



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

MAESTRÍA DE EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS II

**“Auditoría interna al SGSI de la CNT E.P. para el proceso de venta
e instalación de productos y servicios de datos e internet para
clientes corporativos en el D.M.Q.”**

TESIS DE GRADO

Autores: Ing. Karina Del Pilar Pabón Molineros

Tutor: Ing. Nancy Velásquez V., MSc

SANGOLQUI, DICIEMBRE 2013

CARTA DE AUSPICIO



Quito, 28 de febrero del 2013


CARTA DE AUSPICIO

Corporación Nacional de Telecomunicaciones

CNT EP

La Corporación Nacional de Telecomunicaciones CNT EP, **AUSPICIA** el Proyecto de Tesis de Grado para obtener el título de Master en Evaluación y Auditoría de Sistemas Tecnológicos en la Escuela Politécnica del Ejército denominada: "**AUDITORÍA INTERNA AL SGSI DE LA CNT E.P. PARA EL PROCESO DE VENTA E INSTALACIÓN DE PRODUCTOS Y SERVICIOS DE DATOS E INTERNET PARA CLIENTES CORPORATIVOS EN EL D.M.Q.**", que será realizado por la Srta. Ing. Karina del Pilar Pabón Molineros, Analista de Soporte de Aplicaciones de la Gerencia de Soporte de TI.

Atentamente,



Ing. José Adrián Pino
**ENCARGADO DE AUDITORIA
INTERNA DEL SGSI – CNT EP**

CONTIGO+
Y Mejor Comunicados

CONVENIO DE CONFIDENCIALIDAD



GERENCIA NACIONAL DE TECNOLOGIAS DE LA INFORMACION
CORPORACION NACIONAL DE TELECOMUNICACIONES CNT EP

CONVENIO DE CONFIDENCIALIDAD


PRIMERA.- COMPARECIENTES:

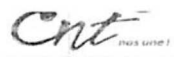
Comparecen a la celebración del presente Convenio de Confidencialidad, por una parte, **Ana Yépez Montalvo**, Representante del Gerente General de la CNT EP para el SGSI en representación de la Corporación Nacional de Telecomunicaciones CNT EP, a quien en adelante y para efectos del presente convenio se lo denominará simplemente "CNT EP"; y, por otra parte, Karina del Pilar Pabón Molineros con CC 1714881958, colaborador de la empresa, a quien en adelante y para efectos del presente convenio se lo denominará simplemente "EL CUSTODIO".

SEGUNDA.- ANTECEDENTES.-

- 2.1. El presente Convenio de Confidencialidad nace por la necesidad de precautelar la información de la CNT EP a la que, la Ing. Pabón tendrá acceso dentro de la auditoría interna al Sistema de Gestión de Seguridad de la Información (SGSI) en la que participará bajo el auspicio de la CNT EP.
- 2.2. La CNT EP se rige por la Ley Orgánica de Empresas Públicas, la misma que en su Art. 20 "PRINCIPIOS QUE ORIENTAN LA ADMINISTRACION DEL TALENTO HUMANO DE LAS EMPRESAS PUBLICAS", numeral 6 establece "*Confidencialidad en la información comercial, empresarial y en general, aquella información, considerada por el Directorio de la empresa pública como estratégica y sensible a los intereses de ésta, desde el punto de vista tecnológico, comercial y de mercado, la misma que goza de la protección del régimen de propiedad intelectual e industrial de acuerdo a los instrumentos internacionales y la Ley de Propiedad Intelectual, con el fin de precautelar la posición de las empresas en el mercado*".
- 2.3. EL CUSTODIO labora en la CNT EP como Analista de Soporte de Aplicaciones de TI, quien maneja y controla información que es considerada como confidencial y en razón de que dentro de sus funciones tiene acceso a distinta información confidencial que la CNT EP así la cataloga, es necesario salvaguardar los intereses de la empresa.
- 2.4. En razón de lo indicado en los subnumerales precedentes, es voluntad de las partes el suscribir el presente Convenio de Confidencialidad, a fin de precisar las obligaciones y responsabilidades que tiene EL CUSTODIO para la CNT EP

TERCERA.- OBJETO.-

Por medio del presente instrumento EL CUSTODIO se obliga expresamente para con la CNT EP a guardar confidencialidad sobre el contenido de toda la información considerada como confidencial, a la que tiene acceso en virtud de los servicios o trabajos que realiza y que le ha sido remitida de manera verbal, visual, por escrito o por cualquier otra forma tangible o intangible. 



GERENCIA NACIONAL DE TECNOLOGIAS DE LA INFORMACION
CORPORACION NACIONAL DE TELECOMUNICACIONES CNT EP

El manejo y custodia de la información confidencial a la que tiene acceso EL CUSTODIO se hará de acuerdo a los siguientes términos:

- 3.1 La información confidencial se mantendrá en absoluta reserva y, bajo ningún concepto, podrá ser divulgada a persona natural o jurídica alguna, ajena a la CNT EP, salvo autorización expresa de ésta última u orden de autoridad pública competente. En este último caso EL CUSTODIO informará a la CNT EP de la existencia de tal requerimiento en el plazo de un día hábil contado desde la fecha de recepción del mismo.

Las obligaciones estipuladas en este Convenio de Confidencialidad no alcanzan a aquella información confidencial que:

- 3.1.1 Sea de dominio público o se convierta en información de dominio público, excepto que lo sea como resultado del incumplimiento a las obligaciones de este Convenio de Confidencialidad;
- 3.1.2 EL CUSTODIO haya tenido acceso o haya producido de modo independiente con anterioridad a este Convenio de Confidencialidad;
- 3.1.3 Aquella que se torne disponible de modo no confidencial y que provenga de una fuente distinta a la CNT EP y sus representantes; o,
- 3.1.4 Fuere desarrollada por EL CUSTODIO o sus allegados, independientemente de o sin referencia a cualquier información confidencial de la CNT EP. En una situación así, EL CUSTODIO deberá tener la carga de la prueba de tal desarrollo independiente.
- 3.2 EL CUSTODIO empleará sus mejores esfuerzos para que la información confidencial de la CNT EP, que esté a su disposición, sea manejada con cautela y para los fines relacionados para los que le haya sido proporcionada dicha información;
- 3.3 EL CUSTODIO se obliga a la custodia de la información confidencial, aplicando las mismas medidas utilizadas en la custodia de la información similar propia;
- 3.4 EL CUSTODIO se obliga a utilizar la información objeto del presente convenio únicamente para los fines para los que le haya sido proporcionada dicha información; y,
- 3.5 Al darse cuenta de cualquier pérdida, uso no autorizado o revelación de la información confidencial de la CNT EP, EL CUSTODIO acuerda adoptar las medidas necesarias para ayudar a la CNT EP, a remediar tal uso no autorizado o revelación de la información confidencial.



GERENCIA NACIONAL DE TECNOLOGIAS DE LA INFORMACION
CORPORACION NACIONAL DE TELECOMUNICACIONES CNT EP

La aplicación de este principio no exime al CUSTODIO de responder judicial y extrajudicialmente respecto de los perjuicios causados a la CNT EP, a causa de la divulgación de información confidencial no autorizada.

CUARTA.- MATERIALES

Todos los materiales incluyendo, sin estar limitada a: documentos, dibujos, modelos, aparatos, esquemas, diseños, listas y cualquier cuerpo tangible que contenga información confidencial de la CNT EP., a las que tenga acceso EL CUSTODIO, deberán ser devueltos a la CNT EP, de acuerdo con las instrucciones razonables de ésta o deberán ser destruidos, incluyendo sus copias, al momento de la terminación de este Convenio o ante el pedido por escrito de la CNT EP.

QUINTA.- ALCANCE DEL CONVENIO

A más de lo antes referido, se considerará como información confidencial al contenido de todo documento o medio que se haya entregado al CUSTODIO, bajo el presente convenio con la leyenda "CONFIDENCIAL". Igual condición tendrá la información que se divulgue en cualquier reunión llevada a cabo entre personal de la CNT EP y EL CUSTODIO.

SEXTA.- NO LICENCIA

Este convenio no confiere al CUSTODIO ninguna licencia para usar la información confidencial de la CNT EP, sino cuenta con autorización para aquello.

SÉPTIMA.- PLAZO

EL CUSTODIO expresamente declara que se obliga a no revelar, difundir o hacer uso en beneficio propio o de terceros, de la información confidencial de la CNT EP salvo los casos previstos en el numeral 3.1 de este Convenio.

El presente Convenio, se entiende vigente a partir de la fecha de su suscripción y terminará en el momento en que la CNT EP así lo decidiere y lo notificare al CUSTODIO. Este Convenio terminará inmediatamente a la recepción de tal notificación, dejándose claramente establecido, que por el hecho de tal terminación, ninguna de las partes deberá a la otra, indemnización alguna, salvo los casos de responsabilidad en que haya incurrido EL CUSTODIO.

Ante la terminación de este Convenio o cuando la CNT EP lo estimare conveniente, EL CUSTODIO cesará inmediatamente el uso de la información confidencial de la CNT EP y cumplirá inmediatamente con lo dispuesto en la Cláusula Cuarta de este Convenio. Ante el pedido de la CNT EP., EL CUSTODIO certificará que ha cumplido con sus obligaciones aquí estipuladas.



GERENCIA NACIONAL DE TECNOLOGIAS DE LA INFORMACION
CORPORACION NACIONAL DE TELECOMUNICACIONES CNT EP

OCTAVA.- DERECHO A INICIAR ACCIONES

En el evento de que se produzca el incumplimiento de lo estipulado en el presente Convenio, la CNT EP tendrá el derecho a iniciar las acciones legales, civiles, penales, o administrativas, de las que se crea asistido, incluyendo la destitución del cargo de EL CUSTODIO por el incumplimiento del presente convenio y/o a la reclamación de daños y perjuicios.

NOVENA.- INDEMNIDAD

EL CUSTODIO reconoce que la divulgación no autorizada de la información confidencial de la CNT EP, que pueda resultar en un perjuicio económico para ésta última, en cuyo caso ésta tendrá derecho al resarcimiento de daños y perjuicios que sea determinado por el Tribunal de Arbitraje o el juez de lo penal, según el caso.

DÉCIMA.- CESIÓN DE DERECHOS

EL CUSTODIO no podrá ceder sus derechos según este convenio, sin el consentimiento previo y por escrito de la CNT EP, salvo el caso de disposición de autoridad competente, en cuyo caso se procederá conforme a lo acordado en el numeral 3.1, de la Cláusula Tercera, de este Convenio.

UNDÉCIMA.- DISPOSICIONES GENERALES

- 11.1 EL CUSTODIO reconoce que la solución para cualquier incumplimiento de los términos de este Convenio se realizará en conformidad con la Ley, y se tendrá especial atención a las disposiciones establecidas en la Ley de Propiedad Intelectual, el Código Penal y demás normativa civil y tratados internacionales ratificados por el Ecuador;
- 11.2 Las partes declaran que, en el evento de incumplimiento o amenaza de los términos de este convenio, la CNT EP, tendrá derecho a iniciar las acciones legales y administrativas que estime del caso y a reclamar por el pago de los correspondientes daños y perjuicios;
- 11.3 Este convenio podrá ser reformado o complementado consensuadamente y por escrito; y,
- 11.4 Si cualquiera estipulación de este Convenio se vuelve inválida o inejecutable, tal estipulación será adecuada por las partes para su ejecución, sin perjuicio de lo cual, el resto del Convenio será mantenido en ejecución total.



GERENCIA NACIONAL DE TECNOLOGIAS DE LA INFORMACION
CORPORACION NACIONAL DE TELECOMUNICACIONES CNT EP

DUODÉCIMA.- LEGISLACIÓN, JURISDICCIÓN Y COMPETENCIA

La Legislación aplicable a este Convenio de Confidencialidad es la ecuatoriana.

Las partes renuncian a utilizar la vía diplomática para todo reclamo relacionado con este Convenio.

Para el caso de controversias relacionadas con la aplicación o interpretación de este convenio, que no sean de carácter penal, los comparecientes renuncian fuero y/o domicilio y se sujetan a la Ley de Arbitraje y Mediación y, en particular, al pronunciamiento de los señores árbitros del Centro de Arbitraje y Mediación de la Procuraduría General del Estado, a cuyo efecto realizan, además, las siguientes precisiones:

- 12.1 El proceso se llevará en la ciudad de Quito, ante el Centro de Arbitraje y Mediación de la Procuraduría General del Estado, conforme su reglamentación interna;
- 12.2 Los árbitros habrán de resolver en derecho;
- 12.3 Los árbitros quedan expresamente facultados para dictar medidas cautelares y para solicitar el auxilio que fuere necesario para ejecutar dichas medidas, en los términos previstos en el Art. 9 de la Ley de Arbitraje y Mediación;
- 12.4 Los costos y gastos en que se incurra, incluidos los honorarios profesionales pactados razonablemente, serán cubiertos por la parte que fuere vencida. A pedido de parte realizado antes de dictar el respectivo laudo, el Tribunal tendrá facultades para regular dichos honorarios, si es que le parecieren considerablemente excesivos o exiguos, en consideración a la cuantía y circunstancias del caso que haya sido puesto en su conocimiento;
- 12.5 Las partes se comprometen a aceptar el Laudo Arbitral. Sin perjuicio del derecho conferido por la Ley ecuatoriana para que la parte afectada pueda demandar la nulidad del laudo, en los casos taxativamente permitidos por dicha Ley, las partes acuerdan que la parte que dedujere un recurso de nulidad que fuere resuelto negativamente para ella, deberá cancelar a la otra parte, a más de todas las obligaciones pendientes o generadas a esa fecha y de aquellas otras obligaciones que, por disposición de la ley, se generasen como efecto de dicha resolución negativa, una indemnización equivalente a la máxima tasa de interés convencional que hubieren generado la suma de todas las citadas obligaciones, desde la fecha de expedición del laudo impugnado, hasta la fecha de pago efectivo. Esta suma será mandada a pagar por el respectivo órgano o juez ejecutor;
- 12.6 De ser requerido, el respectivo laudo será ejecutado ante los jueces competentes de la ciudad de Quito o del lugar en que se encontraren los bienes del ejecutado.



GERENCIA NACIONAL DE TECNOLOGIAS DE LA INFORMACION
CORPORACION NACIONAL DE TELECOMUNICACIONES CNT EP

Para fe y constancia de lo estipulado, las partes suscriben a continuación, en dos ejemplares de igual valor y contenido, en la ciudad de Quito - Ecuador, a 28 de diciembre de 2012

Ana Yépez Montalvo
Representante del Gerente General para el SGSI
CORPORACION NACIONAL DE
TELECOMUNICACIONES CNT EP

Karina Pabón Molineros
Analista de Soporte de Aplicaciones
GERENCIA NACIONAL DE TI

CERTIFICADO DE TUTORÍA

Ing. Nancy Velásquez V., MSc

CERTIFICO:

Que el trabajo titulado “**Auditoría interna al SGSI de la CNT E.P. para el proceso de venta e instalación de productos y servicios de datos e internet para clientes corporativos en el D.M.Q**”, realizado por Karina Del Pilar Pabón Molineros, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas.

Debido a que se ha cumplido con las normas establecidas por la ESPE para el desarrollo del trabajo de conclusión de carrera, se recomienda su publicación.

El mencionado trabajo consta del documento empastado y disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf).

Sangolquí, Abril de 2014

Ing. Nancy Velásquez V., MSc.

DIRECTOR DE PROYECTO

DECLARACIÓN DE RESPONSABILIDAD

Yo, Karina Del Pilar Pabón Molineros

DECLARO QUE:

El proyecto de Maestría denominado “**Auditoría interna al SGSI de la CNT E.P. para el proceso de venta e instalación de productos y servicios de datos e internet para clientes corporativos en el D.M.Q**”, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en el trabajo correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de Maestría en mención.

Sangolquí, Abril de 2014

Ing. Karina Del Pilar Pabón Molineros

AUTORIZACIÓN DE PUBLICACIÓN

Yo, Karina Del Pilar Pabón Molineros

Autorizo a la Universidad de las Fuerzas Armadas la publicación, en la biblioteca virtual de la Institución, del trabajo” **“Auditoría interna al SGSI de la CNT E.P. para el proceso de venta e instalación de productos y servicios de datos e internet para clientes corporativos en el D.M.Q”**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, Abril de 2014

DEDICATORIA

Dedico a mi madre y hermanos este trabajo; que con su apoyo incondicional y su fe depositada en mí, me dieron la seguridad y confianza para culminar esta etapa de mi vida profesional, ellos son el motivo que me impulsa a seguir adelante.

AGRADECIMIENTO

Agradezco a Dios por darme la oportunidad de vivir y hacer realidad este sueño, a mi madre y mis hermanos por su cariño, sus sacrificios y por estar siempre a mi lado, a mis amigos por su apoyo, alegría y amistad incondicional.

Un especial reconocimiento a mi mentora y amiga la Ing. Nancy Velásquez y mi compañero y amigo el Ing. José Adrián Pino por su paciencia, apoyo incondicional, comentarios oportunos y guía a lo largo del desarrollo de este trabajo.

A la Corporación Nacional de Telecomunicaciones CNT EP, por permitirme formar parte de su familia y auspiciar este proyecto depositando su confianza en mí.

A la Escuela Politécnica del Ejército por concederme la satisfacción de crecer como profesional con los conocimientos impartidos durante mi formación de cuarto nivel.

Finalmente quiero agradecer a todas las personas que en algún momento fueron parte de esta etapa de formación, por brindarme una mano, un minuto de su tiempo y lo más importante su cariño.

ÍNDICE GENERAL

CAPÍTULO 1.....	1
1.1. Introducción	1
1.2. Justificación e Importancia	2
1.3. Planteamiento del problema.....	6
1.4. Formulación del problema a resolver.....	6
1.5. Objetivo General	6
1.6. Objetivos Específicos.....	7
CAPÍTULO 2.....	8
2.1. Estado del arte a nivel mundial y local	8
2.2. Marco Teórico.....	25
2.3. Seguridad de la Información	25
2.4. Seguridad de la Información VS. Seguridad Informática	27
2.5. Norma ISO/IEC 27001:2005 Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad - Requerimientos.....	28
Auditoria al SGSI.....	39
2.6. Marco Conceptual	40
2.6.1. Sistema de Gestión de Seguridad de la Información (SGSI)	40
2.7. Auditoria de sistemas de gestión.....	47
CAPÍTULO 3.....	53
3. SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN	53
3.1. Situación actual de la empresa CNT con respecto a la seguridad de la información	53
3.1.1. La empresa CNT	53
3.1.2. Estructura organizacional CNT EP.	59
3.1.3. Área de seguridad de la información	60
3.2. Sistema de Gestión de Seguridad de la Información (SGSI) de la CNT EP.....	61
CAPÍTULO 4.....	71
4.1. Planificar la auditoría interna al SGSI según lo establecido en la Normativa para Auditorías Internas del SGSI.	71
4.2. Elaborar el Plan de Auditoría.....	85

	xiv
4.3. Realizar la auditoría interna.....	97
4.3.1. Reunión de Apertura y actividades.....	97
4.3.2. Realización de Auditoría (25 -02-2013 / 01-03-2013) AI1.....	99
4.3.3. Recopilación de datos (04 -03-2013 / 08-03-2013) AI1.....	102
4.4. Verificación de controles.....	103
4.5. Elaborar el informe de auditoría interna y desarrollar un plan de acción preliminar.....	106
4.6. Presentación de hallazgos a la alta gerencia.....	107
4.6.1. Resumen de Hallazgos Identificados en la Auditoría Interna Febrero AI 1	111
4.6.1.1. Hallazgos.....	111
4.6.1.2. Conclusiones de Auditoría Interna (AI 1).....	120
4.6.1.3. Tratamiento de hallazgos de Auditoría Interna (AI1).....	121
4.6.2. Resumen de Hallazgos Identificados en la Auditoría Interna Septiembre AI 2	123
4.6.2.1. Hallazgos Auditoría Interna (AI 2).....	123
4.6.2.2. Conclusiones de Auditoría Interna (AI 2).....	125
4.6.2.3. Tratamiento de hallazgos (AI2)	126
4.7. Experiencia y Discusión.....	127
4.7.1. Introducción.....	127
4.7.2. Antecedentes.....	129
4.7.3. Situación actual y objetivo de la discusión.....	130
4.7.4. Metodología.....	133
4.7.5. Evaluación de resultados.....	138
4.7.6. Conclusiones y trabajos futuros.....	141
CAPÍTULO 5.....	142
5. CONCLUSIONES Y RECOMENDACIONES.....	142
BIBLIOGRAFÍA.....	146
ANEXOS.....

