara para la gestion de altas y bajas de usuarios que se retiran de la organizacion y los traslados o movimientos de personal, sin embargo se puede evidenciar que los tiempos de respuesta para la baja y modificacion de los privilegios de un usuario no son inmediatos a su notificacion.	M	Javier Garcia
13	9.2	Desarrollo de software	9.2.6	Retirada o adaptacion de los derechos de acceso	Gerente de Fabricas Continuas Gerente de Infraestructura	**No Conformidad Menor**	Se evidenci la existencia de la politica de cambio d eprivilegios y control de accesos para los traslados o movimientyos de personal, se evidencia la gestion correcta por el area de infraestructura, sin embargo el retiro y adaptacion de privilegios no se realiza inmediatamente se sinforma por parte d ela gerencia a cargo.	M	Javier Garcia
25	16.1	Desarrollo de software	16.1.3	Notificacion de los puntos debiles de la seguridad	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Menor**	Se notifican los incidentes de seguridad a traves de correo el cual no es automatico"mensajes de infraestructura", pero no existe un procedimiento formal, tampoco se realiza notificacion en la intranet corporativa.	M	Javier Garcia
27	16.1	Desarrollo de software	16.1.5	Respuesta a los incidentes de seguridad	Gerente de Infraestructura Coordinador de Fabricas Continuas	**No Conformidad Menor**	la respuesta a estos incidentes es lenta debido a la falta de una metodologia clara de notificacion y respuesta, generalmente se recargan los incidentes unicamente en el area de infraestructura	M	Javier Garcia

3.3 Oportunidades de Mejora.

Nro.	Código	Proceso Auditado	Clausula 27001:2013	Descripción del control	Responsable	Clasificación	Detalle	Tipo No Conformidad U-No usa M-Mal uso O-Oportunidad de mejora	Auditor
1	6.1	Desarrollo de software	6.1.1	Conjunto de políticas para la seguridad de la informacion	Gerente de Fabricas Continuas	**Oportunidad de Mejora**	La organinzacion cuenta con un documento de politicas de seguridad que es conocido por todos los procesos de la organizacion.	O	Javier Garcia
2	6.1	Desarrollo de software	6.1.2	Segregacion de tareas	Gerente de Fabricas Continuas	**Oportunidad de Mejora**	Las tareas de seguridad de la informacion se asignan a los gerentes y coordinadores de cada proyecto, adicionalmente el area de infraestructura asigna y monitorea el acceso y uso de los recursos, y el area de control de operaciones ejerce vigilancia; no existe la figura de CIO o responsible de seguridad de la informacion en la organizacion a nivel Colombia	O	Javier Garcia
4	6.2	Desarrollo de software	6.2.2	Teletrabajo	Gerente de Fabricas Continuas	**Oportunidad de Mejora**	Existe una politica de teletrabajo y trabajo flexible, sin embargo no se implementa ya que actualmemnte no se realiza teletrabajo en ningun proyecto.	O	Javier Garcia
5	7.1	Desarrollo de software	7.1.1	Investigacion de anteoedentes antes de la contratacion.	Gerente de Fabricas Continuas	**Oportunidad de Mejora**	En la organizacion existe un protocolo de reclutamiento y seleccion del personal, sin embargo solo se llevan a cabo estudios de seguridad cuando el proyecto del cliente asi lo requiere o cuando existe solicitud expresa del cliente.	O	Javier Garcia
18	11.1	Desarrollo de software	11.1.3	Seguridad de Oficinas, despachos y recursos	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se evidencia que en las instalaciones en las que funciona la fabrica de sofware se dispone de CCTV conectados al area de seguridad del edificio, sin embargo esta vigilancia deberia ser propia de la organizacion.	O	Javier Garcia
20	11.2	Desarrollo de software	11,2,8	Equipo informatico de usuario desatendido	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se evidencia la correcta gestion de los incidentes presentados por los usuarios a traves del servicedesk, por esta razon no se encuentran estaciones desatendidas al momento de la auditoria	O	Javier Garcia
22	14.2	Desarrollo de software	14.2.7	Externanilzacion del desarrollo de Software	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se omite ya que la organizacion no externaliza el desarrollo de software, este se realiza inhouse por las fabricas internas, sin embargo se debe generar una politica de desarrollo con externos.	O	Javier Garcia
24	16.1	Desarrollo de software	16.1.2	Notificacion de los eventos de seguridad de la informacion	Gerente de Infraestructura Coordinador de Fabricas Continuas	**Oportunidad de Mejora**	De manera local no existe un procedimiento de notificacion de eventos de seguridad de la informacion, el monitoreo se realiza desde casa matriz en Brasil donde se notifica al gerente de infraestructura y al gerente de operaciones en colombia sobre las anomalias presentadas.	O	Javier Garcia
31	18.2	Desarrollo de software	18.2.2	Cumplimiento de las normas y politicas de seguiuridad	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se tiene la confianza de que el personal de la organizacion cumple con las politicas de seguridad, el control de las politicas de seguridad lo realizan los jefes directos y el area de infraestructura.	O	Javier Garcia
32	18.2	Desarrollo de software	18.2.3	Comprobacion del cumplimiento	Gerente de Fabricas Continuas Gerente de Infraestructura	**Oportunidad de Mejora**	Se realiza por los jefes directos de los colaboradores y cargos de control, igualmente por infraestructura, no existe una politica o buena practica oficializada para la revision del cumplimiento de la politica de seguridad.	O	Javier Garcia