ÍNDICE TABLAS

Tabla 1. Países vs Certificaciones	20
Tabla 2. Localización geográfica del proyecto de Tesis.	64
Tabla 3. Requisitos de ISO/IEC 27001:2005 - R 4.	75
Tabla 4. Requisitos de ISO/IEC 27001:2005 R5 - R6 - R7 - R8.....	75
Tabla 5. Controles a ser validados en las Auditorias planificadas Anexo A5.	76
Tabla 6. Controles a ser validados en las Auditorias planificadas Anexo A6 – A7.	77
Tabla 7. Controles a ser validados en las Auditorias planificadas Anexo A8 – A9.	78
Tabla 8. Controles a ser validados en las Auditorias planificadas. Anexo A 10 - 15.....	80
Tabla 12. Elaboración de plan de auditoría.	85
Tabla 9. Áreas a ser Auditadas.....	89
Tabla 10. Cronograma de auditoria por áreas.	90
Tabla 11. Delegados por cada área a ser auditada.....	94
Tabla 13. Cronograma de trabajo acordado para.....	98
la realización de auditoria interna.	98
Tabla 14. Cronograma semana 1 Auditoría AI1.	99
Tabla 15. Equipos de trabajo por área a ser auditado.....	99
Tabla 16. Cronograma semana 2 Auditoria.....	102
Tabla 12. Equipos de trabajo por área a ser auditado.....	110
Tabla 16. Hallazgos de Auditoría AI 1.....	111
Tabla 17. Hallazgos de Auditoría AI 2.....	124

Índice Gráficos e Imágenes

Imagen 1. Tomado de la norma BS ISO/IEC 27001:2005.....	10
Gráfico 1. Certificaciones ISO/IEC 27001 a nivel mundial.....	19
Imagen 2. TELCONET EC página pública de Telconet	21
Imagen 3. MOVISTAR página pública de telefónica.	22
Imagen 4. De Seguridad de la Información.....	25
(ITGLOBAL, 2011)).....	25
Imagen 5. Huella electrónica (Legal, 2013).....	27
Imagen 6. Áreas que abarca la seguridad de la Información.....	30
(Deloitte, 2012).....	30
Imagen 7. Modelo PDCA para SGSI.	31
Imagen 8. Conceptos tomados de la norma BS ISO/IEC 27001:2005 - Informe (Deloitte, 2012).....	40
Imagen 9. Beneficios.....	42
Imagen 10. Auditorias	47
Imagen 11.- Logo institucional. Corporación Nacional de Telecomunicaciones.....	53
Imagen 12.- Servicio de Telefonía Fija, Movil y Pública.	56
Imagen 13.- Servicio de Internet Fija y Movil.	57
Imagen 14.- Servicio de Televisión Satelital CNT TV. (Corporación Nacional de Telecomunicaciones CNT EP., 2013)	58
Imagen 15: Estructura Organizacional CNT EP.	59
(Corporación Nacional de Telecomunicaciones CNT EP., 2013).....	59

Imagen 16: Hoja de ruta SGSI CNT EP.....	63
Imagen 17. Captura de pantalla Documento “Metodología de Evaluación de Riesgos” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: confidencial. (CNT EP., 2012)	66
Imagen 18. Captura de pantalla Documento “Informe de Aceptación del Riesgo Residual” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: confidencial.....	67
Imagen 19. Captura de pantalla Documento “Informe de Tratamiento de Riesgos” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: confidencial.....	67
Imagen 20. Captura de pantalla Documento “Declaración de..... Aplicabilidad” alojado en el Sistema MAI, aplicación interna	68
CNT EP. Tipo de documento: confidencial.	68
(CNT EP, 2012)Control 4.3 Requisitos de Documentación.....	68
Imagen 22. Captura de pantalla Documento “Normativa para..... Auditorias Internas al SGSI” alojado en el Sistema MAI,	72
aplicación interna CNT EP. Tipo de documento: confidencial.	72
Imagen 23. Captura de pantalla Documento “Normativa de Auditores internos del SGSI” punto 7, roles y requisitos de auditores internos para el SGSI. Alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial.....	86
Imagen 24. Captura de pantalla Documento “Normativa para Auditores internos del SGSI de la CNT EP”. Alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial.	87
Imagen 25. Captura de pantalla Documento “Procedimiento de Auditorias Internas”. Alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial.	87

Imagen 26. Captura de pantalla Documento “Inventario de Activos de Información” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial.	92
Imagen 27. Captura de pantalla Documento “Inventario de Activos de Información_ objetivos” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial.....	92
Imagen 28. Captura de pantalla de revisión y aprobación de Documento “Plan de Auditoria Interna” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial.	96
Imagen 29. Captura de pantalla del Documento “Procedimiento..... para Acciones Correctivas y Acciones Preventivas” alojado en el Sistema MAI, aplicación interna CNT EP..... Tipo de documento: Confidencial.	106
Imagen 30. Captura de pantalla del Documento “Informe Auditoría..... Interna Enero 2013” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial. AI1 Enero	108
Imagen 31. Captura de pantalla del Documento “Informe Auditoría..... Interna Septiembre 2013” alojado en el Sistema MAI, aplicación..... interna CNT EP. Tipo de documento: Confidencial. AI2 Septiembre	108
Gráfico 3. Hallazgos de Auditoría Interna AI 2 (NC+ = No conformidades mayores; NC- = No Conformidades Menores; OM = Oportunidades de Mejora).....	123
Gráfico 4. No conformidades AI1	131
Imagen 32. Captura de pantalla de boletín interno Medio de Difusión CONTIGO CNT- Seguridad de la Información.....	136

Imagen 33. Captura de pantalla Curso: Seguridad de la Información. Aplicación interna	
CNT EP.	138
Gráfico 5. No conformidades AI2	139
Gráfico 6. Comparación de Resultados entre la	140
Auditoría de Febrero y la Auditoría de Septiembre.	140

RESUMEN

La decisión de una organización de dar el adecuado tratamiento a los riesgos asociados a la seguridad de su información mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para obtener una certificación internacional, es una decisión estratégica, sustentada en el análisis de la naturaleza de la organización, el ámbito donde se desarrolla y produce, las necesidades de la empresa, sus clientes y proveedores, su situación en el mercado y el posicionamiento en el país donde se encuentra. El trabajo debe ser arduo en la implantación del SGSI y más aún en la puesta en marcha y mantención. El presente proyecto apoyará a la Corporación Nacional de Telecomunicaciones CNT EP., en este camino exitoso hacia la certificación internacional bajo la norma ISO/IEC 27001:2005 en la parte de verificación, con lo cual se valorará el estado situacional de su SGSI, elaborando un plan de trabajo de la auditoría interna al sistema de seguridad de la información para el proceso estratégicamente escogido por la organización, verificando la implementación y operación de los controles de acuerdo al Anexo A de la norma ISO/IEC 27001:2005, documentando hallazgos, diferenciando no conformidades mayores, menores y oportunidades de mejora, además emitiendo un informe de hallazgos para presentarlos a la alta dirección, apoyando así a la elaboración del plan de acción a ejecutarse para el cierre de observaciones. También apoyará en la transición de concientizar a toda la organización para que acepte este nuevo reto y se comprometa enteramente en el rol que le toca asumir.

Palabras claves: Auditoría, certificación, SGSI, ISO/IEC 27001:2005,
Hallazgos.

ABSTRACT

The decision of an organization to give the suitable treatment to the risks associated with the Information Security by means of the implementation of an Information Security Management System. (ISMS) to obtain an international certification; is a strategic decision sustained in the analysis of organization's nature, the area where it's develops and produces, company's need, his clients and suppliers, his situation on the market and the positioning in de country. The work must be arduous in the implantation of the ISMS and furthermore in the execution and subsistence. The present project will promote to the Corporación Nacional de Telecomunicaciones CNT EP., in this successful way, towards the international certification under the norm ISO/IEC 27001:2005 in the part of check, it'll value the situational condition of his ISMS, elaborating a work plan of the internal audit to Information Security Management System for the process strategically chosen by the organization, checking the implementation and operation of the controls of agreement to the Annexe To of the norm ISO/IEC 27001:2005, Documenting findings differentiating major, minor non-conformance and opportunities of improvement, issuing a report of findings to present them to the Senior Member, promoting to the production of the action plan to execute for the closing observation. Also it will promote on the transition of sensitizing the whole organization in order that accepts this new agreeing challenge the role that he has to assume.

Keywords: Audit, Certification, ISMS, ISO/IEC 27001:2005, Findings.

CAPÍTULO 1

1.1.1. Introducción

La Corporación Nacional de Telecomunicaciones CNT EP., (en adelante corporación o CNT EP.), decidió dar el adecuado tratamiento a los riesgos asociados a la seguridad de su información mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para obtener la certificación internacional ISO/IEC 27001:2005.

La CNT E.P., necesita obtener esta certificación para satisfacer los nuevos requerimientos del mercado. Los clientes corporativos exigen con mayor frecuencia a los proveedores oferentes de servicios de internet y datos en las licitaciones la certificación en la norma ISO/IEC 27001:2005. Por consiguiente, ésta le permitirá a la CNT EP., alcanzar ventaja competitiva y estratégica en especial en el segmento de clientes corporativos

La corporación desarrolló e implementó un SGSI de acuerdo a las condiciones del negocio y las necesidades de sus clientes, se implantó en aproximadamente ocho meses con el apoyo de consultoría externa y el compromiso de la Gerencia General.

De acuerdo con la norma para alcanzar la certificación internacional la CNT EP debe realizar a intervalos planificados Auditorías Internas a su SGSI para determinar si cumple con los requisitos de la norma ISO/IEC 27001:2005, la legislación y las regulaciones relevantes.

Como premisa inicial, se presumió que la corporación cumplía parcialmente con los requisitos de la Norma ISO/IEC 27001:2005. Para comprobarlo, se realizó el estudio del estado del arte de los Sistemas de Gestión de Seguridad de la Información y el proceso para obtener la certificación internacional ISO/IEC 27000:2005. Se elaboró el plan de trabajo de auditoría interna de acuerdo con lo especificado en la cláusula seis de la norma ISO/IEC 27001:2005, se ejecutó la auditoría interna del SGSI y se analizó los resultados

1.1.2. Justificación e Importancia

De acuerdo a la naturaleza del negocio de la corporación y en base a las necesidades de resguardo de los activos de información, se estableció el SGSI con el siguiente alcance: Venta e instalación de productos y servicios de datos e internet para clientes corporativos en el D.M.Q, definido en el documento “Manual del SGSI”, la Corporación decidió certificarse bajo la norma ISO/IEC 27001:2005, cumpliendo los controles aplicables de la norma los cuales elevarán los atributos de negocio basados en la información estratégica de la empresa apalancados en su misión, visión, estrategia de innovación y transformación empresarial CNT EP 2011 – 2015.

A continuación se listan cada uno de los atributos de negocio con su respectiva descripción:

“Innovación: incrementar la capacidad de encontrar nuevas y mejores maneras para identificar y aprovechar oportunidades de negocio, crecer según las

posibilidades de la corporación, poder interactuar de manera ágil con el entorno y ofrecer nuevos servicios atractivos para los clientes actuales y potenciales

Excelencia en la gestión: asegurar la calidad de los procesos y operaciones, teniendo a disposición información de calidad, ejecutando procesos estandarizados y siendo eficientes en la atención de solicitudes internas y externas, con el objetivo de maximizar los beneficios para los interesados (clientes, sociedad, regulador, accionistas, proveedores, empleados).

Servicio al cliente: generar en los clientes confianza en la corporación y satisfacción en los servicios que se les brinda con base en un manejo de la información alineado con las buenas prácticas de seguridad de la información, una operación confiable y segura, transparencia y buen gobierno; siendo así reconocidos como socios estratégicos de nuestros clientes.

Imagen/reputación: asegurar el cumplimiento de los objetivos estratégicos de la corporación, evitando la difusión de noticias negativas en los medios, protegiendo así el prestigio y los intereses de los accionistas, los clientes, los proveedores y los empleados.” (CNT EP., 2012)

Estos atributos fueron utilizados para realizar el análisis de impacto al negocio y la evaluación de riesgos de seguridad de la información, los mismos que

contribuyeron para establecer los objetivos establecidos en el SGSI, los cuales se detallan a continuación brevemente:

- Administrar los riesgos de seguridad de la información en los activos establecidos por la corporación.
- Evolucionar la seguridad de la información en la CNT EP por medio de la toma de conciencia de todos sus servidores y demás personal relacionado.
- Alinear la orientación estratégico de seguridad de la información con la estrategia del negocio de la CNT EP a través de la identificación y clasificación de los activos de información de la corporación con base en su impacto en los atributos claves del negocio. (CNT EP., 2012)

Estos objetivos fueron creados para apoyar en la orientación estratégica de seguridad de la información con la estrategia del negocio de la empresa, los cuales sin duda, apoyarían a incrementar la percepción de CNT EP., como una empresa que responde a los requerimientos de seguridad de la información de sus partes interesadas (empleados, clientes, proveedores, entes de regulación y control) mediante la implementación de controles de seguridad en los activos de información y al desarrollo de iniciativas de sensibilización al interior de la Corporación, fortaleciendo el funcionamiento seguro de los servicios informáticos brindados a clientes externos e internos de la CNT EP, a través de la gestión de la seguridad de la información acorde con las buenas prácticas y la norma ISO/IEC 27001:2005

Por todos los puntos mencionados, la CNT EP requiere realizar esta auditoría interna para detectar las no conformidades mayores, no conformidades menores y oportunidades de mejora asociadas al SGSI de la CNT EP, con respecto a la Norma ISO/IEC 27001:2005 según los resultados obtenidos determinar la factibilidad de certificación del SGSI de acuerdo a la norma ISO/IEC 27001:2005, se generará un informe de hallazgos de la auditoría interna realizada.

1.1.3. Planteamiento del problema

El no realizar la auditoría interna al SGSI de la CNT EP, implica incumplir el requisito número seis: Auditorías Internas de la norma internacional ISO/IEC 27001:2005, el mismo que es mandatorio y paso previo a la auditoría de certificación a ser realizada por una entidad certificadora.

1.1.4. Formulación del problema a resolver

La problemática se centra en tres preguntas:

- ¿El Sistema de Gestión de Seguridad de la Información de la CNT EP cumple con los requisitos de la Norma ISO/IEC 27001:2005?
- ¿Los controles del SGSI de la CNT EP, han sido implementados de acuerdo a lo establecido por la Norma ISO/IEC 27001:2005?
- ¿Se han implementado las acciones correctivas al SGSI de la CNT EP? detectadas en la pre auditoría realizada por Deloitte.

1.1.5. Objetivo General

Detectar las no conformidades mayores, no conformidades menores y oportunidades de mejora asociadas al SGSI de la CNT EP, con respecto a la Norma ISO/IEC 27001:2005 por medio de la auditoría interna

1.1.6. Objetivos Específicos

- Elaborar el plan de trabajo de la auditoria interna al SGSI de la CNT EP, una vez realizada la revisión documental del SGSI en cada una de las áreas involucradas.
- Verificar la implementación y operación de los controles especificados en los Anexos A5 al A15 de la Norma ISO/IEC 27001:2005:2005.
- Documentar los hallazgos diferenciando no conformidades mayores, no conformidades menores, oportunidades de mejora y observaciones.
- Informar los hallazgos a la alta dirección.

CAPÍTULO 2

2.1.1. Estado del arte a nivel mundial y local

Al hablar sobre seguridad de la información, llega a la mente modelos de seguridad tradicionales que se enfocan en la seguridad externa y en mantener alejados a los atacantes externos, colocando en un nivel de menor importancia a las amenazas que se encuentran dentro de la organización, según la apreciación de Deloitte:

“Las principales fallas de seguridad son:

- Violaciones de seguridad que involucra a terceros - 25 %
- Errores de los empleados u omisiones - 20 %
- Adaptación tardía a nuevas tecnologías - 18 %
- Abuso del empleado de los sistemas e información de TI - 17 %
- Otros - 20%” (Deloitte, 2012)

El hecho de que exista la factibilidad de acceso a la información por medios como: las redes sociales, teléfonos móviles, computación en la nube, ha causado que el entorno de riesgo para las organizaciones cambie de acuerdo con el avance de la tecnología.

Con este antecedente tenemos los siguientes cuestionamientos:

- ¿Cuál es el nivel aceptable de riesgo asociado a los activos de información, donde la marca de una organización está en juego?
- ¿La solución es prohibir los accesos para reducir los riesgos?
- En verdad, ¿es necesario retrasarnos tecnológicamente para protegernos en el futuro?

La seguridad de la información debe estar alineada estratégicamente con las necesidades del negocio; no solo depende del área de tecnología (TI), es un tema organizacional y las respuestas se deben buscar en base al nivel de tolerancia de riesgos de la empresa.

La seguridad de la información no es solamente implementación de controles, es la gestión para proteger la información. La unificación de todas las áreas impactadas y el compromiso de la alta dirección al enfocarse en la protección proactiva y equilibrada entre el uso de los recursos de la empresa y lo que requiere la organización.

La tendencia de seguridad de la información actualmente es aumentar la confianza de nuestros clientes, proveedores y socios de una manera sustentable. Los ataques serán inevitables, pero las organizaciones deben enfocarse en soluciones que planeen, protejan, predigan y respondan ante las amenazas. Es por esto, que se hace necesario implantar sistemas que abarquen estas tareas de forma metódica, documentada y basada en objetivos de seguridad y evaluación continua de riesgos que

abarque personas, procesos y tecnología a los que esté sometida la información de la organización.

La familia de Normas ISO/IEC 27000 son estándares desarrollados por (*International Organization for Standardization ISO*) quienes son el organismo encargado de promover el desarrollo de normas internacionales de fabricación tanto de productos como de servicios, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional que proporcionan un marco de referencia de la gestión de la seguridad de la información que pueden ser implementados en cualquier empresa sea pequeña, mediana o grande y cualquiera sea su naturaleza.



Imagen 1. Tomado de la norma BS ISO/IEC 27001:2005.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión

de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña y sin importar el tipo de industria en el que se desempeñan.

Dentro de la familia de las ISO 27000 se pueden encontrar:

ISO/IEC 27000: Proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción del ciclo Plan-Do-Check-Act y términos y definiciones que se emplean en toda la serie 27000.

ISO/IEC 27001: Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (actualmente anulada) y es la norma que permite certificar a las organizaciones, por medio de auditores externos. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO/IEC 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Este estándar internacional puede ser aplicado e implementado en cualquier organización, sin importar su tamaño o naturaleza.

ISO/IEC 27002: Es el nuevo nombre de ISO/IEC 17799:2005, es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

ISO/IEC 27003: No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

ISO/IEC 27004: No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

ISO/IEC 27005: Publicada en segunda edición el 1 de Junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

ISO/IEC 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

ISO/IEC 27007: No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO/IEC 19011.

ISO/IEC TR 27008: No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

ISO/IEC 27010: Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información.

ISO/IEC 27011: Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002.

ISO/IEC 27013: Es una guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

ISO/IEC 27014: En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía de gobierno corporativo de la seguridad de la información.

ISO/IEC TR 27015: Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002.

ISO/IEC TR 27016: En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía de valoración de los aspectos financieros de la seguridad de la información.

ISO/IEC TS 27017: En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía de seguridad para Cloud Computing.

ISO/IEC 27018: En fase de desarrollo, con publicación prevista en 2013. Consistirá en un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.

ISO/IEC TR 27019: En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía con referencia a ISO/IEC 27002 para el proceso de control de sistemas específicos al sector de la industria de la energía.

ISO/IEC 27031: No certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio.

ISO/IEC 27032: Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus

dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP). Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de Seguridad Cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad.

ISO/IEC 27033: Parcialmente desarrollada. Norma dedicada a la seguridad en redes, consistente en 7 partes: 27033-1, conceptos generales; 27033-2, directrices de diseño e implementación de seguridad en redes; 27033-3, escenarios de referencia de redes; 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad; 27033-5, aseguramiento de comunicaciones mediante VPNs; 27033-6, convergencia IP (prevista para 2013); 27033-7, redes inalámbricas (prevista para 2013).

ISO/IEC 27034: Parcialmente desarrollada. Norma dedicada la seguridad en aplicaciones informáticas, consistente en 5 partes: 27034-1, conceptos generales; 27034-2, marco normativo de la organización; 27034-3, proceso de gestión de seguridad en aplicaciones (sin previsión de publicación); 27034-4, validación de la

seguridad en aplicaciones (sin previsión de publicación); 27034-5, estructura de datos de protocolos y controles de seguridad de aplicaciones (sin previsión de publicación).

ISO/IEC 27035: Proporciona una guía sobre la gestión de incidentes de seguridad en la información.

ISO/IEC 27036: En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía en cuatro partes de seguridad en las relaciones con proveedores: 27036-1, visión general y conceptos; 27036-2, requisitos comunes; 27036-3, seguridad en la cadena de suministro TIC; 27036-4, seguridad en outsourcing (externalización de servicios).

ISO/IEC 27037: Publicada el 15 de Octubre de 2012. Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

ISO/IEC 27038: En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía de especificación para seguridad en la redacción digital.

ISO/IEC 27039: En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).

ISO/IEC 27040: En fase de desarrollo, con publicación prevista no antes de 2014. Consistirá en una guía para la seguridad en medios de almacenamiento.

ISO/IEC 27041: En fase de desarrollo, con publicación prevista no antes de 2014. Consistirá en una guía para la garantizar la idoneidad y adecuación de los métodos de investigación.

ISO/IEC 27042: En fase de desarrollo, con publicación prevista no antes de 2014. Consistirá en una guía con directrices para el análisis e interpretación de las evidencias digitales.

ISO/IEC 27044: En fase de desarrollo, con publicación prevista no antes de 2014. Gestión de eventos y de la seguridad de la información - Security Information and Event Management (SIEM).

ISO 27799: Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes.

Para cubrir los objetivos, se utiliza la norma ISO/IEC 27001:2005 que nos especifica los requisitos para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) y el Anexo A con los respectivos controles.

La información crítica de una empresa está presente en los sistemas informáticos, pero también en papel, en diferentes tipos de archivos y soportes, se transmite a terceros, se muestra en diversos formatos audiovisuales, se comparte en conversaciones telefónicas y reuniones y está presente en el propio conocimiento y experiencia de los trabajadores. ISO/IEC 27001:2005 propone un marco de gestión de la seguridad de toda la información de la empresa en donde su objetivo principal es minimizar los riesgos para la empresa en cuanto a pérdida de dinero, pérdida de imagen, pérdida de clientes, pérdida de la confidencialidad, integridad y disponibilidad de la información.

La presencia masiva de sistemas informáticos en el tratamiento de la información lleva a menudo a centrar la atención sólo en la seguridad informática, dejando así expuesta información esencial que no fluye por los sistemas de información que se enmarca en lo que es la seguridad de la información que abarca los procesos, las personas y la demás documentación física. Por ende la aplicación de controles considera temas como los aspectos organizativos, la clasificación de la información, la inclusión de la seguridad en las responsabilidades laborales, la

formación en seguridad de la información, la conformidad con los requisitos legales o la seguridad física, además de controles propiamente técnicos.

Con el rápido avance de la ciencia y la tecnología, cada día las organizaciones están dando mayor importancia al control en la seguridad de la información, una empresa para ser competitiva debe satisfacer los requisitos de los clientes entregándole cumplimiento en sus requisitos y eficiencia en los procesos.

La implementación de un sistema de gestión es una decisión estratégica que debe involucrar a toda la organización y que debe ser dirigida y apoyada desde la dirección.

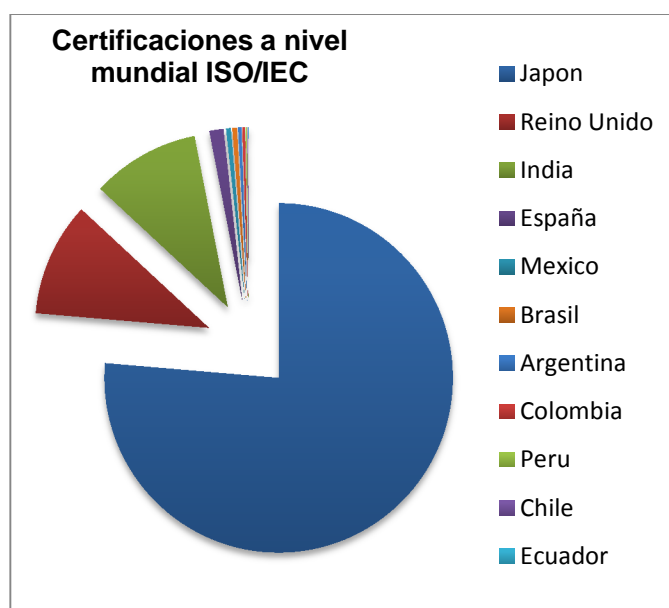


Gráfico 1. Certificaciones ISO/IEC 27001 a nivel mundial.

La auditoría interna es la herramienta para verificar que el SGSI cumpla con los requisitos de la norma, y el primer paso para solicitar la auditoría de certificación a una empresa acreditada.

De acuerdo al registro de *International Register of ISMS Certificates* para el agosto del 2012 existen 7940 organizaciones con certificación ISO/IEC 27001:2005 en el mundo. La lista se encuentra encabezada por Japón con 4152 certificaciones, seguido de Reino Unido con 573 certificaciones e India con 546 certificaciones.

Entre los países latinoamericanos y de habla hispana, España encabeza la lista con 72 certificaciones, México con 25, Brasil con 24, Argentina con 17, Colombia con 14, Perú con 7, Chile con 5, Ecuador con 2 y Bolivia con 1 certificación.

Tabla 1. Países vs Certificaciones

PAÍSES	CERTIFICACIONES
Japón	4152
Reino Unido	573
India	546
España	72
México	25
Brasil	24
Argentina	17
Colombia	14
Perú	7
Chile	5
Ecuador	2
Bolivia	1

En Ecuador, existen dos empresas que han conseguido la certificación en sistemas de seguridad de la información.

1. **TELCONET**, es una empresa que brinda servicios de telecomunicaciones con un portafolio de servicios ofrecido a través de NGN (Next Generation Networking) cuya misión se enfoca en proveer servicios de comunicación de video, voz y datos.

Obtuvieron la certificación ISO/IEC 27001:2005 en el año 2008 su política de seguridad es:

"Proveer servicios de telecomunicaciones con un sistema de gestión de seguridad de la Información basado en la prevención y enfocado en minimizar el riesgo de incidentes que atenten contra la confidencialidad, integridad y disponibilidad de Telconet". (Telconet, 2013)



Imagen 2. TELCONET EC página pública de Telconet

2. **MOVISTAR – TELEFÓNICA EC** es la segunda empresa que obtuvo la certificación, la cual brinda servicios de telefonía móvil e internet y datos. Telefónica posee todo un sistema de gestión integrado con certificaciones en cuatro áreas: calidad

de procesos (ISO 9001:2000), ambiental (ISO 14000); seguridad y salud ocupacional (OHSAS 18000) y seguridad en la información (ISO/IEC 27001:2005). Esta última fue obtenida en el segundo semestre del 2012. (TELEFÓNICA, 2013)



Imagen 3. MOVISTAR página pública de telefónica.

Beneficios:

Para una empresa, los beneficios de implementar las normas ISO 9001, ISO 14001 e ISO/IEC 27001:2005 dentro de un sistema integrado de gestión se verán reflejados en:

- Posicionamiento de la organización en el mercado.
- Confianza y satisfacción de los clientes.
- Seguridad, eficiencia y productividad en la gestión organizacional.
- Aumento de la eficiencia del uso de los recursos de los procesos que forman parte de los sistemas de gestión.
- Mejora en la capacidad de reacción de la organización frente a posibles amenazas contra sus sistemas documentales e información confidencial.
- Reducción de recursos y de tiempo empleado en la realización de los procesos integrados.

- Reducción de costos en el mantenimiento del sistema y de evaluación externa, simplificación del proceso de auditoría.
- Menos costos en consultoría de implementación.
- Menos horas de trabajo interno por parte de la organización.
- Aumento de control interno.
- Cambio de cultura organizacional.
- Reducir impacto en la organización cuando un riesgo se materializa.
- Soporta la continuidad del negocio.

Los beneficios anteriores debido a que los clientes al saber que una empresa está certificada en cualquiera de estas normas o en las tres, sienten confianza y respaldo en que los servicios y productos ofrecidos cuentan con procedimientos y controles basados en estándares internacionales que permiten minimizar los riesgos y buscar la excelencia.

Debido a que la ISO/IEC 27001:2005 es un estándar internacional que brinda lineamientos para implementar un sistema de gestión de seguridad de la información, puede ser aplicado e implementado en cualquier organización cuyos procesos requieran de información para llevarse a cabo.

Como parte del presente proyecto se realizó una investigación por muestreo donde se tomaron las licitaciones en las que la CNT EP participó en el año 2011 y se encontró que más del 50% de los clientes corporativos demandan que su proveedor de servicios de internet y datos cuenten con la certificación ISO/IEC 27001:2005.

Por lo tanto, se determina que el área de tecnología que es donde cada organización se basa en sus procesos y sistemas. En muchos países como España, se han promulgado leyes de protección y privacidad de la información, haciendo que las empresas tengan como requisito legal implementar servicios de control y protección de la información, no solo por cumplir con los requisitos legales, sino porque los datos de los clientes y la información de las organizaciones son unos de los principales activos de estas empresas.

2.1.2. Marco Teórico

2.1.3. Seguridad de la Información

La Seguridad de la Información consiste en proteger uno de los activos más importantes del negocio, la información. Sin embargo debemos recalcar la distinción con lo que significa “Seguridad Informática”.



Imagen 4. De Seguridad de la Información.

(ITGLOBAL, 2011))

Seguridad Informática: es la protección de las infraestructuras tecnológicas, aplicaciones, sistemas operativos y base de datos sobre las que funciona la empresa.
Seguridad de la Información: tiene como objetivo la protección de los activos de información como: documentos físicos, hardware, software y personas entre otros. Basada en que la información es clave importante para una organización para la operación y el cumplimiento de sus objetivos.

No es fácil controlar las vulnerabilidades asociadas a los activos de información, convirtiéndose en una tarea ardua de realizar pero que cuya respuesta se centra en un sistema de gestión de seguridad de la información.

Un Sistema de Gestión aplicado a la Seguridad de la Información (SGSI), tiene como objetivo mantener siempre el riesgo por debajo de umbrales asumidos por la organización. Para esto es necesario implementar controles que mitiguen riesgos asociados a la integridad, disponibilidad y confidencialidad asociados a los activos de información, sin olvidar que la eficacia de estos controles depende de una revisión periódica, incorporando mejoras constantemente y siempre bajo las directrices de una política de seguridad definida por la empresa.

Los costes derivados de la pérdida de la información no son sólo económicos directos, sino que también afectan a la imagen de la empresa, por lo que, cada vez más, la seguridad de la información forma parte de los objetivos de las organizaciones, sin embargo, a pesar de esa concienciación generalizada, aún muchas compañías no enfrentan este aspecto con la globalidad con la que debe tratarse.

Existe otro factor que afecta a la estrategia de seguridad de una organización, las inversiones realizadas en materia de seguridad de la información a menudo no se ejecutan en base a una planificación de tratamiento de riesgos, lo cual no permite generar trazabilidad entre el control implementado y el activo de información a proteger.

El punto fundamental de partida con garantía de éxito para el establecimiento y mantenimiento de la seguridad de la información es definir claramente objetivos a partir de los cuales debe desarrollar políticas que definan el marco para implementar

medidas de seguridad, teniendo en cuenta aspectos como las leyes y regulaciones que rigen a la organización.

2.1.4. Seguridad de la Información VS. Seguridad Informática

A primera vista "Seguridad Informática" y "Seguridad de la Información" pueden parecer exactamente lo mismo, sobre todo si se tiene en cuenta que el desarrollo y la evolución de la tecnología tienden hacia el modelo de "digitalizar" y "manejar" cualquier tipo de información mediante un sistema informático. No obstante, aunque están destinados a vivir en armonía y trabajar conjuntamente, cada uno de las áreas de seguridad tiene objetivos y actividades diferentes.



Imagen 5. Huella electrónica (Legal, 2013)

Como conclusión la Seguridad de la Información es la disciplina que se encarga de tratar riesgos asociados a la confidencialidad, integridad y disponibilidad de los activos de información. Mientras que la seguridad informática se encarga de tratar riesgos sobre activos tecnológicos; por consiguiente la seguridad de la información contiene a la seguridad informática.

2.1.5. Norma ISO/IEC 27001:2005 Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad - Requerimientos

ISO/IEC 27001 proporciona los requerimientos para el sistema de gestión de la seguridad de la información que permita a la organización establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un SGSI documentado dentro del contexto del conjunto de los riesgos de la actividad de una organización.

ISO/IEC 27001:2005 se diseña para “asegurar un adecuado y proporcionado control de la seguridad que proteja adecuadamente los activos de información y dar confianza a los clientes y otras partes interesadas.” (27001:2005, 2005)

Es aplicable a cualquier organización, independientemente de su tipo, tamaño y la naturaleza de su actividad.

La norma ISO/IEC 27001:2005 define cómo organizar la seguridad de la información en cualquier tipo de organización: con o sin fines de lucro, privados o públicos, pequeños o grandes. Siendo hoy en día la norma que constituye la base para la gestión de la seguridad de la información.

La ISO/IEC 27001:2005 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una

organización. También permite que una organización se certifique, lo cual significa que una entidad de certificación independiente comprueba que la empresa ha definido e implementado el SGSI de acuerdo a la norma ISO/IEC 27001:2005.

La Norma ISO/IEC 27001:2005 es un estándar internacional preparado por el Comité Técnico Conjunto ISO/IEC JTC, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad TI.

Este estándar proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción del SGSI debe ser una decisión estratégica de la organización cuyo diseño e implementación es influenciado por las necesidades y objetivos del negocio, requisitos de seguridad.

La norma específica el enfoque por procesos para la gestión de la seguridad de la información, enfatiza la importancia de entender los requisitos de seguridad de la información de la organización y la necesidad de establecer una política y objetivos para seguridad de la información, implementar controles para manejar los riesgos de seguridad, el monitoreo y revisión de desempeño del SGSI y el mejoramiento continuo en base a la medición del objetivo.



Imagen 6. Áreas que abarca la seguridad de la Información.

(Deloitte, 2012)

ISO/IEC 27001:2005 adopta el modelo del proceso PDCA (Plan – Do – Check –Act) Planear, Hacer, Chequear, Actuar, el cual se aplica en todos los procesos SGSI. (27001:2005, 2005)

La imagen 2, muestra el modelo PDCA además de los vínculos en los procesos presentados en las Clausulas 4, 5, 6, 7 y 8 de la Norma ISO/IEC 27001:2005.

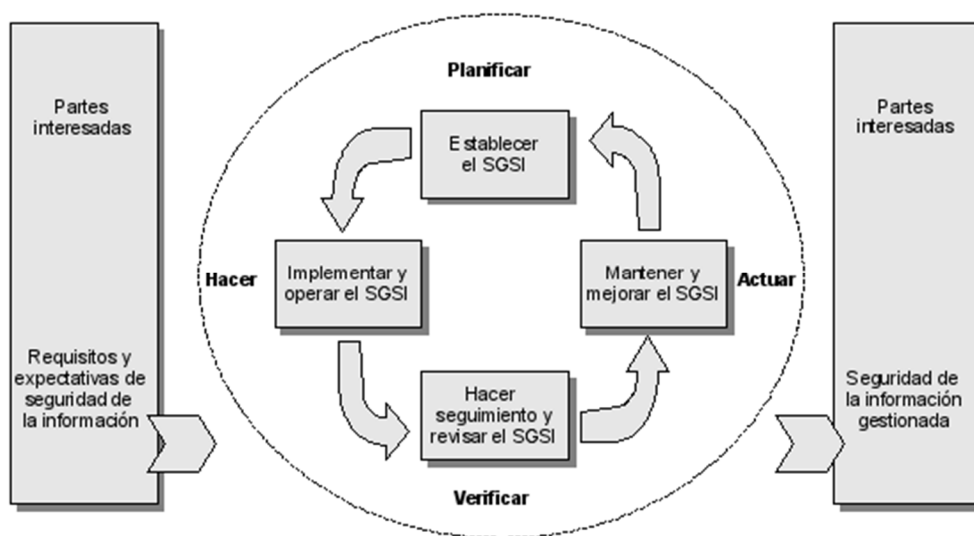


Imagen 7. Modelo PDCA para SGSI.

Este estándar proporciona un modelo sólido para implementar la evaluación de riesgo, diseño e implementación de seguridad y re-evaluación de seguridad.

Componentes

Requisitos: Los requisitos indicados en este estándar son genéricos y aplicables para cualquier organización para lo cual no es aceptable la exclusión de ningún requisito especificado en la norma.

Contiene las cláusulas descritas a continuación:

Clausula 4: Sistema de gestión de seguridad de la información

“La organización debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrentan.”

Clausula 5: Responsabilidad de la gerencia

“Compromiso de la gerencia

La gerencia debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI al:

- a) establecer una política SGSI;
- b) asegurar que se establezcan objetivos y planes SGSI;
- c) establecer roles y responsabilidades para la seguridad de información;
- d) comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y cumplir la política de seguridad de la información, sus responsabilidades bajo la ley y la necesidad de un mejoramiento continuo;
- e) proporcionar los recursos suficientes para desarrollar, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI;

f) decidir el criterio para la aceptación del riesgo y los niveles de riesgo aceptables;

g) asegurar que se realicen las auditorías internas SGSI; y

h) realizar revisiones gerenciales del SGSI. ” (27001:2005, 2005)

Clausula 6: Auditorías internas SGSI

“La organización debe realizar auditorías internas SGSI a intervalos planeados para determinar si los objetivos de control, controles, procesos y procedimientos del SGSI:

a) cumplen con los requisitos de este Estándar Internacional y la legislación y regulaciones relevantes;

b) cumplen con los requisitos de seguridad de la información identificados;

c) se implementan y mantienen de manera efectiva; y

d) se realizan conforme lo esperado.

Se debe planear un programa de auditoría tomando en consideración el estatus e importancia de los procesos y áreas a ser auditados, así como los resultados de auditorías previas. Se debe definir el criterio, alcance, frecuencia y métodos de auditoría. La selección de los auditores y la realización de las auditorías deben asegurar

la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo.

Las responsabilidades y requisitos para la planeación y realización de las auditorías, y para el reporte de resultados y mantenimiento de registros se deben definir en un procedimiento documentado.

La gerencia responsable para el área siendo auditada debe asegurar que se den sin demora las acciones para eliminar las no-conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el reporte de los resultados de verificación.”

Clausula 7: Revisión Gerencial del SGSI

“La gerencia debe revisar el SGSI de la organización a intervalos planeados (por lo menos una vez al año) para asegurarse de su continua idoneidad, conveniencia y efectividad. Esta revisión debe incluir oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad de la información. Los resultados de las revisiones deben documentarse claramente y se deben mantener registros”.

Clausula 8: Mejoramiento del SGSI

“8.1 Mejoramiento continuo

La organización debe mejorar continuamente la efectividad del SGSI a través del uso de la política de seguridad de la información, objetivos de seguridad de la información, resultados de auditoría, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión gerencial.

8.2 Acción correctiva

La organización debe realizar las acciones para eliminar la causa de las no-conformidades con los requisitos del SGSI para poder evitar la recurrencia. El procedimiento documentado para la acción correctiva debe definir los requisitos para:

- a) identificar las no-conformidades;
- b) determinar las causas de las no-conformidades;
- c) evaluar la necesidad de acciones para asegurar que las no-conformidades no vuelvan a ocurrir;
- d) determinar e implementar la acción correctiva necesaria;
- e) registrar los resultados de la acción tomada; y
- f) revisar la acción correctiva tomada.

8.3 Acción preventiva

La organización debe determinar la acción para eliminar la causa de las no-conformidades potenciales de los requisitos SGSI para evitar su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas para el impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir los requisitos para:

- a) identificar las no-conformidades potenciales y sus causas;
- b) evaluar la necesidad para la acción para evitar la ocurrencia de no-conformidades;
- c) determinar e implementar la acción preventiva necesaria;
- d) registrar los resultados de la acción tomada; y
- e) Revisar la acción preventiva tomada.”

Cualquier exclusión de los requisitos para satisfacer el criterio de aceptación del riesgo tiene que ser justificada y debe ser debidamente evidenciada que los riesgos asociados han sido aceptados por los responsables.

Controles: Control es lo que permite garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable.

El estándar internacional ISO/IEC 27001:2005 especifica en su “Anexo A” un listado completo de objetivos de control y los controles de cada uno de ellos, los mismos que se alinean con ISO/IEC 27002:2005 Cláusulas del 5 al 15. Las listas en la Tabla A.1 no son muy grandes por lo que la organización puede considerar o no todos los controles o adicionar algunos si los requiere.