4 Conclusiones.

A nivel general se puede diagnosticar un cumplimiento intermedio de los requisitos de la norma NTC ISO IEC 27001:2013 en la organización, esto debido a que las NO conformidades encontradas pesan bastante sobre el sistema de gestión de seguridad de la información al referirse específicamente a los controles criptográficos, separación de áreas de desarrollo, prueba y producción, valoración de los incidentes de seguridad de la información y la revisión independiente del sistema de gestión de seguridad que garantizan la integridad, confidencialidad y disponibilidad de los sistemas de información.

Aunque la tabla anteriormente expuesta nos muestre un cumplimiento promedio del 80%, la realidad es que esta solamente es la vista cuantitativa, al tener en cuenta la vista cualitativa el porcentaje de cumplimiento desciende alrededor del 50 % y si se tienen en cuenta dominios de seguridad de la información como el 10. Controles Criptográficos y el 16 Gestión de incidentes de la seguridad de la información el porcentaje de cumplimiento desciende incluso por debajo del 50% mereciendo una atención especial por parte de los líderes del área, procesos relacionados y los directivos de la organización.

Actualmente la mayoría de actividades de seguridad de la información recaen sobre el área de infraestructura que tienen entre otras actividades que fijar medianamente su atención en la seguridad de la información reduciendo la importancia que tiene esta área de la información.

El entorno de desarrollo presenta fuertes debilidades respecto a la seguridad de la información que allí se trabaja, al no estar separadas estas áreas y aisladas de otras áreas administrativas de la organización los riesgos de modificación, pérdida o robo de la información tienden a aumentar y si a esto se le suma la confianza de los líderes del proceso en lugar de un control estandarizado los resultados pueden ser catastróficos para la organización y para sus clientes.

La inexistencia de políticas y controles criptográficos que se reflejen en comunicación encriptada, infraestructuras PKI, comunicaciones y enlaces seguros expone la información de la organización a riesgos innecesarios que se convierten en vulnerabilidades de la información.

La falta de normas y políticas que establezcan procedimientos claros de recopilación de evidencias puede dar lugar a que incidentes de seguridad ocasionados por individuos dentro o fuera de la organización puedan ser correctamente reseñados y judicializados por las autoridades en Colombia, dando lugar a que estas conductas queden impunes y la imagen de la organización se desvalorice.

La falta de concienciación y capacitación en seguridad de la información así como la falta de un procedimiento de revisión independiente de la seguridad de la información entorpece la evolución del sistema de gestión de seguridad de la información ocasionando entropía y haciendo el sistema lento ante posibles amenazas o vulnerabilidades que puedan aparecer en el medio.

Las no conformidades menores detalladas en este reporte tienen menor peso cuantitativo que una no conformidad mayor, sin embargo también dan lugar a vulnerabilidades que pueden ser explotadas por agentes internos y externos, y de la misma manera califica en sistema como no apto para una certificación por organismo competente.

Las no conformidades solo se catalogan como Mayores o Menores en una auditoria interna, en una auditoria externa de certificación o recertificación una no conformidad tiene en ambos casos la misma importancia inhabilitando el sistema completo para poder ser certificado.