Los objetivos de control y los controles de estas tablas deben seleccionarse como parte del proceso SGSI especificado en el requisito 4 (Sistema de gestión de seguridad de la información) en el punto 4.2.1 (Establecer y manejar el SGSI) de la norma.

Cabe mencionar que el anexo A proporciona una base de referencia de 133 controles que son los mínimos que se deberán aplicar, o justificar su no aplicación, pero cabe especificar que si a través de la evaluación de riesgos se determina que es necesaria la creación de nuevos controles, la implantación del SGSI impondrá la inclusión de los mismos, sino seguramente el ciclo no estará cerrado y presentará huecos claramente identificables.

Los controles del Anexo A están agrupados en los siguientes dominios:

A.5 Política de seguridad

A.6 Organización de la información de seguridad

A.7 Administración de recursos

A.8 Seguridad de los recursos humanos

A.9 Seguridad física y del entorno

A.10 Administración de las comunicaciones y operaciones

A.11 Control de accesos

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

A.13 Administración de los incidentes de seguridad

A.14 Administración de la continuidad de negocio

A.15 Cumplimiento (legales, de estándares, técnicas y auditorías).

Auditoría al SGSI

En la tradicional auditoría de sistemas, el auditor aplica directamente las herramientas de auditoría o sus mejores prácticas para comprobar la solidez del sistema. Incide de forma clara para determinar incumplimientos, en las auditorías de seguridad se explora para determinar agujeros de seguridad y amenazas. Se utilizan técnicas de hacking ético, aplicaciones específicas u otras de ingeniería social y muchas herramientas más.

En la Auditoría Interna del **SGSI** existen varias diferencias con las anteriores, está orientada hacia la mejora continua del SGSI, se basa en actividades que aporten hallazgos para la gestión de la seguridad. Requiere personal cualificado como auditor de la norma ISO/IEC 27001:2005, en auditoría de sistemas de gestión, en los procesos del negocio a ser auditados.

Resumiendo, la Auditoría de Sistemas Informáticos tiene una vertiente más técnica y se centra en la verificación de controles en el procesamiento de la información en sistemas informáticos, incidiendo sobre los mismos para poder evaluar su eficacia y poder presentar el correspondiente informe a la alta dirección, la Auditoría Interna del SGSI se enfoca a la mejora continua del Sistema de Gestión de Seguridad de la Información.

2.1.6. Marco Conceptual

2.1.7. Sistema de Gestión de Seguridad de la Información (SGSI)

Los sistemas de gestión de la seguridad de la información (SGSI) proveen a las organizaciones los elementos para gestionar de manera efectiva la seguridad de la información

El SGSI debe ayudar al mantenimiento y la mejora de las oportunidades competitivas, los movimientos monetarios, la rentabilidad, el cumplimiento legal y la imagen corporativa.



Imagen 8. Conceptos tomados de la norma BS ISO/IEC 27001:2005 - Informe (Deloitte, 2012)

El desarrollo de un SGSI representa un acercamiento “proactivo”, sistemático y lógico para dirigir los problemas de la seguridad de la información, en sustitución de un lento acercamiento “reactivo” a las brechas de seguridad.

Las organizaciones están sometidas a amenazas internas y externas y existe el riesgo de que se materialicen.

La organización puede responder mediante:

- Políticas y visiones corporativas;
- Cultura y valores corporativos;
- Marketing y comunicación;
- SGSI.

El SGSI se entiende como un entorno de trabajo para la organización que necesita de un seguimiento continuo y de revisión periódica para proveerlo de una dirección efectiva para las actividades de la organización en materia de seguridad de la información y como repuesta a los cambios internos y a los factores externos. Cada individuo en cada organización debe aceptar las responsabilidades en las mejoras de la seguridad de la información.

Beneficios del SGSI

El establecimiento y funcionamiento de un SGSI por sí mismo no necesariamente obtiene como resultado una inmediata reducción de los riesgos adversos de la seguridad de la información. En esencia, un SGSI es una herramienta que otorga a la organización de la capacidad de lograr controlar sistemáticamente un nivel de seguridad de la información implantado.



Imagen 9. Beneficios

El sistema debe proporcionar beneficios económicos tales como:

- Incrementa el conocimiento en seguridad de la información.
- Minimiza los riesgos en materia de confidencialidad, integridad y disponibilidad de la información.
- Reduce el tiempo de investigación de las brechas de seguridad.
- Mejora continua de la seguridad de la información, mediante la supervisión, revisión y eficacia de los procesos implantados.
- Aporta un valor añadido y/o diferencial a la organización.
- Reduce el adiestramiento del personal nuevo.
- Reduce litigios.
- Exterioriza una clara vocación del cumplimiento de leyes y regulaciones.
- Certifica una especial solvencia técnica en materia de seguridad de la información.

- Incrementa la confianza de los clientes y las partes interesadas.

Una vez que se obtiene la certificación del SGSI según la norma ISO/IEC 27001:2005 a través de un organismo independiente, la organización obtiene unos beneficios tales como:

- Incremento de la imagen corporativa.
- Perfil mejorado y credibilidad.
- Ventaja competitiva en el posicionamiento de mercado.

Alcance

Según el requisito cuatro de la ISO/IEC 27001:2005 el SGSI requiere definir un alcance tanto a nivel de procesos como a nivel geográfico. La organización que selecciona el proceso prioritario a controlar los riesgos de negocio y la ubicación geográfica.

Aplicación

Los requerimientos son genéricos y aplicables a todas las organizaciones, sea cual sea su tipología, tamaño y producto o servicio ofrecido. Cuando alguno de los requerimientos no pueda ser aplicado “debido a la naturaleza de la organización y su actividad” estos deben ser considerados por exclusión y detallados en el documento “declaración de aplicabilidad” de la organización.

Implementación

Para la implementación de un SGSI, se debe considerar los siguientes puntos esenciales:

- Definir el alcance del SGSI.
- Establecer el compromiso y la completa aplicación de la Alta dirección en el proyecto desde el inicio hasta el fin.
- Establecer el nivel de seguridad deseado, tamaño y complejidad de la organización.

Como se había mencionado anteriormente, el estándar internacional adopta el modelo PDCA el mismo que menciona que no es suficiente con el diseño e implementación del SGSI, sino que es necesario garantizar la revisión periódica y realiza una continua actualización y mejora del mismo, permitiendo a cada

organización utilizar los instrumentos que consideren oportunos para medir y controlar la mejora el sistema.

Un SGSI debe identificar fundamentalmente, los objetivos y alcance del sistema, los procesos de negocio críticos para la organización.

Certificación

La certificación del SGSI favorece a fomentar las actividades y procesos de protección de la información dentro de las organizaciones, mejorando su imagen y generando confianza ante terceros.

Cuando ha finalizado el proceso de implantación del SGSI y si la organización lo decide, tiene la opción de certificar su SGSI conforme a normativas internacionales, ISO/IEC 270001:2005.

El SGSI según la norma ISO/IEC 27001:2005 se lo puede integrar a los sistemas de gestión de la calidad ISO 9001 y gestión medioambiental ISO 14001.

El proceso de certificación lo realiza una tercera entidad acreditada, la misma que evaluará el SGSI de la organización y expedirá un certificado que demuestre que la organización satisface los requisitos de la norma ISO/IEC 27001:2005. El certificado se mantendrá siempre y cuando la organización continúe cumpliendo los requisitos de la norma.

La certificación demuestra a clientes, competidores, proveedores, personal e inversores, que una organización emplea buenas prácticas revisadas y aprobadas a nivel internacional. Un certificado de seguridad de tercera parte, ayuda a que una organización demuestre que gestiona eficientemente la seguridad de su negocio, provee la implicación, participación y motivación del personal en mantener la política de seguridad de la organización, establece procedimientos que mejoran continuamente su actividad y evidencia un enfoque innovador con visión al futuro.

2.1.8. Auditoria de sistemas de gestión

Normas

En noviembre de 2011, fue publicada la norma 27007:2011 Tecnología de la información ISO / IEC - Técnicas de seguridad - Directrices para la seguridad de la información de gestión de los sistemas de auditoría.



Imagen 10. Auditorias

Esta norma proporciona orientación para auditores internos, auditores externos, organismos de certificación y otros, permite realizar la auditoria del sistema de gestión para el cumplimiento de la norma ISO/ IEC 27001.

ISO/IEC 27007 se refiere en gran parte a la norma ISO 19011, el cual es el estándar ISO de auditoria para sistemas de gestión ambiental y de calidad, el cual proporciona orientación adicional y específica para el SGSI.

La estructura de la norma abarca los aspectos específicos de auditoría de cumplimiento del SGSI:

- La gestión del programa de auditoría SGSI (determinación de lo que se debe auditar, cuándo y cómo; asignación de auditores apropiados, la gestión de riesgos de auditoría, el mantenimiento de los registros de auditoría, mejora continua de procesos);
- Realización de un SGSI auditoría (proceso de auditoría - la planificación, la realización, las actividades clave de la auditoría, incluyendo trabajo de campo, análisis, presentación de informes y seguimiento);
- Gestión de los auditores SGSI (competencias, habilidades, atributos, evaluación).

ISO/IEC 19011

Según la ISO/IEC 19011 a una auditoría se define como:

“Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios acordados. ”. (SGS, 2012)

La ISO 19011 también contiene las siguientes directrices:

- Los principios de la auditoría.

- Gestion de los programas de auditorias.
- Actividades de la auditoria.
- La competencia de los auditores.

Principios de Auditoria

La auditoría se basa en un número de principios fundamentales que aseguran que la auditoria es una herramienta eficiente y segura. La comprensión y seguimiento de estos principios aseguran que las conclusiones de la auditoria sean relevantes y suficientes, y que auditores que están trabajando por separado alcancen conclusiones parecidas en circunstancias similares.

Tres de los principios de auditoria se relacionan con las características personales de los auditores:

Conducta ética: la función del auditor engloba confianza, integridad, confidencialidad y discreción. Los auditores se rigen bajo estrictos códigos de conducta.

Objetividad: Los hallazgos de la auditoria, las conclusiones de la auditoria y los informes de la auditoria reflejan la veracidad y precisión de las actividades de la auditoria. Cualquier opinión no resuelta o divergente entre el equipo auditor y el auditado y cualquier obstáculo encontrado debe ser informada.

Ser profesional: los auditores deben practicar y conocer la importancia de la tarea y de lo confidencial de sus actuaciones.

Independencia: Los auditores son objetivos e independientes. Los miembros del equipo auditor deben estar libres de conflictos de intereses.

Evidencias: La evidencia de la auditoría es verificable. Se basa en muestras de la información disponible, puesto que la auditoría se realiza en un periodo finito de tiempo y con recursos limitados. Sin embargo las muestras deben ser apropiadas para confiar en las conclusiones de la auditoría. (SGS, 2012)

Tipos de Auditoría

Existen tres tipos de auditorías:

Auditoría de primera parte (auditoría interna): Es la auditoría realizada por la organización a sus propios sistemas y procedimientos. Su objetivo es asegurar el mantenimiento, desarrollo y mejora del sistema de calidad. En ISO/IEC 27001:2005 como requisito es la cláusula 6.

Auditoría de segunda parte (auditoría externa): Es la auditoría realizada organización a sus proveedores y subcontratistas. El objetivo es determinar la adecuación de los proveedores, determinar la capacidad de los proveedores para suministrar recursos de acuerdo con la seguridad de la información.

Auditoría de tercera parte (auditoría externa): Es una evaluación realizada por un organismo que es comercial y contractualmente independiente de la organización, sus proveedores y sus clientes. Generalmente, una evaluación realizada por un organismo de certificación de acuerdo con un Sistema de Gestión de Seguridad de la Información de acuerdo con ISO/IEC 27001:2005. Su objetivo es determinar que el Sistema de Gestión de Seguridad de la información de una organización ha sido documentado e implementado de acuerdo con una norma determinada. (SGS, 2012)

Proceso de Auditoría

La realización de las tareas de cualquier auditoría en forma sistemática y organizada, requiere del cumplimiento de tres etapas básicas que son:

- Planificación
- Ejecución
- Conclusiones

Cada una de estas etapas constituye otros procesos: (SGS, 2012)

Planificación

La etapa de planificación es la determinación precisa de los objetivos y sub objetivos de la auditoría, genera el programa de trabajo que es el detalle de los procedimientos o técnicas seleccionados para reunir evidencia válida y suficiente, respecto de cada uno de los objetivos y sub objetivos determinados.

Ejecución

La etapa de ejecución, es aquella donde llevamos a cabo los procedimientos definidos en la planificación y que se reflejan en los programas de trabajo.

De la aplicación de cada procedimiento obtenemos conclusiones respecto del objetivo vinculado al mismo, en muchos casos resulta necesaria la aplicación de más de un procedimiento por cada objetivo, para poder reunir evidencia suficiente que permita la obtención de conclusiones sobre el mismo. Esta última etapa del proceso de auditoría se caracteriza fundamentalmente, por la síntesis de las conclusiones particulares de cada procedimiento aplicado, para llegar a una o varias conclusiones generales sobre la tarea realizada. Esta etapa termina con la emisión del correspondiente informe de auditoría.

CAPÍTULO 3

3. SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

3.1.1. Situación actual de la empresa CNT con respecto a la seguridad de la información.

3.1.2. La empresa CNT



Imagen 11.- Logo institucional. Corporación Nacional de Telecomunicaciones

La Corporación Nacional de Telecomunicaciones (en adelante CNT EP o corporación) nace el 30 de octubre del 2008, resultado de la fusión de las extintas Andinatel S.A. y Pacifictel S.A.; transcurrido un poco más de un año, el 14 de enero del 2010, la CNT S.A., se convierte en empresa pública, y pasa a ser, desde ese momento, la **CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP**, empresa estatal líder en el mercado de las telecomunicaciones del Ecuador. Posteriormente, el 30 de julio del 2010, se oficializó la fusión de la Corporación con la empresa de telefonía móvil ALEGRO (TELECSA). La CNT potencia la cartera de productos, enfocando los esfuerzos empresariales en el empaquetamiento de servicios y en la convergencia de tecnologías.

La corporación en base al desarrollo empresarial generado estos años se guía a través del siguiente precepto como misión empresarial:

“Unimos a todos los ecuatorianos integrando nuestro país al mundo, mediante la provisión de soluciones de telecomunicaciones innovadoras, con talento humano comprometido y calidad de servicio de clase mundial.” (Corporación Nacional de Telecomunicaciones CNT EP., 2013)

Esta misión se encuentra alineada estratégicamente con los objetivos que la corporación pretende cumplir a futuro, desarrollados claramente en su visión empresarial:

“Ser la empresa líder de telecomunicaciones del país, por la excelencia en su gestión, el valor agregado que ofrece a sus clientes y el servicio a la sociedad, que sea orgullo de los ecuatorianos.” (Corporación Nacional de Telecomunicaciones CNT EP., 2013)

El portafolio de servicios que ofrece la corporación abarca los siguientes productos:

Telefonía Fija: CNT presta servicios de telefonía fija residencial a cobertura nacional, siendo la empresa que posee la mayor cantidad de abonados suscritos a nivel nacional. Este servicio se extiende tanto a personas naturales como a clientes corporativos.

Telefonía Móvil: a partir de la fusión con la extinta Telecsa, CNT presta servicios de telefonía móvil prepago y pospago dirigido a personas naturales y clientes corporativos. Brinda gran variedad de planes tarifarios, según su oferta comercial los precios ofrecidos sean los más asequibles del mercado, y aplican a las tecnologías GSM, 3,5G y HSPA PLUS y LTE.

Telefonía pública: como parte de su portafolio y como servicio que brinda una oportunidad de creación de negocio con miras de crecimiento CNT ofrece cabinas y locutorios telefónicos; además, de terminales de comunicación instalados en las vías públicas, centros de concentración y tráfico de personas, colegios y universidades, proporcionando gran facilidad de acceso a la comunicación urgente con calidad de voz y tarifas convenientes hacia cualquier destino del mundo (llamadas locales, nacionales, celulares e internacionales).



Imagen 12.- Servicio de Telefonía Fija, Movil y Pública.

Internet fijo: Este servicio garantiza una conexión permanente a internet a través de una de las redes más avanzadas de América Latina y soporte técnico permanente. El servicio se soporta en las mejores plataformas tecnológicas que aseguran un performance óptimo con altos estándares internacionales. Su cobertura es a nivel nacional.

Internet móvil: Al igual que telefonía móvil, este servicio aplica a las tecnologías GSM, 3,5G y HSPA PLUS. El servicio asegura conexión a internet en cualquier lugar de cobertura y sobre cualquier terminal que soporte telefonía móvil y datos.



Imagen 13.- Servicio de Internet Fija y Movil.

Televisión Satelital: CNT ofrece planes y paquetes de calidad con la mejor tecnología que brinda una mejor resolución en imagen, programación variada en contenidos de audio y video y con cobertura a través de todo el territorio ecuatoriano.

El servicio se ofrece por suscripción y muestra canales internacionales, nacionales, regionales y señales de audio.



Imagen 14.- Servicio de Televisión Satelital CNT TV. (Corporación Nacional de Telecomunicaciones CNT EP., 2013)

3.1.3. Estructura organizacional CNT EP.



Imagen 15: Estructura Organizacional CNT EP.

(Corporación Nacional de Telecomunicaciones CNT EP., 2013)

La corporación mantiene una estructura organizacional basada en niveles jerárquicos; donde, el primer nivel compone al directorio y los miembros del staff (Auditoria Interna). En el segundo nivel se encuentran las Gerencias Nacionales; entre las cuales, se encuentra la Gerencia Nacional de Tecnologías de la Información (GNTI).

La GNTI apoya y brinda servicios a la CNT EP., con sistemas y aplicaciones que apalancan al negocio para cumplir con sus objetivos estratégicos. La GNTI posee

tres gerencias (Soporte, Producción, Soluciones) y una jefatura de staff (Gestión de Calidad) la cual abarca al área de seguridad de la información.

3.1.4. Área de seguridad de la información

De acuerdo a la estructura organizacional de la CNT EP, el área de seguridad de la información se encuentra ubicada en el nivel II, bajo la Gerencia Nacional de Tecnologías de la información en la jefatura de Gestión de la Calidad, es una unidad de staff dentro de la Gerencia de TI de modo que tiene injerencia sobre todas las áreas de esta.

El nivel estratégico de la seguridad de la información está materializado en el Comité de Riesgos, que a su vez cumple como Comité de Seguridad de la Información, este se encuentra conformado por el Gerente General y todos los Gerentes Nacionales de la CNT EP, incluyendo al Oficial de Seguridad de la Información y a los especialistas en riesgos.

El nivel operativo comprende un grupo de analistas de seguridad de la información quienes se encargan de apoyar al Oficial de Seguridad de la Información según su respectiva rama de especialización (forense, seguridad en redes, gestión de riesgos, auditoría.) El enfoque del área de seguridad de la información en la CNT EP., está basado tanto en temas proactivos como reactivos. La pro actividad realiza un adecuado análisis de riesgos, identifica vulnerabilidades y amenazas para implementar oportunamente los distintos controles.

El enfoque reactivo se orienta a la gestión de requerimientos e incidentes de seguridad de la información.

El SGSI de la CNT EP nació como un proyecto estratégico para cubrir la necesidad de la Gerencia Comercial debido al incremento de licitaciones que demandan poseer la certificación ISO/IEC 27001:2005, la iniciativa y dirección del proyecto fue encabezada por el grupo de seguridad de la información, a tal punto que una vez que el sistema ha sido implementado, la gestión, monitoreo y mejora depende del grupo de seguridad de la información.

El grupo que conforma el área de seguridad de la información está compuesto por un equipo de nueve profesionales encabezados por el Oficial de Seguridad de la Información, de los cuales, cuatro han aprobado el curso de certificación de Auditor Líder ISO/IEC 27001:2005.

Los profesionales de apoyo al Oficial de Seguridad de la Información tienen distintas ramas de especialización lo que permite administrar adecuadamente la seguridad de la información en base a una metodología de valoración de riesgos y con enfoque de mejora continua.

3.1.5. Sistema de Gestión de Seguridad de la Información (SGSI) de la CNT EP.

Dentro de los riesgos a los que se expone la corporación, existe el riesgo de seguridad de la información; por tal razón, la alta dirección tomó la decisión de

desarrollar e implementar un Sistema de Gestión de Seguridad de la información (SGSI), alineado a la norma ISO/IEC 27001:2005 y optar por la certificación internacional.

La iniciativa de CNT E.P. de obtener esta certificación, nace de la necesidad de satisfacer las nuevas exigencias del mercado. Los clientes corporativos exigen con mayor frecuencia en sus licitaciones que los proveedores de servicios de internet y datos posean la certificación ISO/IEC 27001:2005. De modo que la Corporación al obtener este reconocimiento, incrementaría su imagen corporativa al prestar servicios de mayor calidad avalado por un tercero, generando valor y mayores ingresos al estado.

La hoja de ruta de la Imagen 6, muestra los pasos a seguir para definir e implementar un SGSI de acuerdo con ISO/IEC 27001:2005., la misma nos guiará en la descripción el Sistema de Gestión de Seguridad de la Información de la CNT EP., y así entender su desarrollo y gestión, como preámbulo a la auditoria interna a realizarse.

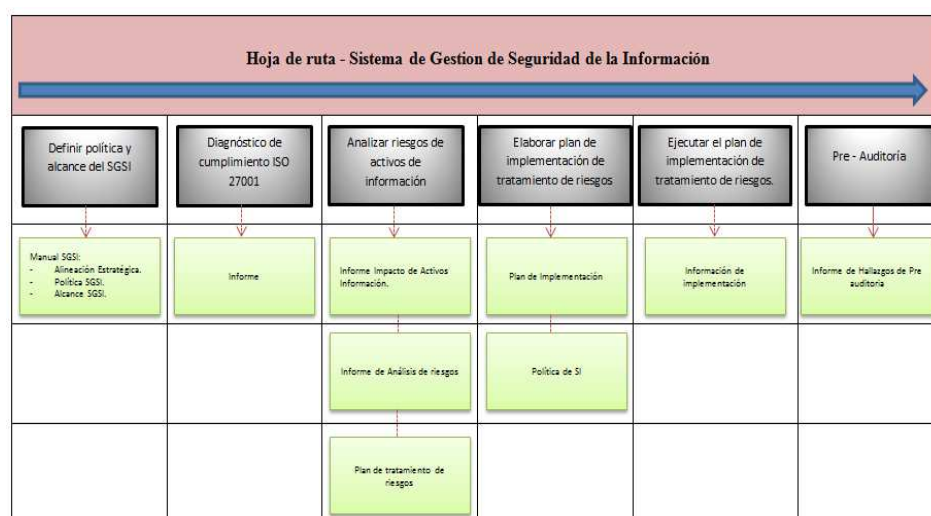


Imagen 16: Hoja de ruta SGSI CNT EP.

El alcance del sistema de gestión de seguridad de la información de la CNT EP., posee un alcance enfocado en el proceso de:

Venta e instalación de productos y servicios de datos e internet para clientes corporativos en el D.M.Q.

Siendo este alcance aplicado para el Distrito Metropolitano de Quito, en la Tabla 2 se registran las direcciones de las instalaciones de la corporación donde se encuentran las áreas a ser auditadas.

Para almacenar y respaldar la documentación utiliza la aplicación interna de Manejo Automático de la ISO (MAI) la cual forma parte del cumplimiento de la norma especificado en la cláusula 4 de la Norma ISO/IEC 27001:2005:2005 (4.3 Requisitos de Documentación).

Tabla 2. Localización geográfica del proyecto de Tesis.

Oficina:	Amazonas y Veintimilla. Edificio CETA.	Gerencia Nacional Jurídica.
Oficinas:	Nueve de Octubre y Cordero. Edificio DROIRA	Gerencia de O&M Core y Plataformas.
	Eloy Alfaro y Nueve de Octubre. Edificio DORAL.	Gerencia Comercial. Gerencia Nacional de Desarrollo Organizacional.
	Jorge Drom y Gaspar de Villarroel. Edificio IÑAQUITO.	Gerencia Nacional de TI Representante de Gerente General. Gerencia de Soluciones. - Desarrollo TI. - Arquitectura TI. BDD, Servidores, Redes TI. - Data Center TI. Gestión de la Calidad TI. - Gestor de Cambios. - Encargado SGSI. - Oficial de Seguridad de la Información.
	Reina Victoria y Veintimilla. Edificio MARISCAL.	Gerencia Nacional de O&M TX.
	Amazonas y Corea. Edificio VIVALDI.	Gerencia Soluciones Corporativas. Seguridad Física.

Para almacenar y respaldar la documentación utiliza la aplicación interna de Manejo Automático de la ISO (MAI) la cual forma parte del cumplimiento de la norma especificado en la cláusula 4 de la Norma ISO/IEC 27001:2005:2005 (4.3 Requisitos de Documentación).

En base al documento de Metodología de Evaluación de Riesgos, almacenado en el MAI, se ha realizado la evaluación de riesgos de seguridad de los activos de información para tomar las medidas necesarias y mantener los riesgos en niveles aceptables, esta clasificación de activos determinó el nivel de impacto cualitativo que tendría para el negocio la pérdida de cualquiera de los atributos de la información: Integridad, disponibilidad y confidencialidad.

El impacto de esta situación podría ocasionar fuga de información sensible, que podría afectar a la corporación en su imagen, ingresos monetarios e incluso originar problemas legales.

La selección de activos críticos fue determinado en base a un nivel de impacto y vulnerabilidad los cuales requerían la implementación de controles para aumentar la mitigación de los riesgos que tengan asociados.

En la identificación del universo de vulnerabilidades, se elaboró un documento con las posibles amenazas y vulnerabilidades a la seguridad de la información por tipo de activo de información que es afectado junto con los controles de la norma

ISO27001. De la misma forma la identificación del universo de amenazas, incluye una lista de referencia de aquellas que tienen una probabilidad de ocurrencia alta en el entorno de la organización.

Sobre el **enfoque de riesgos**: la corporación utilizó una metodología de valoración de riesgos que permitió determinar:

- Identificar los activos de información dentro del alcance del SGSI.
- Clasificar los activos críticos según su impacto
- Identificar Amenazas y vulnerabilidades.
- Analizar y evaluar riesgos.
- Determinar la aceptación del riesgo.
- Identificar y evaluar opciones de tratamiento de riesgos.
- Identificar posibles controles a implementar.

Sobre todos los resultados obtenidos, la CNT EP tiene registrado en su aplicación interna MAI los documentos que hacen referencia a esta información:

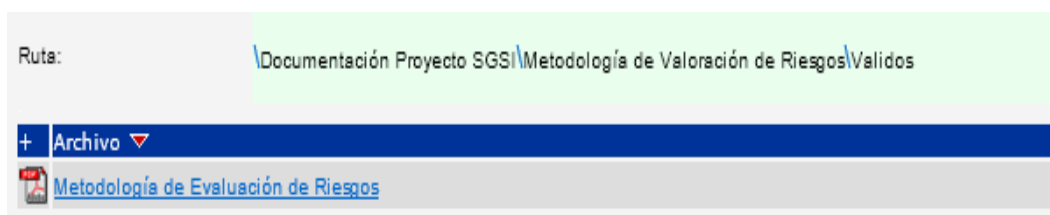


Imagen 17. Captura de pantalla Documento “Metodología de Evaluación de Riesgos” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: confidencial. (CNT EP., 2012)

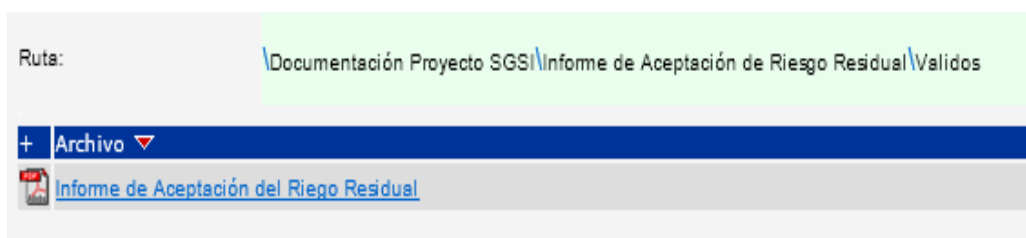


Imagen 18. Captura de pantalla Documento “Informe de Aceptación del Riesgo Residual” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: confidencial.

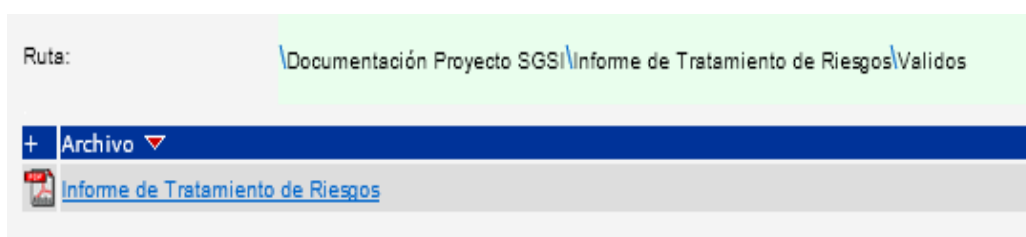


Imagen 19. Captura de pantalla Documento “Informe de Tratamiento de Riesgos” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: confidencial.

Sobre el **objeto y campo de aplicación**, debido a la naturaleza del negocio de la corporación, además del alcance de su SGSI; la CNT EP ha decidido excluir un control de la Norma ISO/IEC 27001:2005:2005., exactamente el control A.10.9 Seguridad en Comercio Electrónico (A.10.9.1 Comercio electrónico, A.10.9.2 Transacciones en línea).

Los controles aplicables fueron evaluados de acuerdo a la documentación entregada por la corporación y su aplicabilidad con el Anexo A de la norma.

Su especificación se encuentra debidamente documentados en su “Declaración de Aplicabilidad”.

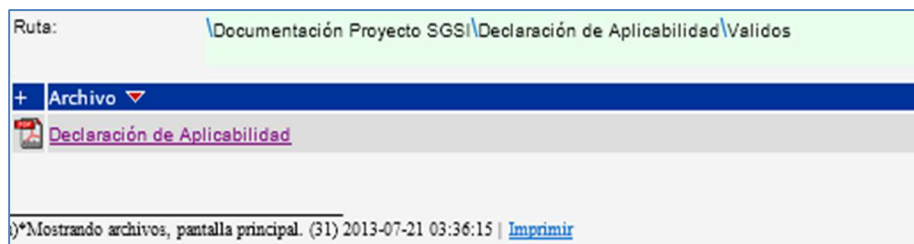


Imagen 20. Captura de pantalla Documento “Declaración de Aplicabilidad” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: confidencial.

Además es pertinente mencionar que de la norma indicada se ha cumplido con los requisitos del 4 al 8 sin excepción alguna.

Sobre el **establecimiento y gestión del SGSI de la CNT EP.**, la corporación brinda servicios de telecomunicaciones manteniendo un alto nivel de protección de la información que maneja a través de su SGSI, garantizando el cumplimiento, mantenimiento y mejora continua de dicho sistema concediendo los medios y recursos necesarios para cumplir con los objetivos establecidos. La pirámide documental del SGSI de la CNT EP incluye los siguientes elementos:



(CNT EP, 2012) Control 4.3 Requisitos de Documentación.

Sobre la **responsabilidad de la dirección**: la Gerencia General demuestra su compromiso comunicando la importancia de cumplir con los requisitos impuestos dentro de los distintos controles que forman parte del SGSI, realizando las revisiones de la dirección y asegurando la disponibilidad de los recursos necesarios para continuar operando y mejorando el SGSI.

La CNT con el objeto de cumplir con la formación, toma de conciencia y competencia, realiza charlas trimestrales y actualizadas para la concientización y capacitación a sus colaboradores. El oficial de Seguridad de la información realiza un plan de capacitación el cual es revisado y actualizado trimestralmente.

Para cumplir con dicha planificación, se hace uso de cualquier medio tecnológico, físico o publicitario que permita llegar a toda la CNT EP, considerando evaluaciones al personal que ha sido capacitado para medir su nivel de asimilación del conocimiento y para determinar el grado de compromiso que tienen con la Seguridad de información de la CNT EP.

Sobre **auditorías internas**: la CNT EP ha elaborado el plan de auditoría del SGSI concebido para realizarse anualmente con una periodicidad semestral.

Las auditorías internas buscan determinar si el sistema de gestión de la seguridad de la información se mantiene conforme con los requisitos de la Norma

ISO27001:2005 y que ha sido implementado, mantenido y operado por los colaboradores de CNT EP.

Sobre la **mejora del SGSI**: a través del modelo PDCA, la CNT ha establecido su SGSI como un modelo que le permita mejorar continuamente incluyendo una política del SGSI, amparada por la Política de Seguridad de la información y demás controles tanto técnicos como no técnicos así como los resultados de las auditorías y demás revisiones que continuamente arrojan no conformidades u oportunidades de mejora, las mismas que se ven traducidos en acciones preventivas y correctivas.

Por acciones correctivas, la CNT EP ha definido un proceso para la realización de acciones correctivas que busca eliminar las causas de las no conformidades para prevenir la recurrencia.

Con respecto a las acciones preventivas, la CNT EP se preocupa por identificar no conformidades potenciales y sus causas por medio de revisiones periódicas realizadas por parte del equipo de Seguridad de la Información, las revisiones se ejecutan según lo indicado en cada procedimiento que forma parte del SGSI. Con lo anteriormente mencionado el SGSI de la CNT EP, ha sido definido, desarrollado, implementado y monitoreado continuamente conforme los requisitos de la Norma ISO/IEC 27001:2005:2005.

CAPÍTULO 4

La auditoría interna consiste en verificar de manera objetiva si los controles del SGSI en la empresa se encuentran operando correctamente y apalancando a la seguridad de la información de la CNT EP., de manera objetiva.

Para cumplir con las auditorías internas semestrales, según lo estipulado en la Normativa para auditorías internas se debe realizar lo siguiente:

- Planificar la auditoría interna al SGSI según lo establecido en la Normativa para Auditorías Internas del SGSI.
- Elaborar el plan de auditoría
- Realizar la auditoría interna.
- Elaborar el informe de auditoría interna y desarrollar el plan de acción preliminar.
- Presentar y Entregar del informe final de la auditoría interna con los hallazgos a la alta gerencia.

4.1.1. Planificar la auditoría interna al SGSI según lo establecido en la Normativa para Auditorías Internas del SGSI.

Para la planificación de la auditoría, se hará referencia al documento “Normativa para Auditorías Internas al SGSI”, el mismo que tiene como objetivo normalizar los distintos requisitos y controles que deben revisarse en cada auditoría interna realizada al SGSI de la CNT EP, considerando que todo el SGSI es evaluado en el año.

Con esta aclaración, es responsabilidad del oficial de seguridad de la información y del delegado de la Gerencia General asegurar la ejecución de dos auditorías internas anuales.

Como consideración se debe tener presente que las auditorías internas son un requisito del capítulo seis de la Norma ISO/IEC 27001:2005 cuyo incumplimiento afectaría de manera significativa al SGSI; además, de ser uno de los pilares de la mejora continua.

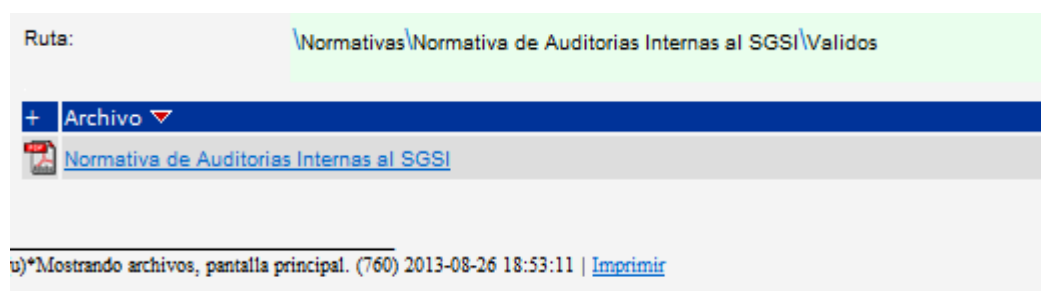


Imagen 22. Captura de pantalla Documento “Normativa para Auditorías Internas al SGSI” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: confidencial.

Como referencias para la elaboración de la “Normativa para Auditorías Internas al SGSI” se toma:

- ISO/IEC 27001:2005
- Procedimiento de Auditorías Internas de CNT EP.
- Normativa para Auditores Internos del SGSI de la CNT EP.

Con respecto a las auditorías internas del SGSI de la CNT EP se debe:

- Realizarse anualmente con una periodicidad semestral.
- Los registros que deben generarse por cada auditoría interna son:
 - Plan de trabajo de la auditoría interna.
 - Informe de auditoría interna (Resumen ejecutivo e informe detallado de hallazgos)
 - Listado de asistencia con firmas de los asistentes a la presentación de hallazgos
 - Plan de acción para cerrar las no conformidades halladas.
- Los formatos de elaboración de los registros de auditoría deberán ser tomados de los que se generaron en la última auditoría interna realizada, por lo cual todos deben ser publicados en el sistema MAI.
- Todos los controles y requisitos de la norma ISO/IEC 27001:2005 deben ser probados en su totalidad en el periodo de un año; de tal modo que, la distribución de dichos controles y requisitos para las revisiones en las auditorías internas están detalladas en el anexo 1 del documento “Normativa para Auditorías Internas al SGSI”.
- El Oficial de Seguridad de la Información deberá nombrar un delegado quien se encargue de:
 - Dirigir la realización de la auditoría interna.
 - Coordinar con el equipo de auditores las actividades y entregables.
 - Elaborar los registros respectivos.

- Convocar y presentar los resultados de la auditoría.
 - Asegurar que se cumpla con el plan de acción.
 - Proporcionar al encargado del SGSI todos los registros formalizados y en formato PDF para que sea publicado en la aplicación interna MAI.
- Una de las actividades de toda auditoría interna es la validar que el plan de acción generado en la última auditoría interna ha sido cerrado.

Para este apartado es importante mencionar que los recursos asignados en la participación de la auditoría interna deben cumplir con la normativa establecida, el no cumplimiento de la misma acarreará sanciones de acuerdo a lo establecido en los procedimientos internos de la corporación que forman parte del SGSI.

De acuerdo a los periodos planificados por parte de la Normativa en este año las auditorías se realizarán:

- Auditoría 1 (AI 1): Febrero 2013.
- Auditoría 2 (AI 2): Septiembre 2013.

Cabe indicar que de acuerdo a la “Normativa para Auditorías Internas del SGSI”, y el objetivo de realizar la revisión de los requisitos y controles en el lapso de un año, los controles que no se encuentren marcados en la columna AI1 (Auditoría 1), serán tomados en cuenta en la siguiente auditoría semestral, los cuales podrán ser

identificados al estar marcados en la columna AI2 (Auditoría 2). Los requisitos a ser tomados en cuenta en la auditoria de finales de febrero 2013 son:

Tabla 3. Requisitos de ISO/IEC 27001:2005 - R 4.

REQUISITOS	AI1	AI2
4 Sistema de gestión de seguridad de la información		
4.1 Requisitos generales	x	
4.2 Establecer y manejar el SGSI	x	
4.2.1 Establecer el SGSI	x	
4.2.2 Implementar y operar el SGSI	x	
4.2.3 Monitorear y revisar el SGSI	x	
4.2.4 Mantener y mejorar el SGSI	x	
4.3 Requisitos de documentación	x	
4.3.1 General	x	
4.3.2 Control de documentos	x	
4.3.3 Control de registros	X	

Tabla 4. Requisitos de ISO/IEC 27001:2005 R5 - R6 - R7 - R8.

REQUISITOS	AI1	AI2
5 Compromiso de la Gerencia		

5.1 Compromiso de la gerencia	X
5.2 Gestión de recursos	X
5.2.1 Provisión de recursos	X
5.2.2 Capacitación, conocimiento y capacidad	X
6 Auditorías internas SGSI	
7 Revisión Gerencial del SGSI	
7.1 General	x
7.2 Insumo de la revisión	x
7.3 Resultado de la revisión	x
Continúa	
8 Mejoramiento del SGSI	
8.1 Mejoramiento continuo	x
8.2 Acción correctiva	x
8.3 Acción preventiva	x

Los controles a ser tomados en cuenta son:

Tabla 5. Controles a ser validados en las Auditorías planificadas Anexo A5.