Las no conformidades mayores para este informe se describen como controles reglamentarios para la norma NTC ISO-IEC 27001:2013 que no existen en la organización; las no conformidades menores corresponden a controles establecidos pero que no se están llevando a cabo de manera correcta.

Respecto a las opciones de mejora detalladas estás corresponden a controles de la norma NTC ISO-IEC 27001:2013 que se están llevando a cabo de manera correcta pero que aún se pueden optimizar para mejorar sus resultados.

EL levantamiento de las no conformidades y aplicación de oportunidades de mejora corresponde a los líderes de proceso de cada área quienes serán los responsables de analizar la causa raíz de cada no conformidad y presentar al auditor en un plazo no mayor a 20 días posterior a la detección de la no conformidad un plan de mejora que de origen a la mitigación de la no conformidad y permita aumentar la confiabilidad del sistema de gestión de seguridad de la información, en este caso el auditor interno o auditor líder, o responsable de calidad y operaciones serán los únicos que podrán validar la no conformidad como gestionada y conforme de acuerdo a la norma NTC ISO IEC 27001:2013.

5 Recomendaciones.

Se recomienda la inversión en personal capacitado en Seguridad de la Información de manera Local en Colombia el cual tenga a cargo las actividades de seguridad, apoyo a infraestructura, recursos humanos y el área jurídica las cuales se encuentran estrechamente relacionadas en la operación segura de un Sistema de gestión de seguridad en cualquier organización.

Se recomienda a la dirección establecer una estrategia de promoción de la seguridad de la información, esta estrategia debe abordar todas las áreas de la organización desde el momento de la vinculación de personal, promoción a través de los medios institucionales, cursos virtuales, intranet, correo electrónico y posters ubicados en sitios estratégicos, esto permitirá aumentar la sensibilidad del personal de la organización hacia la seguridad de la información.

La inversión en software de control y gobernabilidad de la información en la organización es una opción que debe considerar, esto permitiría llevar un correcto manejo y trazabilidad de las políticas de seguridad de la información, su correcto cumplimiento y gestionar el SGSI de manera local, a estos sistemas se pueden vincular las estadísticas del IDS, de los incidentes detectados por la consola de antivirus y los incidentes de seguridad registrados de manera general.

El área de seguridad de la información debe ser un área independiente de las demás, incluso infraestructura, no se puede confundir las actividades de esta área con las de seguridad de la información si se quiere implementar un ISMS que permanezca actualizado, bajo control y objeto de certificación.

Es muy importante cumplir con cada uno de los controles detallados en la norma, por ello se debe considerar por parte de la dirección realizar las inversiones necesarias para separar las áreas de levantamiento de requerimientos, desarrollo, pruebas y producción de las fábricas de software.

Al separar las áreas es recomendable que a estas áreas solamente pueda acceder personal autorizado por lo cual se deben implementar mecanismos de control para el acceso físico a las instalaciones de las fábricas de software.

Los equipos de las fábricas de software deben poseer un aislamiento especial de internet a través del cortafuegos, no es recomendable que desde los mismos equipos de la fábrica los colaboradores se puedan conectar a corros personales, redes sociales y sitios de almacenamiento en la nube, esto claramente ocasiona una vulnerabilidad de seguridad.

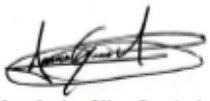
Se recomienda a la dirección establecer un cronograma de auditorías de seguridad de la información de manera periódica en la cual se pueda evaluar el alcance y cumplimiento de los requisitos de control de la norma, de esta manera se logra preparar el SGSI para la certificación oficial por organismo competente.

Informe Final de Auditoria Interna ISO 27001:2013 al proceso de Desarrollo de Software

Fin del Informe.

Informe Elaborado por:

El Auditor,



Ing. Javier Olivo Garcia Araque

Est. Especialización en seguridad Informática UNAD.

ANEXO H

RESUMEN ANALITICO “RAE”

RESUMEN ANÁLITICO RAE.