OBJETIVOS DE CONTROL Y CONTROLES	AI1	AI2
A.5 POLÍTICA DE SEGURIDAD		
A.5.1 Política de Seguridad de Información	x	
A.5.1.1 Documento de la política de seguridad de la información	x	
A.5.1.2 Revisión Política de seguridad de la información	x	

OBJETIVOS DE CONTROL Y CONTROLES	A	AI2
A.6 ORGANIZACIÓN DE SEGURIDAD DE INFORMACION	II	
A.6.1 Organización Interna		X
A.6.1.1 Compromiso de la dirección en la seguridad de la información		X
A.6.1.2 Coordinación de la seguridad de la información		X
A.6.1.3 Asignación de responsabilidades de la seguridad de la información		X
A.6.1.4 Proceso de autorización para medios de procesamiento de la información		X
A.6.1.5 Acuerdo de Confidencialidad		X
A.6.1.6 Contacto con las Autoridades		X
A.6.1.7 Contacto con grupos interesados especialistas		X
A.6.1.8 Revisión Independiente de seguridad de la información		X
A.6.2 Partes externas		X
		Continúa
A.6.2.1 Identificación de riesgos relacionados con partes externas		X
A.6.2.2. Tratamiento de la seguridad cuando negociamos con clientes		X
A.6.2.3 Requisitos de seguridad en acuerdos con terceras partes		X

Tabla 6. Controles a ser validados en las Auditorías planificadas Anexo A6 – A7.

A.7 GESTIÓN DE ACTIVOS	
A.7.1 Responsabilidad	X
A.7.1.1 Inventario de activos	X
A.7.1.2 Propiedad de los activos	X
A.7.1.3 Uso aceptable de los activos	X
A.7.2 Clasificación de la información	X

A.7.2.1 Guías de clasificación	x
A.7.2.2 Etiquetado y gestión de información	x

Tabla 7. Controles a ser validados en las Auditorías planificadas Anexo A8 – A9.

OBJETIVOS DE CONTROL Y CONTROLES	AI1	AI2
A.8 SEGURIDAD DEL PERSONAL		
A.8.1 Antes del trabajo	X	
A.8.1.1 Funciones y Responsabilidades	X	
A.8.1.2 Selección	X	
A.8.1.3 Términos y condiciones de la relación laboral	X	
		Continúa
A.8.2 Durante del trabajo	X	
A.8.2.1 Gestión de las responsabilidades	X	
A.8.2.2 Educación y formación en seguridad de la información	X	
A.8.2.3 Proceso disciplinario	X	
A.8.3 Terminación o cambio de trabajo	X	
A.8.3.1 Terminación de responsabilidades	X	
A.8.3.2 Devolución de activos	X	
A.8.3.3 Eliminación de derechos de acceso	X	
A.9 SEGURIDAD FÍSICA Y DEL ENTORNO		
A.9.1 Áreas seguras	X	
A.9.1.1 Perímetro de seguridad física	X	
A.9.1.2 Control de acceso físico	X	
A.9.1.3 Seguridad de oficinas, recintos e instalaciones	X	
A.9.1.4 Protección contra amenazas externas o medioambientales	X	
A.9.1.5 Trabajo en áreas seguras	X	
A.9.1.6 Acceso público, despacho y áreas de carga	X	

A.9.2 Seguridad de los equipos	X
A.9.2.1 Ubicación y protección de los equipos	X
A.9.2.2 Suministro de energía	X
A.9.2.3 Seguridad del cableado	X
A.9.2.4 Mantenimiento de los equipos	X
	Continúa
A.9.2.5 Seguridad de los equipos fuera de las instalaciones	X
A.9.2.6 Disposición segura o re utilización de equipos	X
A.9.2.7 Retiro de bienes	X

Tabla 8. Controles a ser validados en las Auditorías planificadas. Anexo A 10 - 15.

OBJETIVOS DE CONTROL Y CONTROLES	AI1	AI2
A.10 GESTION DE COMUNICACIONES Y OPERACIONES		
A.10.1 Procedimientos Operacionales y Responsabilidades		X
A.10.1.1 Procedimientos de operación documentados		X
A.10.1.2 Gestión de Cambios		X
A.10.1.3 Separación de funciones		X
A.10.1.4 Separación de las instalaciones, desarrollo y producción		X

A.10.2 Gestión de Servicios entregados por terceras partes	x
A.10.2.1 Entrega de servicios	x
A.10.2.2 Monitoreo y revisión de servicios suministrados por terceras partes	x
A.10.2.3 Gestión de cambios en servicios hechos por terceras partes	x
A.10.3 Planeación y Aceptación del Sistema	x
A.10.3.1 Planeación de la capacidad	x
A.10.3.2 Aceptación del sistema	x
A.10.4 Protección contra software malicioso y código móvil	x
A.10.4.1 Controles contra software malicioso	x
A.10.4.2 Controles contra software móvil	x
A.10.5 Backup-up	x
A.10.5.1 Back-up de la información	x
A.10.6 Gestión de la seguridad de la red	x
A.10.6.1 Controles de red	x
Continúa	
A.10.6.2 Seguridad de los servicios de red	x
A.10.7 Gestión de los medios	x
A.10.7.1 Gestión de los medios removibles	x
A.10.7.2 Eliminación de medios	x
A.10.7.3 Procedimientos para el manejo de la información	x
A.10.7.4 Seguridad de la documentación del sistema	x
A.10.8 Intercambio de Información	x
A.10.8.1 Procedimientos y políticas para el intercambio de información	x
A.10.8.2 Acuerdos de Intercambio	x
A.10.8.3 Medios físicos en tránsito	x
A.10.8.4 Correo electrónico	x
A.10.8.5 Sistemas de información de negocios	x
A.10.9 Seguridad en Comercio Electrónico	x
A.10.9.1 Comercio electrónico	x
A.10.9.2 Transacciones en línea	x
A.10.9.3 Información disponible públicamente	x
A.10.10 Monitoreo	x
A.10.10.1 Auditoria de ingresos al sistema "Log-in"	x
A.10.10.2 Monitoreo del uso del sistema	x
A.10.10.3 Protección de logs de información	x
A.10.10.4 Eventos del Administrador y operador	x

A.10.10.5 Ingresos fallidos al sistema	x
A.10.10.6 Sincronización de relojes	x
A.11 CONTROL DE ACCESO	
A.11.1 Requisitos del Negocio para el Control de Acceso	x
A.11.1.1 Políticas para el control de acceso	x
A.11.2 Administración de Accesos de Usuarios	x
A.11.2.1 Registro de usuarios	x
A.11.2.2 Administración de privilegios	x
A.11.2.3 Administración de contraseñas para usuarios	x
A.11.2.4 Revisión de los derechos de acceso de los usuarios	x
A.11.3 Responsabilidades de los Usuarios	x
A.11.3.1 Uso de contraseñas	x
A.11.3.2 Equipo de cómputo de usuario desatendido	x
A.11.3.3 Política de puesto de trabajo despejado y bloqueo de pantalla	x
Continúa	
A.11.4 Control de Acceso a Redes	x
A.11.4.1 Política de uso de los servicios en red	x
A.11.4.2 Autenticación de usuarios para conexiones externas	x
A.11.4.3 Identificación de equipos en red	x
A.11.4.4 Protección de puertos de diagnóstico y configuración remota	x
A.11.4.5 Segmentación de redes	x
A.11.4.6 Control de conexión a las redes	x
A.11.4.7 Control de enrutamiento en la red	x
A.11.5 Control de Acceso al Sistema Operativo	x
A.11.5.1 Procedimientos de identificación de usuarios segura	x
A.11.5.2 Identificación y autenticación de usuarios	x
A.11.5.3 Sistema de administración de contraseñas	x
A.11.5.4 Uso de utilidades del sistema	x
A.11.5.5 Time-out de session	x
A.11.5.6 Limitación del tiempo de conexión	x
A.11.6 Control de Acceso en la información y a las aplicaciones	x
A.11.6.1 Restricción de acceso a la información	x
A.11.6.2 Aislamiento de sistemas relevantes	x
A.11.7 Computación móvil y trabajo remoto	x
A.11.7.1 Computación y comunicaciones móviles	x
A.11.7.2 Trabajo remoto	x

A.12 ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
A.12.1 Requisitos de Seguridad de los Sistemas	x
A.12.1.1 Análisis y especificación de los requisitos de seguridad	x
A.12.2 Procesamiento Correcto de Aplicaciones	x
A.12.2.1 Validación de los datos de entrada	x
A.12.2.2 Control al procesamiento interno	x
A.12.2.3 Autenticación de mensajes	x
A.12.2.4 Validación de los datos de salida	x
A.12.3 Controles Criptográficos	x
A.12.3.1 Política en el uso de controles criptográficos	x
A.12.3.2 Administración de llaves	x
A.12.4 Seguridad de los archivos del Sistema	x
A.12.4.1 Control operativo del software	x
A.12.4.2 Protección de los datos de prueba del sistema	x
Continúa	
A.12.4.3 Control de acceso a código de programas fuente	X
A.12.5 Seguridad en los Procesos de Desarrollo y Soporte	X
A.12.5.1 Procedimientos de control de los cambios	X
A.12.5.2 Revisión técnica de aplicaciones después de cambios en el sistema	X
A.12.5.3 Restricciones en los cambios a los paquetes de software	X
A.12.5.4 Fuga de información	X
A.12.5.5 Desarrollo externo de software	X
A.12.6 Gestión de Vulnerabilidad Técnica	X
A.12.6.1 Control de vulnerabilidades técnicas	X
A.13 GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE INFORMACIÓN	
A.13.1 Reporte de incidentes y anomalías de Seguridad de Información	x
A.13.1.1 Reporte de los incidentes en seguridad de información	x
A.13.1.2 Reporte de las debilidades en la seguridad	x
A.13.2 Gestión de los incidentes e imprevistos en la Seguridad de la Información	x
A.13.2.1 Responsabilidades y procedimientos	x
A.13.2.2 Aprendizaje desde los incidentes en la seguridad de la información	x
A.13.2.3 Recolección de evidencias	x
A. 14 GESTION DE CONTINUIDAD DEL NEGOCIO	
A.14.1 Aspectos de Seguridad de Información en Gestión de Continuidad del Negocio	X

A.14.1.1 Incluyendo información de seguridad en el proceso de gestión de continuidad del negocio	X
A.14.1.2 Continuidad del negocio y avalúo de riesgos	x
A.14.1.3 Desarrollo e implementación del plan de continuidad incluyendo seguridad de la información	x
A.14.1.4 Planeación de la estructura de la continuidad del negocio	x
A.14.1.5 Prueba, mantenimiento y reevaluación del plan de continuidad del negocio	x
A.15 CONFORMIDAD	
A.15.1 Conformidad con los Requisitos Legales	x
A.15.1.1 Identificación de la legislación aplicable	x
A.15.1.2 Derechos de propiedad intelectual	x
A.15.1.3 Protección de los registros de la organización	x
A.15.1.4 Protección de los datos y privacidad de la información personal	x
Continúa	
A.15.1.5 Protección del uso inadecuado de los recursos de procesamiento de la información	x
A.15.1.6 Reglamentación de los controles criptográficos	x
A.15.2 Conformidad de Política de Seguridad, Normas y el Cumplimiento Técnico	x
A.15.2.1 Conformidad de la política de seguridad y normas	x
A.15.2.2 Verificación de conformidad técnico	x
A.15.3 Consideraciones de Auditoría de Sistemas de Información	x
A.15.3.1 Controles de auditoría de sistemas de información	x
A.15.3.2 Protección de las herramientas de auditoría de sistemas de información	x

Las áreas a intervenir:

- Gerencia Comercial, Clientes corporativos y pymes (RG2).
- Soluciones Corporativas
- O&M Core y Plataformas
- O&M TX (MPLS)
- Gerencia Nacional de TI

- Áreas de Soporte del SGSI (Jurídico, Seguridad Física, Asuntos regulatorios y Desarrollo Organizacional.)

4.1.2. Elaborar el Plan de Auditoría

Como parte de las actividades para la elaboración del plan de auditoría y en base a la Normativa para auditorías internas se han determinado cuatro aspectos con los cuales se procederá con la creación de dicho documento: identificación, agenda, logística y autoridad.

A continuación se detalla en la Tabla 2., los ítems por cada uno de estos aspectos y su resultado.

Tabla 12. Elaboración de plan de auditoría.

ITEM	DETALLE
Fecha de elaboración de Plan de Auditoría	<p>La fecha de elaboración del plan de auditoría se registra en: Enero 2013</p> <p>Como insumo para este documento se requirió:</p> <ul style="list-style-type: none"> - Un cronograma tentativo de la auditoría, - Controles a revisar, - Activos de información, - Nombre de un delegado tentativo por cada área auditada y - Integrantes del equipo auditor.
Clase de auditoría.	

Auditoría Interna (Primera parte)

Proceso

Proceso de venta e instalación de productos y servicios de datos e internet para clientes corporativos en el D.M.Q.

Auditor líder

El oficial de Seguridad delegó a un analista de seguridad que cumpla con el perfil requerido.

Para nuestra auditoría se designó a un Analista de Seguridad de la Información Líder Auditor. ISO/IEC 27001:2005:2005

Continua

Líder de equipo auditor

Para la selección de los auditores que participaron en la auditoría interna, se tomó como referencia la “Normativa de Auditores Internos”, el cual indica los roles y requisitos que deben poseer los:

Encargados de la Auditoría:

Encargados de Entrevistas de Auditoría y;

Personal de apoyo de la auditoría.

ROL	REQUISITOS
Encargado de la Auditoría	<ul style="list-style-type: none"> - Tener experiencia como auditor en ISO 27001:2005 - Haber aprobado el curso de preparación sea de Auditor Interno o de Auditor Líder ISO 27001:2005
Encargado de Entrevistas de Auditoría	<ul style="list-style-type: none"> - Haber aprobado el curso de preparación sea de Auditor Interno o de Auditor Líder ISO 27001:2005
Personal de Apoyo a la Auditoría	<ul style="list-style-type: none"> - Haber participado en alguna capacitación de 27001:2005.

Imagen 23. Captura de pantalla Documento “Normativa de Auditores internos del SGSI” punto 7, roles y requisitos de auditores internos para el SGSI. Alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial.

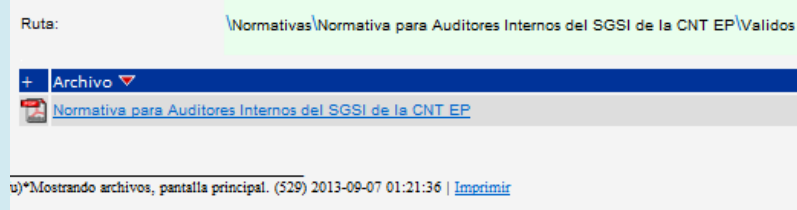


Imagen 24. Captura de pantalla Documento “Normativa para Auditores internos del SGSI de la CNT EP”. Alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial.

Esta normativa, se alinea con el “Procedimiento de Auditorías Internas” el cual tiene como objetivo determinar un procedimiento para ejecutar auditorías internas y así cumplir con los requisitos del Sistema de Gestión tanto de calidad como de Seguridad de la información de CNT EP.

Continúa

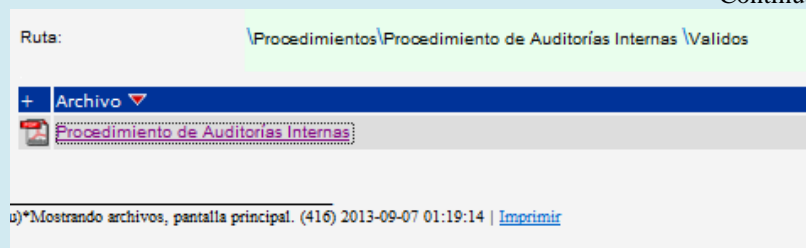


Imagen 25. Captura de pantalla Documento “Procedimiento de Auditorías Internas”. Alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial.

Objetivos de la auditoría.

Realizar una auditoría interna de la implantación de la norma ISO/IEC 27001:2005, mediante la definición y aplicación de un plan de trabajo de auditoría.

Detectar las no conformidades mayores, no conformidades menores y oportunidades de mejora asociadas al SGSI de la CNT EP, con respecto a la Norma ISO 27001:2005.

Realizar un informe de hallazgos de la Auditoría Interna ISO/IEC 27001:2005 del Sistema de Gestión de Seguridad de la Información de la CNT EP.

Proporcionar seguimiento al cierre de no conformidades encontradas en la Pre Auditoría al SGSI realizada por Deloitte en julio del 2012.

Continúa

Alcance de la auditoria.

El alcance de la auditoria es el mismo del Sistema de Gestión de la Seguridad de la Información de CNT EP:

Venta e Instalación de Productos y Servicios de Datos e internet a Clientes Corporativos, y es aplicable para el Distrito Metropolitano de Quito.

Criterios de la auditoria.

Para determinar la valorización se realiza en base a Hallazgos vs Requisitos y Controles de la Norma ISO/IEC 27001:2005.; donde:

No conformidades mayores (en adelante NC+): Incumplimiento de Requisitos del 2 al 4 de la Norma. Ej. Se considera una no conformidad mayor el no poseer un requisito el cual es obligatorio.

No conformidades menores (en adelante NC-): Implantación de controles del A5 al A15 de la Norma. Ej.: Si existe el control, pero no está operando eficazmente se considera una no conformidad menor.

Oportunidades de Mejora (en adelante OP): Recomendaciones para mejorar el proceso.

Continúa

AGENDA:**Actividades de la auditoria.**

En este aspecto se realiza cada una de las actividades que se ejecutarán en la auditoria, con fechas, horarios (hora de inicio, hora final) las áreas a ser auditadas junto con los auditores que realizarán dicha actividad y el lugar donde se realizará. Determinando:

Actividades a realizarse para la auditoria interna de la norma ISO/IEC 27001:2005

Definición de Áreas involucradas para la realización de Auditoria Interna.
Establecimiento de un Programa General de Auditoría por áreas involucradas

Definición de equipos de trabajo

Definición de personal a ser evaluado y establecimiento de cronograma de reuniones

Selección de activos de información a ser evaluados aplicando los controles de la norma ISO/IEC 27001:2005

Selección de procedimientos, estándares, normativas y documentos a ser evaluados aplicando los controles de la norma ISO/IEC 27001

Definición de un programa detallado de auditoría por áreas involucradas.

Reunión de apertura de la auditoria:

Fecha: Jueves, 21 de Febrero del 2013:

Hora de Inicio: 09H00 Hora Fin:11H00

Áreas a ser auditadas

Considerando el procedimiento interno de Prestación de Servicios de Datos, Internet y Valor Agregado para clientes Corporativos y Pymes y los

anexos del A5 al A15 de la norma ISO/IEC 27001:2005; se han definido las siguientes áreas involucradas:

- Comercial
- Soluciones Corporativas
- O&M Core y Plataformas
- O&M TX (MPLS)
- Gerencia Nacional de TI
- Áreas de Soporte del SGSI (Jurídico, Seguridad Física, Asuntos regulatorios y Desarrollo Organizacional.)

Definición de equipos de trabajo

Para la definición de equipos de trabajo se consideraron a todos los integrantes del grupo de Seguridad de la Información de la CNT EP., y como parte de la realización de Tesis previo la obtención del título de magister auspiciado por la corporación, el investigador formó parte del equipo auditor para la realización de la presente auditoría, de modo que cada equipo de trabajo este conformado por un Auditor líder y un asistente, el total se formaron cuatro de equipos.

Continúa

Las áreas a ser auditadas son:

Tabla 9. Áreas a ser Auditadas.

ÁREA
Gerencia Comercial
Gerencia Soluciones Corporativas
Gerencia de O&M Core y Plataformas
O&M TX
Desarrollo TI
Arquitectura TI
BDD TI
Gestión de la Calidad de TI
GNTI
Redes TI

Servidores TI
Data Center TI
Gestor de Cambios
Encargado SGSI
Oficial de Seguridad de la Información
Representante de Gerente General
JUR
ARI
Seguridad Física
DEO

Continúa

Una vez definidas las áreas involucradas, los equipos de trabajo y considerando: el tiempo de trabajo, los requisitos y los controles a ser auditados; se establece en términos de tiempo la realización de las auditorías tomando en cuenta que en una sola visita se debe completar tanto las entrevistas como la auditoría de controles.

Tabla 10. Cronograma de auditoría por áreas.

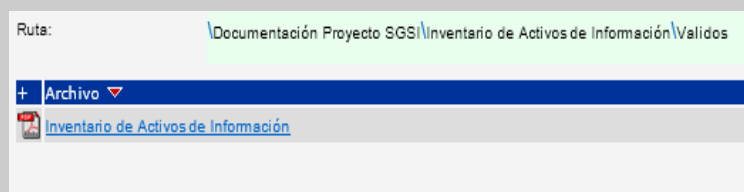
Fecha / Área	25-feb	25-feb	27-feb	28-feb	01-mar
Gerencia Comercial	X				
Gerencia Soluciones Corporativas			X		
Gerencia de O&M Core y Plataformas	X				
O&M TX		X			
Desarrollo TI			X		
Arquitectura TI				X	
BDD TI					X

Gestión de la Calidad de TI					X
GNTI		X			
Redes TI		X			
Servidores TI			X		
Data Center TI		X			
Gestor de Cambios	X				
Encargado SGSI		X			
Oficial de Seguridad de la Información	X				
Continúa					
Representante de Gerente General		X			
JUR	X				
ARI	X				
Seguridad Física			X		
DEO				X	

Activos seleccionados

Por temas de confidencialidad la organización auspiciante no autoriza la divulgación de esta información.

Los activos de información se encuentran detallados en el documento: "Inventario de Activos de Información". Almacenado en la aplicación interna MAI.




u*Mostrando archivos, pantalla principal. (41) 2013-08-27 19:56:55 | [Imprimir](#)

Imagen 26. Captura de pantalla Documento “Inventario de Activos de Información” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial.

Procedimientos seleccionados

Los procedimientos a ser revisados fueron seleccionados considerando aquellos que se alineen con los activos de información determinados y que cubrían más áreas dentro de la organización. A continuación se detallan los procesos escogidos por área involucrada:

Continúa

	INVENTARIO DE ACTIVOS DE INFORMACIÓN			
	Responsable: Seguridad de la Información	Fecha: Octubre 2011	Versión: 1.0	Página Número: 4 de 7

1. Objetivo

Relacionar los activos de información que han sido identificados para el Proceso de Venta e Instalación de Productos y Servicios de Datos e Internet para Clientes Corporativos en el Distrito Metropolitano de Quito.

2. Trabajo realizado

1. Se realizaron entrevistas con los dueños de los procesos (o sus delegados) para identificar los activos de información, y la información que generan, procesan y/o resguardan.

Las personas entrevistadas fueron las siguientes:

Nombre	Área
Juan Francisco Makionado	Clientes Corporativos y PYMES
Oscar Correa	Soluciones Corporativas
Edwin Logroño	Soluciones Corporativas
Ana Alquiunga	Soluciones Corporativas
Richard Montalvo	Soluciones Corporativas
Edmundo Albuja	O&M Regionales (Multiservicios)
Jairo Suntaxi	O&M de Plataformas IP-MPLS
Geovanny Chanataxi	O&M de Soluciones (Soluciones de Internet, TV y Datos)
Pablo Zapata	O&M de Soluciones (Soluciones de Internet, TV y Datos)
Cristhian Andrango	O&M de Soluciones (Soluciones de Internet, TV y Datos)
Edith Ocampo	O&M de Soluciones (Soluciones de Internet, TV y Datos)
Jessica Cruz	O&M de Soluciones (Soluciones de Internet, TV y Datos)

Imagen 27. Captura de pantalla Documento “Inventario de Activos de Información_ objetivos” alojado

en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial.

Área Comercial

Procedimiento para cambio de formatos a la gerencia de soluciones corporativas

Gerencia de Soluciones Corporativas

Procedimiento Cambio de Formatos Gerencia de Soluciones Corporativas
Estándar de seguridad de documentos electrónicos
Procedimiento de Configuración de Enrutadores de Prestación de Servicios de Clientes Corporativos de la CNT EP

Gerencia Nacional de Desarrollo Organizacional

N/A

Jefatura de IP MPLS

Procedimiento de administración de privilegios de acceso a la red MPLS
Estándar de Usuarios y Contraseñas para Acceso a Recursos de MPLS
Continúa

Gerencia Nacional de Tecnologías de la Información

Procedimiento para la Administración de OpenFlexis
Procedimiento Administración Seguridad Red Interna CNT EP
Procedimiento para la creación, modificación y eliminación de accesos de usuarios en sistemas y aplicaciones
Procedimiento Creación de VLANS
Procedimiento Manejo de logs de Auditoria en Sistemas Operativos de Servidores
Procedimiento para la revisión de privilegios de acceso
Procedimiento de control de acceso a la red de comunicaciones de la CNT EP
Procedimiento de control de acceso remoto autorizado a la red de CNT EP
Procedimiento Verificación de Tablas Auditadas
Procedimiento de creación de VLANs
Procedimiento Asignación Eliminación de Puertos a VLANS
Procedimiento de traslados de equipos del Data Center de la CNT EP
Procedimiento de control físico y ambiental del Data Center de la CNT EP
Procedimiento de generación y almacenamiento de copias de respaldo
Procedimiento de control de almacenamiento y control de acceso a documentos
Procedimiento de Control de Calidad
Proceso de Gestión de Cambios
Procedimiento para actualización de sistemas operativos en servidores
Procedimiento de manejo y reporte de fallas de sistemas operativos

Procedimiento para segregación de funciones en sistemas operativos de servidores
 Normativa de Roles y responsabilidades de seguridad
 Normativa de control de acceso
 Normativa de Administración de Seguridad de la red interna
 Estándares de programación del área de desarrollo de TI
 Estándar de seguridad de los documentos electrónicos

Gerencia Nacional Jurídica

N/A

Jefatura de O&M Core y Plataformas

Procedimiento de control de cambios en las plataformas de servicios complementarios del ISP
 Procedimiento de reporte y manejo de fallos de los equipos del ISP de la CNT EP
 Procedimiento de control físico y ambiental del nodo del ISP
 Procedimiento de acceso y control de cambios al archivo maestro de direccionamiento ip corporativos
 Procedimiento de generación y almacenamiento de copias de respaldo

Continúa

Jefatura de Seguridad y Vigilancia

Estándar de seguridad física y ambiental de documentos físicos
 Procedimiento de Acceso a los edificios administrativos de la CNT EP.
Gerencia Nacional de Asuntos Regulatorios e Interconexión
 N/A

LOGÍSTICA:

Logística

En este aspecto se fijan elementos como, cronograma de trabajo, delegados por área a ser auditada, seguridad, transporte, idioma, equipos de medición (todo lo necesario para llevar a cabo la auditoria).

Cronograma de reuniones

Considerando los equipos de trabajo para las entrevistas donde se evaluarán tanto requisitos como controles de la norma ISO/IEC 27001:2005, se detalla el siguiente cronograma, en el cual constan los delegados por área a ser auditada:

Tabla 11. Delegados por cada área a ser auditada

ÁREA	CONTACTO	EDIFICIO
-------------	-----------------	-----------------

Gerencia Comercial	Jefe comercial de clientes VIP	Doral
Gerencia Soluciones	Gerente de Soluciones	Vivaldi
Gerencia de O&M Core y Plataformas	Jefe de operación y mantenimiento	Droira
O&M TX	Jefe de MPLS	Mariscal
Desarrollo TI	Jefe Desarrollo TI	Iñaquito
Arquitectura TI	Jefe Arquitectura TI	Iñaquito
BDD TI	DBA	Iñaquito
Gestión de la Calidad de GNTI	Jefe de control de calidad	Iñaquito
Redes TI	Gerente Nacional de TI	Iñaquito
Servidores TI	Administrador de Redes	Iñaquito
Data Center TI	Administrador de Jefe Data Center	Iñaquito
Gestión de Cambios	Gestor de Cambios	Iñaquito
Encargado SGSI	Encargado SGSI	Iñaquito
Oficial de Seguridad de la Información	Oficial de Seguridad de la Información	Iñaquito
Representante de Gerente General	Representante de Gerente General	Iñaquito
JUR	Analista Jurídico	CETA
		Continúa
ARI	Jefe de Interconexión	Vivaldi
Seguridad Física	Jefe de Seguridad y Vigilancia	Droira
DEO	Gerente de R.R.H.H.	Doral

Recursos (Transporte y comunicación.)
Para la realización de las auditorías, el equipo de trabajo coordinó en algunos casos la movilización a los diferentes edificios
Para confirmaciones, agendas, comunicaciones vía telefónica, se utilizó la red interna de CNT EP, el cual incluye telefonía IP, internet e intranet.

Materiales
Los documentos se elaboraron dentro de las instalaciones de CNT EP., por lo que todos los materiales de oficina, el uso de equipos informáticos (PCS, impresoras, scanner) fue proporcionado por la corporación.

Idioma:
Los delegados a ser entrevistados no requieren de un traductor al hablar el idioma castellano y ser ciudadanos ecuatorianos; por lo que, el equipo auditor se exenta de contratar servicios adicionales de traducción si su perfil no incluye el habla de idiomas extranjeros.

Levantamiento de información:
Para levantar la información que permita determinar si los hallazgos son no conformidades mayores y menores, se realizaron verificaciones in situ, entrevistas, revisiones vs preguntas y respuestas de los entrevistados,

constatación de controles administrativos los cuales se tomará como evidencia para el informe preliminar que realizará cada equipo de trabajo.

AUTORIDAD

Autoridad Por último, se realiza el r (CNT EP, 2012)registro de la firma del Oficial de Seguridad de la Información por la revisión del documento y del representante de la Gerencia General para la aprobación del documento.

Revisión del Documento			
Nombre	Cargo	Versión	Firma
No Autorizado	Oficial de Seguridad de la Información	1.0	No Autorizado

Aprobación del Documento			
Nombre	Cargo	Versión	Firma
No Autorizado	Representante del Gerente General	1.0	No Autorizado

Imagen 28. Captura de pantalla de revisión y aprobación de Documento "Plan de Auditoria Interna" alojado en el Sistema MAI, aplicación interna CNT EP.
Tipo de documento: Confidencial.

4.1.3. Realizar la auditoría interna.

La auditoría interna inicia con la reunión de apertura, en la que se presenta a los participantes los lineamientos para proseguir con la auditoria in situ a realizarse, además de definir fechas de revisión, reunión de cierre y presentación de resultados.

4.1.4. Reunión de Apertura y actividades.

Fecha: Jueves, 21 de febrero de 2013 y Viernes 23 de febrero de 2013.

En base al plan de auditoria elaborado y de acuerdo a los aspectos descritos en el punto 4.2., se ejecutó la auditoria interna iniciando con la reunión de apertura registrada con fecha jueves, 21 de febrero del 2013 desde las 09h00 a.m. hasta las 11H00 a.m. presentándose el plan de auditoria acordando que el mismo sería ejecutado en el transcurso de las siguientes dos semanas laborables, fue revisado por todo el equipo auditor y líder de auditoría, realizándose ajustes de acuerdo a la fase de planificación.

Se efectuaron ejercicios sobre cómo realizar las entrevistas, algunas pautas para mostrar confianza a los auditados, del cómo va a ser la comunicación con los delegados de cada área a ser auditada, como actuar si existiera controversia entre auditor y auditado la misma que deberá quedar resuelta en el transcurso de la auditoria, como realizar las observaciones, revisión de documentos donde se deben mantener la confidencialidad de toda la información revisada y metodología para realizar la auditoria, siendo esta última propia de CNT EP.

Se definió el tiempo de duración para cada entrevista en la cual se tomó en cuenta la movilización y la auditoria misma, el tiempo otorgado fue de dos horas; en este periodo se incluye el tiempo de espera para el inicio de cada entrevista de auditoria cuyo umbral fue de diez minutos, al igual que la fecha de la reunión de cierre.

Tabla 13. Cronograma de trabajo acordado para la realización de auditoria interna.

	Lunes	Martes	Miércoles	Jueves	Viernes
S1	Auditorias				
S2	Inf. Preliminar Equipo Auditor	Inf. Preliminar Equipo Auditor	Inf. Preliminar/Reunión Cierre	Elaboración Inf. Auditoría/Plan Acción Preliminar	Presentación

Consecutivamente se realizó la actividad de acordar entrevistas con los delegados de cada área auditada, tomando la premisa que de acuerdo a la disposición de la Gerencia General es de carácter obligatorio colaborar con las auditorías a realizarse y participar activamente el día que haya sido designado para la entrevista, en casos de fuerza mayor el delegado debió designar a personal de apoyo para que participe en la auditoria. Esta actividad tomó un tiempo de dos días a partir de la reunión de apertura (21-02-2013) hasta el siguiente día (22-02-2013) en coordinar agendas, transporte y material de apoyo.

Para el contacto con el personal a ser auditado se determinó que al menos con cuarenta y ocho horas (48h) de anticipación se confirmará el lugar y fecha de la

auditoría conforme al plan enviado por los medios de comunicación masiva interna de la CNT EP. En caso de que se requiera una reprogramación se lo realizará dentro de los días de la auditoría ya establecidos.

4.1.5. Realización de Auditoría (25 -02-2013 / 01-03-2013) AI1

Tabla 14. Cronograma semana 1 Auditoría AI1.

Lunes	Martes	Miércoles	Jueves	Viernes
25 de febrero	26 de febrero	27 de febrero	28 de febrero	01 de Marzo
S1		Auditorias		

En la semana del 25 de febrero al 01 de marzo se realizó la auditoria propiamente dicha, los respectivos grupos de trabajo se trasladaron a las diferentes áreas a ser auditadas de acuerdo al cronograma siguiente:

Tabla 15. Equipos de trabajo por área a ser auditado

Área	25- feb	25- feb	27- feb	28- feb	01- mar
------	------------	------------	------------	------------	------------

Gerencia Comercial	X	
Gerencia Soluciones Corp.		X
Gerencia de O&M Core y Plataformas	X	
Continua		
O&M TX		X
Desarrollo TI		X
Arquitectura TI		X
BDD TI		X
Gestión de la Calidad de GNTI		X
Redes TI	X	
Servidores TI		X
Data Center TI		X
Gestor de Cambios	X	
Encargado SGSI		X
Oficial de Seguridad de la Información	X	
Representante de Gerente General		X
JUR	X	
ARI	X	
Seguridad Física		X
DEO		X

Los equipos de auditores ejecutaron las respectivas entrevistas y recopilaron la evidencia de cumplimiento (registros de auditoría) con los cuales posteriormente se elaboraron los informes preliminares.

En esta misma semana se envió la convocaría vía oficio a la áreas involucradas a la presentación oficial del informe de auditoría y la convocatoria a la reunión de cierre a los miembros del equipo de auditores para evitar contratiempos de última hora.

4.1.6. Recopilación de datos (04 -03-2013 / 08-03-2013) AI1

La segunda semana, el día lunes 04 de marzo hasta el día viernes 08 de marzo de 2013, correspondió a la recopilación de los informes preliminares de cada equipo auditor, la elaboración del informe preliminar con la valoración de hallazgos vs controles de la norma y presentación oficial a la alta dirección.

Tabla 16. Cronograma semana 2 Auditoria.

	Lunes	Martes	Miércoles	Jueves	Viernes
	04 de Marzo	05 de Marzo	06 de Marzo	07 de Marzo	08 de Marzo
S2	Inf. Preliminar Equipo Auditor	Inf. Preliminar Equipo Auditor	Inf. Preliminar/Reunión Cierre	Elaboración Inf. Auditoría/Plan Acción Preliminar	Presentación

Para cumplir con esta acción cada auditor líder elaboró un formato preliminar que contenía las observaciones encontradas en la auditoría realizada según la designación de áreas descritas en el punto 4.3.2., para luego entregarlo al encargado de la auditoría interna, quien a su vez consolidó los hallazgos en un informe preliminar de previa revisión y aprobación.

4.1.7. Verificación de controles.

Una vez que se ha completado la auditoria, el auditor líder realizó una revisión privada de hallazgos, cuyo resultado fue puesto en consideración en la reunión de cierre.

La revisión realizada por el auditor líder incluyó:

- Revisión de las listas de verificación,
- Un estudio de las notas y/u observaciones tomadas en las entrevistas por todos los miembros del equipo auditor.
- Lista de hallazgos
- Enumeración de las no conformidades y áreas de mejora.
- Redacción y clasificación de las acciones correctivas (Plan de Acción).

Los hallazgos de auditoria fueron clasificados de acuerdo a lo indicado en el plan de auditoria descrito en el punto 4.2, donde:

- Una NC+ se levanta cuando el proceso o procedimiento que está siendo auditado no opera o funciona como debería; en ISO/IEC 27001:2005, una NC+ es un incumplimiento de un requisito específico.

Estas NC fueron registradas de acuerdo a la evaluación realizada con el apoyo de la respectiva evidencia de auditoría, la misma que fue revisada con el delegado del

área auditada obteniendo el reconocimiento de la evidencia, indicando que esta es precisa y que la NC es entendida.

- La declaración de los hallazgos se realizó incluyendo:
- Una visión global del hallazgo.
- Una descripción de la no conformidad.
- Si aplica un muestreo de evidencias y
- Un resumen del requisito.

En los hallazgos encontrados también se encontraron Oportunidades de Mejora, las mismas que en gran parte son un valor añadido a la auditoria y que posiblemente no requieran de una acción correctiva pero que si desean ser comentadas por el equipo auditor.

Estas observaciones incluyeron:

- Puntos que preocupan, pero aún no lo suficiente como para ser considerados una NC y que necesiten encontrarse en el plan de acción.
- Situaciones que si no se identifican, en lo posterior podrían incurrir en NC.

Con estas aclaraciones, a continuación mostramos la matriz de hallazgos encontrados en la auditoría interna realizada en el mes de Febrero 2013 con el

desarrollo de los conceptos descritos en base a los anexos de la norma y los controles aplicables de la corporación, esto se podrá verificar en la sección anexos.

4.1.8. Elaborar el informe de auditoría interna y desarrollar un plan de acción preliminar.

El contenido de este informe fue puesto en consideración en la reunión de cierre que tuvo como fecha de registro el día miércoles 06 de marzo del 2013 desde las 14h30 hasta las 16h30, donde se expuso las novedades encontradas en la auditoria, auto evaluando la identificación o levantamiento de hallazgos y analizando cada uno de los hallazgos encontrados para clasificarlos como:

No Conformidades (NC+/-): las cuales serán tratadas con: Acciones correctivas o acción preventivas de acuerdo al procedimiento Acciones Correctivas y Acciones Preventivas.

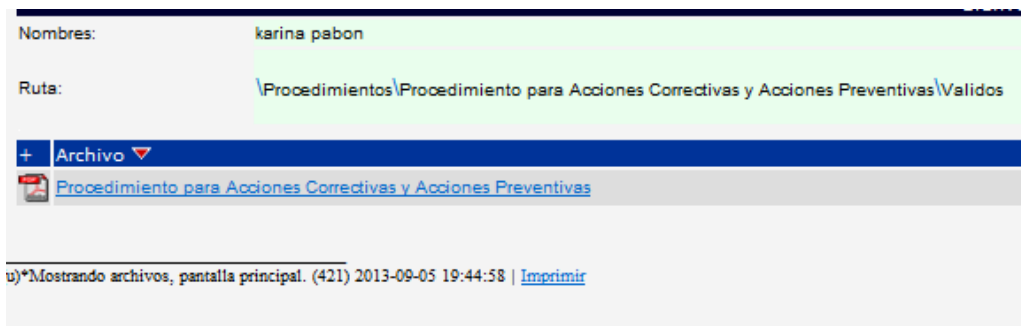


Imagen 29. Captura de pantalla del Documento “Procedimiento para Acciones Correctivas y Acciones Preventivas” alojado en el Sistema MAI, aplicación interna CNT EP.

Tipo de documento: Confidencial.

Oportunidades de mejora: a las cuales se les dará tratamiento inmediato quedando solventadas en el lugar que se haya efectuado la auditoria interna.

Una vez con el informe preliminar aprobado se conversó con cada entrevistado para obtener su opinión y aprobación sobre el hallazgo encontrado; esto, con la finalidad de generar el respectivo plan de acción.

Una vez concluido el informe preliminar y formalizado el plan de acción, se elaboró el resumen ejecutivo y el informe detallado de la auditoría interna para posteriormente presentarlos a las gerencias de la CNT EP., estas presentaciones se realizaron los días viernes 08 de marzo del 2013 para la AI1, y el día miércoles 11 de septiembre del 2013 para la AI2.

4.1.9. Presentación de hallazgos a la alta gerencia

El informe de auditoría es un medio formal para comunicar los objetivos, el alcance, las observaciones, hallazgos, conclusiones y recomendaciones. Este informe representa el momento adecuado para separar lo significativo de lo no significativo, debidamente evaluados por su importancia y vinculación con el factor riesgo, reflejados en una presentación lógica y organizada, el cual debe poseer la suficiente información para que sea comprendido por los destinatarios esperados y facilitar las acciones correctivas.

El resumen ejecutivo se realizó de acuerdo a las especificaciones incluidas en el Plan de Auditoría descrito en el punto 4.2. y también publicado en el sistema MAI.