Título de Documento.	AUDITORÍA AL SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁCION EN EL PROCESO DE DESARROLLO DE SOFTWARE DE ACUERDO A LA NORMA ISO/IEC 27001:2013 EN LA EMPRESA IT STEFANINI COLOMBIA
Autor	GARCIA ARAQUE, Javier Olivo.
Palabras Claves	Auditoria de seguridad de la información, SGSI, Seguridad Informática, Norma NTC ISO 27001:2013
Descripción Trabajo de grado desarrollado con el objetivo de auditar el SGSI de IT Stefanini Colombia.	
Fuentes Bibliográficas	INSTITUTO COLOMBIANO DE NORMALIZACION Y CERTIFICACION. Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos. NTC-ISO/IEC 27001:2013. Bogotá D.C. El instituto 26p. PIATTINI, Mario G.y PESO, Emilio Del. Auditoria Informática un enfoque práctico, 2 edición. Mexico D.F. editorial

	Alfaomega. 2001. 649p. ISBN 978-15-0731-2. SOFTWARE ENGINEERING INSTITUTE. Standard CMMI® Appraisal Method for process Improvement (SCAMPI^{SM}) A, Version 1.3 Method Definition Document. CMU/SEI-2011-HB-001. 2011. United States, 276p

Contenido:

a) Descripción del problema:

¿Por qué la auditoría al sistema de gestión de seguridad información de acuerdo a la norma ISO/IEC 27001:2013 permitirá establecer el estado actual de la seguridad de la información en el proceso de desarrollo de software en la empresa IT STEFANINI COLOMBIA?

b) Objetivo General.

Establecer el estado actual de la gestión de seguridad información en el proceso de desarrollo de software mediante una auditoria interna teniendo como referente la norma ISO/IEC 27001:2013, lo cual permitirá generar un informe final de auditoria con oportunidades de mejora que permitan a la alta dirección contemplar en el plan estratégico la implementación y certificación del estándar ISO 27001:2013.

c) Objetivos Específicos.

- Conocer el funcionamiento de los procesos de desarrollo de software al interior de la empresa para establecer la situación actual en cuanto a la seguridad informática y de la información.
- Elaborar el plan de auditoría y diseñar los instrumentos para recolección de información y pruebas que se llevarán a cabo para determinar los recursos necesarios para llevar a cabo la auditoría al SGSI
- Realizar la evaluación de capacidad y madurez SCAMPI tipo C del proceso según el modelo CMMI L3, aplicar los instrumentos y pruebas de auditoria

que permitan conformar los hallazgos de seguridad encontrados en el proceso de desarrollo de software.

- Elaborar y entregar a la gerencia de IT Stefanini el informe final de auditoria con recomendaciones y observaciones del auditor que permita a la alta dirección contemplar la decisión de implementar y certificar el estándar ISO 27001:2013 en el proceso de desarrollo de software.

d) Resumen de lo desarrollado en el proyecto.

La seguridad de la información es una rama de la informática que se encuentra en auge actualmente y es motivo de preocupación de grandes entidades a nivel global y local, cada día los ataques a las infraestructuras tecnológicas de las organizaciones aumentan de la misma manera que los ataques dirigidos a personas en particular, su objetivo: robo de contraseñas, cuentas de usuario, acceso a información confidencial, secuestro de la información entre otros; el motivo de este trabajo de grado es el exponer al lector una metodología sencilla de para la realización de una auditoria de seguridad de la información basada en la norma NTC ISO IEC 27001:2013 con la cual se aseguran 114 objetivos de control que buscan garantizar los requisitos de seguridad de la información en cualquier sistema de gestión de seguridad de la información conocido por siglas SGSI, a saber “Confidencialidad, Integridad y Disponibilidad de la Información”, para el caso particular de este trabajo se realiza una auditoria de campo a un proceso definido como lo es el proceso de desarrollo de software de la empresa I&T Stefanini S.A en la cual se explora la metodología con la cual opera actualmente el área, y se observa especialmente los aspectos de seguridad de la información que se tienen en cuenta en la operación diaria de las fabricas continuas.

Posteriormente a la observación de estas metodologías se procede a la documentación de los procesos para luego fabricar los instrumentos de auditoria que darán lugar al establecimiento del estado actual del SGSI en esta organización.

Cuando se tabulan estos resultados se puede visualizar el estado actual de cumplimiento a nivel cuantitativo y se procede a la diligenciación del informe final de auditoria el cual es entregado a las directivas de la organización quienes con base en los hallazgos tendrán a decidir si se procede a incluir la mejora y certificación del sistema de gestión de seguridad de la información actual en el plan estratégico del próximo año 2017 , esto permitirá mejorar los procesos internos de la organización tener un mayor reconocimiento en el mercado lo cual

se traducirá en beneficios para clientes y colaboradores.

Para la realización de este trabajo se tuvo en cuenta inicialmente una investigación sobre los estándares definidos en seguridad de la información en la actualidad y los que rigen o se tienen en cuenta en Colombia, posterior a ello se analizó las oportunidades de aplicación de una auditoria en la empresa en la cual desempeña su trabajo el autor logrando la aprobación del mismo por las directivas de la organización.

Desde ese momento se inició con la elaboración de los documentos de auditoria, que se trabajarían durante el proyecto y se investigó en qué manera se pueden enlazar los estándares ya existentes en la organización y que se encuentran certificados actualmente, estos son CMMI 1.3 L3 e ISO 9001:2008, este último ha permitido tener una columna vertebral sobre la cual operar la auditoria del Sistema de gestión de seguridad de la información basándose en la NTC ISO 27001:2013; en cuanto a CMMI este ha permitido observar las prácticas y metodologías de desarrollo de software que se realizan en la organización.

Metodología

Reconocimiento del objeto a auditar.

1. Observación.

Se establece una fase de inicial de observación y acompañamiento a la fábrica de software en la cual se logra detallar el funcionamiento del área, las instalaciones, los equipos y programas utilizados, reconocer al recurso humano que desarrolla la labor y evaluar las medidas de seguridad de la información existentes.

2. Planificación.

Se procede a la realización del plan de auditoria para lo cual se define una fecha inicial y final junto con el área de calidad, infraestructura y los directores de proyectos de la fábrica de software, en ese momento de creación del plan de auditoria se definieron los recursos que se requieran para el desarrollo de la auditoria como son, presupuesto, tiempo, recurso humano, equipos informáticos, instrumentos de auditoria, auditor líder, etc…

3. Ejecución.

Al haber definido los recursos y el plan de auditoria se procede con la ejecución según lo pactado entre las gerencias, la dirección y el equipo auditor definido; durante la auditoria el auditor toma parte objetiva del proceso y toma nota de los hallazgos encontrados para posteriormente elaborar un dictamen preliminar el cual es producto de análisis y revisión por parte del área de Calidad de la organización quien es la encargada de las auditorias y control interno.

4. Informe Final.

Finalmente luego de revisar y analizar los hallazgos con el equipo de calidad se procede a la realización del dictamen final y realización del informe de auditoría en el cual se muestran las oportunidades de mejora en la seguridad de la información del proceso respecto a la norma ISO/IEC 27001:2013, este informe es entregado a la Gerencia General de IT Stefanini para que se implementen las opciones de mejora que permitan contemplar la consolidación del estándar ISO 27001:2013 en el plan estratégico organizacional.

Conclusiones

El diseño de la metodología de la auditoria debe ser claro para permitir un correcto desarrollo durante el tiempo que se lleve a cabo, se debe disponer de los recursos adecuados y los compromisos tanto de la dirección como de los auditados, en el trabajo desarrollado se puede destacar el compromiso de las partes interesadas como la dirección y líderes de procesos relacionados como infraestructura, recursos humanos y las fábricas de desarrollo.

La tarea de auditar un Sistema de gestión cualquiera que sea este es una actividad tediosa y de bastante compromiso, se requiere tener el conocimiento de los procesos y personas a auditar, adicionalmente se requiere conocer el marco legal o normativas que se auditaran ya que no se puede auditar lo que no se conoce, este trabajo de grado ha permitido al autor adentrar en la actividad de la auditoria, comprenderla y ponerla en práctica como futuro especialista en seguridad informática de la UNAD.

Se logra obtener una metodología clara para la realización de auditorías as SGSI, de la misma forma se genera una documentación consistente con el desarrollo de

una auditoria.

El auditor de seguridad informática debe conocer adicionalmente otros marcos de buenas prácticas, tecnologías de apoyo para la auditoria y las amenazas y riesgos actuales o vigentes para detectar factores de exposición a estas que puedan perjudicar el sistema auditado.

La realización de la auditoria documentada en este trabajo de grado ha sido el primer paso en la evaluación y diseño de implementación de un SGSI basado en ISO/IEC 27001:2013, como producto de los hallazgos encontrados se espera la optimización del proceso en cuanto al dominio de seguridad, se espera que el resultado de esta optimización permita la implementación y posterior certificación del sistema frente a un organismo de certificación reconocido.

El especialista en seguridad informática de la UNAD tiene un amplio conocimiento de las tecnologías de apoyo para la seguridad de la información, en este trabajo se evidencio el manejo de los documentos de apoyo como la norma ISO 27001:2013 y el anexo A, adicionalmente otras normas que dictan los procedimientos para la realización de la auditoria de un SGSI como son la ISO 27002:2013, ISO 27003, ISO 27005 e ISO 27006. Adicionalmente se demuestra el manejo de marcos y normas relacionadas como la norma ISO 9001 y CMMI, esto ha permitido aumentar la expectativa de la organización acerca del egresado del programa de especialización en seguridad informática de la UNAD.

Al implementar un SGSI basado en ISO 27001:2013 y certificarlo frente a un ente competente se beneficiará la organización ya que su reputación y reconocimiento en el mercado le permitirá robustecer la marca y abordar una nueva cantidad de negocios que se encuentran en auge actualmente en nuestro país.

El desarrollo de este documento ha permitido encontrar brechas de seguridad en el proceso auditado que por medio de las acciones preventivas y correctivas se espera optimizar los niveles de seguridad aumentando la integridad, confidencialidad y disponibilidad de la información.

Recomendaciones.

Se recomienda la inversión en personal capacitado en Seguridad de la Información de manera Local en Colombia el cual tenga a cargo las actividades de seguridad, apoyo a infraestructura, recursos humanos y al área jurídica, las

cuales se encuentran estrechamente relacionadas en la operación segura de un Sistema de gestión de seguridad en cualquier organización.

Se recomienda a la dirección establecer una estrategia de promoción de la seguridad de la información, esta estrategia debe abordar todas las áreas de la organización desde el momento de la vinculación de personal, promoción a través de los medios institucionales, cursos virtuales, intranet, correo electrónico y posters ubicados en sitios estratégicos, esto permitirá aumentar la sensibilidad del personal de la organización hacia la seguridad de la información.

La inversión en software de control y gobernabilidad de la información en la organización es una opción que debe considerar, esto permitiría llevar un correcto manejo y trazabilidad de las políticas de seguridad de la información, su correcto cumplimiento y gestionar el SGSI de manera local, a estos sistemas se pueden vincular las estadísticas del IDS, de los incidentes detectados por la consola de antivirus y los incidentes de seguridad registrados de manera general.

El área de seguridad de la información debe ser un área independiente de las demás, incluso infraestructura, no se puede confundir las actividades de esta área con las de seguridad de la información si se quiere implementar un ISMS que permanezca actualizado, bajo control y objeto de certificación.

Es muy importante cumplir con cada uno de los controles detallados en la norma, por ello se debe considerar por parte de la dirección realizar las inversiones necesarias para separar las áreas de levantamiento de requerimientos, desarrollo, pruebas y producción de las fábricas de software.

Al separar las áreas es recomendable que a estas áreas solamente pueda acceder personal autorizado por lo cual se deben implementar mecanismos de control para el acceso físico a las instalaciones de las fábricas de software.

Los equipos de las fábricas de software deben poseer un aislamiento especial de internet a través del cortafuegos, no es recomendable que desde los mismos equipos de la fábrica los colaboradores se puedan conectar a correos personales, redes sociales y sitios de almacenamiento en la nube, esto claramente ocasiona una vulnerabilidad de seguridad.

Se recomienda a la dirección establecer un cronograma de auditorías de seguridad de la información de manera periódica en la cual se pueda evaluar el

alcance y cumplimiento de los requisitos de control de la norma, de esta manera se logra preparar el SGSI para la certificación oficial por organismo competente.

Se deben tener en cuenta siempre las auditorias previas en las cuales se pueda encontrar información de hallazgos encontrados con anterioridad y que deban haberse resuelto, esto permite un mayor dominio del proceso, área u organización a auditar.

Siempre se debe apoyar la auditoria contra un marco de buenas prácticas o norma estandarizada vigente, esto asegura que se logren resultados que la industria o la organización espera.

No siempre el objetivo de la implementación de un SGSI o su diagnóstico es lograr una certificación, muchas empresas lo hacen para tener su información segura sin pretender reconocimiento público.

Se recomienda contar con las herramientas informáticas adecuadas para una auditoria debido a que sin ellas difícilmente se podrá realizar un buen diagnóstico del estado actual de un sistema de gestión.

Al desarrollar una auditoria se debe tener en cuenta el mercado del área u organización a auditar con el ánimo de incidir de manera mínima o casi transparente sobre las actividades que el proceso u organización desarrollen.