Ruta: \Documentación Proyecto SGS\Auditorías Internas\Obsoletos		Opciones:
+ Archivo ▾		Última revisión ▾
 Plan de Trabajo Auditoria Interna Enero 2013		2013-01-02 09:50:57
 Plan de Acción AI Enero 2013		2013-02-13 09:02:53
 Informe Auditoria Interna Enero 2013		2013-01-30 09:05:24

Imagen 30. Captura de pantalla del Documento “Informe Auditoría Interna Enero 2013” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial. **AI1 Enero.**

Ruta: Documentación Proyecto SGS\Auditorías Internas\Validos		Opciones:
+	Archivo	Última revisión
	Reporte Asistencia Presentación Hallazgos AI Septiembre 2013	2013-09-13 14:42:50
	Plan de Trabajo Auditoria Interna Septiembre 2013	2013-09-13 14:41:39
	Plan de Acción AI Septiembre 2013	2013-09-13 14:41:18
	Informe Auditoria Interna Septiembre 2013	2013-09-13 14:41:00

Imagen 31. Captura de pantalla del Documento “Informe Auditoría Interna Septiembre 2013” alojado en el Sistema MAI, aplicación interna CNT EP. Tipo de documento: Confidencial. AI2 Septiembre.

La primera auditoría en sitio AI1 se llevó a cabo del 25 de febrero al 01 de marzo del 2013, para lo cual se ejecutaron 20 reuniones que se detallaron en el punto 4.3.2 (CNT EP, 2013).

La segunda auditoria en sitio AI2 se llevó a cabo del 02 al 06 de Septiembre del 2013, para lo cual se ejecutaron 23 reuniones a las áreas mencionadas la Tabla 12 con sus respectivos grupos de trabajo.

Los equipos de trabajo en conjunto detallaron los hallazgos encontrados en cada una de las auditorías realizadas AI 1 y AI 2 registrando los más significativos y los cuales fueron objeto de recomendaciones para ejecutar planes de acción inmediata,

cuyo resumen de los mismos serán indicados en los puntos 4.5.1 y 4.5.2.,
respectivamente.

Tabla 12. Equipos de trabajo por área a ser auditado

	2-sep	3-sep	4-sep	5-sep	6-sep
Gerencia Comercial	X				
Gerencia Soluciones Corporativas		X			
Gerencia de O&M Core y Plataformas	X				
O&M TX					X
Desarrollo TI			X		
Arquitectura TI				X	
BDD TI					X
Aplicaciones de TI					X
Gestión de la Calidad de TI					X
GNTI		X			
Redes TI			X		
Servidores TI			X		
Data Center TI		X			
Gestor de Cambios	X				
Encargado SGSI		X			
Oficial de Seguridad de la Información			X		
Representante de Gerente General				X	
JUR	X				
ARI			X		
Seguridad Física				X	
Gestor de Incidentes		X			
Service Desk	X				
DEO				X	

4.1.10. Resumen de Hallazgos Identificados en la Auditoría Interna Febrero AI 1

Producto de la Auditoría Interna realizada en fechas de Febrero (AI1) se obtuvieron los resultados mostrados en el Grafico 2.

En la AI 1 se identificaron “No Conformidades Mayores” que no permitirían al SGSI de la CNT EP, ser recomendado para certificarse bajo la norma ISO/IEC 27001:2005:2005.

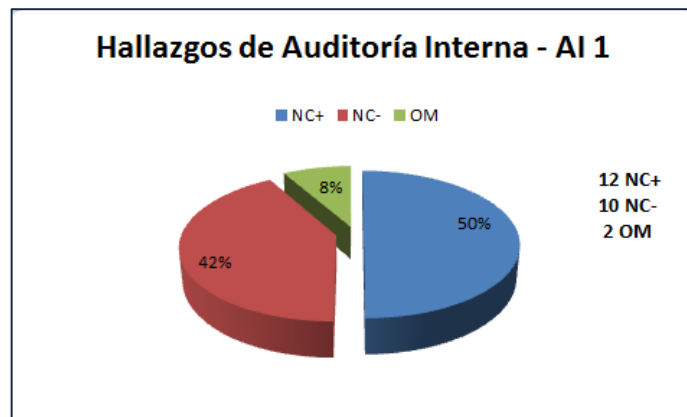


Gráfico 2. Hallazgos de Auditoría Interna AI 1

(NC+ = No conformidades mayores; NC- =

No Conformidades Menores; OM = Oportunidades de Mejora).

4.1.11. Hallazgos

A continuación se muestran los Hallazgos de la auditoria interna de febrero:

Tabla 16. Hallazgos de Auditoría AI 1

N°	Aspecto	Área /Activo	NC +	NC- /OM	N#
1	<p>Aunque el manual del SGSI y los documentos anexos se encuentran publicados en la Herramienta MAI, identificamos que no existe un adecuado conocimiento de las definiciones del SGSI, Manual del SGSI y Política de Seguridad de la información y su ubicación. En las entrevistas realizadas al personal responsable de las áreas involucradas en el proceso sobre el cual se está implantando el Sistema de Gestión de Seguridad de la Información en la Corporación, se verificó que con excepción del oficial de seguridad de la información, el resto de los involucrados los representantes de las área O&M Core y Plataformas, MPLS, Jurídico, ARI, Comercial, GNTI, Seguridad Física y DEO no manejan adecuadamente las definiciones del SGSI, Manual del SGSI, Política de Seguridad de la Información, registros de seguridad y su ubicación.</p>	Áreas involucradas en el alcance del SGSI	X		5.2.2 Capacitación, sensibilización y competencia.
2	<p>Aunque existe un documento que establece el plan de tratamiento para los riesgos identificados en los activos de información, se evidencio que existe confusión y en otros casos desconocimiento de las acciones ejecutadas por cada área para el cumplimiento de dichos planes de tratamiento asociadas a los activos de información y la documentación soporte generada de tal actividad.</p>	Áreas involucradas en el alcance del SGSI	X		4.2.3d Monitorear y revisar el SGSI

Continúa

3	<p>Aunque se ha definido una "Normativa de Administración de incidentes de Seguridad de la información" u "Procedimiento de gestión de incidentes de seguridad de la información", se evidencio que no todo el personal entrevistado tiene claramente definido a quien y como reportar un incidente de Seguridad de la información.</p> <p>Así mismo, algunos de ellos confunden el concepto de incidente de seguridad de la información.</p> <p>En las entrevistas realizadas al personal responsable de las áreas involucradas en el SGSI, se verificó que los representantes de las áreas JUR, GNTI, Seguridad Física y DEO no tienen claro a quien y como reportar un incidente de seguridad de la información</p>	Áreas involucradas en el alcance del SGSI	X	<p>4.2.3 a Monitorear y revisar el SGSI. A13.1.1 Reporte de eventos en la Seguridad de la información. A13.1.2 Reporte de las debilidades en la seguridad A13.2.2 Aprender de los incidentes de la seguridad</p>
4	<p>Aunque se ha definido un programa de Capacitación del SGSI para el personal de CNT EP, en las entrevistas realizadas al personal delegado de las áreas involucradas en el alcance SGSI, se identificó que el 30% de las personas entrevistadas no respondieron claramente su han tenido una capacitación formal de aspectos de seguridad de la información.</p>	Áreas involucradas en el alcance del SGSI	X	<p>5.2.2 Capacitación, sensibilización y competencia.</p>
5	<p>Aunque se ha definido un programa de Capacitación del SGSI para el personal de CNT EP, en las entrevistas realizadas al personal delegado de las áreas involucradas en el alcance SGSI, se identificó que el 30% de las personas entrevistadas no respondieron claramente su han tenido una capacitación formal de aspectos de seguridad de la información</p>	Áreas involucradas en el alcance del SGSI	X	<p>5.2.2 Capacitación, sensibilización y competencia</p>

Continúa

6	<p>De las 21 reuniones programadas, 14 fueron cumplidas con normalidad de acuerdo a lo planificado, 2 fueron cambiadas en día y hora, 2 iniciaron con retraso, 1 no fue y 2 fueron comprometidas por interrupciones durante la entrevista.</p>	<p>Áreas involucradas en el alcance del SGSI</p>	X	<p>5.1d 5.1e Compromiso de la gerencia.</p>
<p>O&M: empezó con 10 min de retraso. BDD: se ausentó de la primera reunión y solicitó una nueva entrevista. QA: Cambio de Hora. Seguridad física: Retraso a la reunión. DEO y COM: Interrupciones durante la entrevista. Arquitectura de TI: No se presentó (a pesar de que se planificó la entrevista para una segunda ocasión).</p>				
7	<p>La declaración de aplicabilidad del SGSI, establece la existencia de la "Normativa de Seguridad de la información para la Administración del Recurso Humano", sin embargo la misma no se encuentra formalizada y difundida.</p>	<p>Áreas involucradas en el alcance del SGSI</p>	X	<p>5.1d Compromiso de la gerencia A8.1.2 Investigación de antecedentes A8.2.1 Responsabilidades de la Gerencia A8.2.3 Proceso disciplinario.</p>

Continua

8	Existe una iniciativa por parte del grupo de seguridad de la información para el último viernes de cada mes dar charlas de sensibilización tanto a nuevos empleados de CNT EP como a proveedores, sin embargo, esta actividad no se cumple adecuadamente ni se encuentra documentada, formalizada ni difundida.	Seguridad de la Información.	X	5.2.2 Capacitación, sensibilización y competencia.
9	En la declaración de aplicabilidad del SGSI, se establece que Términos y definiciones se encuentran plasmados en el documento Normativa de Seguridad del Recurso Humano sin embargo, se evidencio que en la práctica esto ha sido plasmado en el contrato de trabajo que los servidores firman al ingresar a CNT EP.	Seguridad de la Información.	X	A8.1.3 Términos y condiciones

Continua

10	<p>En las revisiones efectuadas se evidenció que la Corporación no cuenta con un plan de continuidad del negocio, formalmente establecido, documentado y probado el cual les permita seguir operando en caso de una contingencia. Existe un proyecto ejecutándose al momento de la Auditoría Interna, cuyo resultado final será el BCP para el proceso del alcance de la Certificación.</p>	Seguridad de la Información.	X	<p>4.2 Establecimiento y manejo del SGSI.</p> <p>A.14 Gestión de la Continuidad del Negocio.</p>
11	<p>Aunque se ha establecido una Normativa de Cumplimiento Legal, este documento no se encuentra bajo conocimiento de los representantes de las Gerencias Nacionales JUR y ARI, a pesar de dichas gerencias participaron en la revisión del mismo.</p>	Jurídica, ARI	X	<p>4.2. b2 Establecer el SGSI.</p> <p>A15.1 Cumplimiento de los requisitos legales.</p> <p>A15.1.4 Protección y privacidad de gastos.</p> <p style="text-align: right;">Continúa</p>
12			X	

	Si bien se ha definido un área específica para la ubicación de equipos de comunicación de la red IP-MPLS, en la visita efectuada a este sitio se verificó que la puerta permanece sin seguro.	IP-MPLS Equipos de comunicación de red de prestación de servicios de datos e internet.		A9.1.2 Controles de ingreso Físico.
13	Aunque se han definido e implementado políticas y estándares de accesos y autenticación de usuarios en los recursos de información, se verificó que no son revisados regularmente con el objetivo de verificar su cumplimiento.	Seguridad de la información	X	A15.2.2 Revisión del cumplimiento técnico.
14	Si bien cada área del alcance del SGSI ingresa solicitudes de cambios y/o modificaciones en sistemas, aplicaciones y servicios especiales. (Bases de datos y operativos), y estas pueden ser ubicadas en el sistema Remedy se identificó que no se mantiene un registro de todos los cambios y/o	Áreas involucradas en el alcance del SGSI	X	A10.1.2 Gestión del Cambio A12.5.1 Procedimiento de Control de Cambio
				Continúa

modificaciones realizados. Además se identificó que no se cuentan con procesos formales para Soluciones de TI y QA.

15	Si bien en los recursos de programación se ha configurado el cambio de clave en el primer inicio de sesión, se evidenció que no exista un proceso formal para la entrega y recepción de claves asignadas a los usuarios con acceso a dichos recursos.	GNTI	X	A11.2.3 Gestión de las claves secretas de los usuarios.
16	Aunque se aprobó el documento "Procedimiento de control de almacenamiento y control de acceso a documentos" que establece una revisión semestral de los usuarios con acceso a documentos en el file server a la fecha de la auditoría dicha revisión no se ha realizado.	Áreas involucradas en el alcance del SGSI	X	A11.1.1 Política de control de acceso. A11.2.4 Revisión de los derechos de acceso del usuario.
17			X	Continúa

	Aunque la Corporación ha establecido personal autorizado para el acceso al Data Center de la GNTI, se identificó que no se realizan revisiones periódicas de tales accesos	Tecnologías de la Información/Data Center Servidor de la BDD y Open Flexis y SAFA		A9.1.2 Controles de ingreso físico
18	Aunque existen controles físicos para el acceso a los edificios de la Corporación, se identificó que estos no siguen un mismo lineamiento y estándar de control de acceso. Se evidenció en las distintas visitas realizadas a los edificios de la CNT EP, que para el acceso a los mismos los guardias de seguridad mantienen diversos controles de revisión y bitácoras de registros no estandarizadas.	Seguridad de la información	X	A9.1.2 Controles de ingreso físico
19	En la Gerencia Comercial, se identificó que el archivo de propuesta comercial no ha sido identificado y etiquetado como público, privado o	Gerencia Comercial	X	A7.2 Clasificación de la información. Continúa

confidencial según corresponda.				
20	En Soluciones Corporativas, se validó que no existe la difusión del nuevo formato de factibilidades técnicas, según se establece en el procedimiento.	Soluciones Corporativas	X	A10.1.2 Gestión de Cambios.
21	En el área de servidores de la GNTI se evidenció que no se cuenta con una Normativa enfocada al borrado de datos en equipos que son reciclados.	GNTI	X	A9.2.6 Seguridad de la eliminación o re-uso del equipo.

4.2.1. Conclusiones de Auditoría Interna (AI 1)

Como conclusiones para esta Auditoría, en la presentación del informe se indicó:

- El sistema de Gestión de seguridad de la información (SGSI) de la CNT EP, implementado para el proceso de “Venta e instalación de productos y servicios de datos e internet para clientes corporativos del distrito metropolitano de Quito” cumple parcialmente los requisitos que demanda la Norma Internacional ISO/IEC 27001:2005:2005 ya que no hubo un acercamiento suficiente a los objetivos de seguridad de la información establecidos en la política del SGSI, así mismo, que los controles implementados no se encuentran operando eficientemente.
- La documentación es adecuada ya que se encuentra orientada a cumplir con los parámetros definidos por CNT EP de acuerdo a su Sistema de

Gestion de Seguridad de la Informacion ISO/IEC 27001:2005; sin embargo, es necesario que la compañía realice un esfuerzo adicional para garantizar que los directivos y sus colaboradores conozcan, comprendan y cumplan con los documentos regulatorios publicados en el Sistema MAI, así como para que se logre un cambio de cultura organización que permita madurar adecuadamente al SGSI.

4.2.2. Tratamiento de hallazgos de Auditoría Interna (AI1)

- Continuar con los planes de sensibilización a todos los colaboradores de todos los niveles de la CNT EP involucrados en el SGSI, enfocándose más en aquellos que no han tenido un nivel adecuado de participación, compromiso y conocimiento.
- Fortalecer con apoyo de los Gerentes involucrados la difusión y aplicación de los controles administrativos del SGSI, mismos que se encuentran publicados en la Herramienta MAI.
- Incentivar el compromiso y cambio de cultura organización en la CNT EP para que la gestión del SGSI sea asumida por todos sus involucrados por convicción más que por obligación.
- La seguridad de la información hace parte del Gobierno Corporativo de la organización por lo cual se recomienda reubicar el nivel jerárquico del grupo de Seguridad de la Información dentro de la CNT EP.
- Realizar una actualización completa de todo el sistema de Gestión de Seguridad de la Información de la CNT EP, para poder evidenciar el cumplimiento del ciclo de vida (PDCA) y se actualice al menos

anualmente el SGSI o cuando exista un cambio grande en la organización.

4.2.3. Resumen de Hallazgos Identificados en la Auditoría Interna Septiembre AI 2

Producto de la Auditoría Interna realizada en fechas de Septiembre (AI2) se obtuvieron los siguientes resultados:

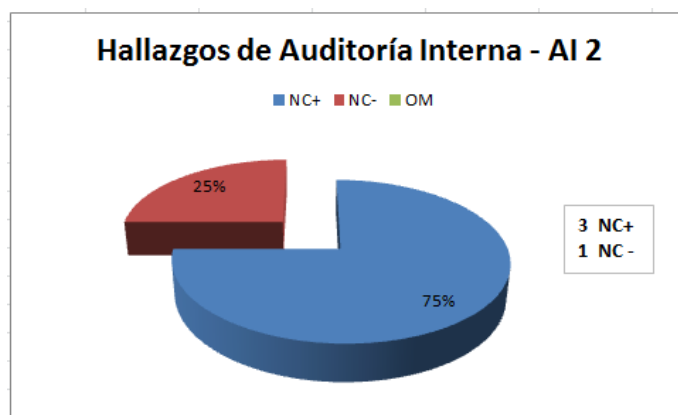


Gráfico 3. Hallazgos de Auditoría Interna AI 2 (NC+ = No conformidades mayores; NC- = No Conformidades Menores; OM = Oportunidades de Mejora).

En la AI 2 se identificaron “No Conformidades Mayores” que no permitirían al SGSI de la CNT EP, ser recomendado para certificarse bajo la norma ISO/IEC 27001:2005:2005, pero estos en menor grado de corrección por lo cual serían mucho mas factibles de tratar y mejorar.

En comparación a los hallazgos encontrados en la anterior auditoría fueron reducidos en gran número.

4.2.4. Hallazgos Auditoría Interna (AI 2)

Tabla 17. Hallazgos de Auditoría AI 2

N°	Aspecto	Área/Activo	NC+	NC-/OM	Numeral
1	Se evidenció que en algunas áreas auditadas que no se tiene una definición clara de la aplicabilidad de los conceptos que son parte del SGSI.	Áreas involucradas en el alcance del SGSI	X		5.2.2 Capacitación, sensibilización y competencia.
2	De las 23 reuniones programadas, 17 fueron cumplidas con normalidad de acuerdo a lo planificado, 3 fueron cambiadas en día y hora, 2 auditorías no se ejecutaron y 1 fue comprometida por interrupciones durante la entrevista.	Áreas involucradas en el alcance del SGSI	X		5.1 Compromiso de la Gerencia.
3	Se identificaron procedimientos que deben ser actualizados, formalizados y difundidos.	Áreas involucradas en el alcance del SGSI		X	4.3.2 Control de documentos
4	Se evidenció que no existe suficiente conocimiento acerca del estado y avance del BCP, específicamente en áreas que están directamente relacionadas a este proceso.	Áreas involucradas en el alcance del SGSI	X		A.14 Gestión de Continuidad del Negocio.
5	Se pudo identificar en algunas áreas que no portaban el carnet corporativo. Se observó que no bloquean los equipos cuando se ausentan de su sitio de trabajo.	Áreas involucradas en el alcance del SGSI		X	A9.1.2 Control de acceso físico
6	No se evidencia la asistencia a las charlas trimestrales del SGSI, a las que deben asistir los involucrados en este proceso.	Áreas involucradas en el alcance del SGSI	X		5.2.2 Capacitación, sensibilización y competencia. Continúa
7	Existen dependencias físicas que no prestan las adecuadas seguridades como cámaras de seguridad o puertas de acceso restringido. Iniciaron proceso de modernización en una de las instalaciones de CNT con la implementación en el control de seguridades de acceso.	Seguridad Física		X	A9.1.2 Control de acceso físico

4.2.5. Conclusiones de Auditoría Interna (AI 2)

Como conclusiones para esta Auditoría, en la presentación del informe se indicó:

- Se detectaron tres “No Conformidades Mayores” que serían causales de no certificación del proceso SGSI en la CNT EP para certificarse bajo la norma ISO/IEC 27001:2005:2005, por lo que se recomienda enfatizar en las capacitaciones a los colaboradores.
- Se identificaron no conformidades que no fueron cerradas en la auditoría interna anterior que mediante la evaluación realizada en el mes de septiembre se volvieron a encontrar y las mismas se engloban en:
 - Compromiso de la Dirección
 - Aplicación de conceptos del SGSI
 - Generación y/o actualización de Procedimientos.
 - Inasistencia a las capacitaciones del SGSI y Seguridad de la Información.

4.2.6. Tratamiento de hallazgos (AI2)

- Aplicar los conceptos de seguridad de la información y los contenidos en la Guía portable para el usuario del sistema de gestión de seguridad de la información.
- Saber ubicar plenamente las políticas, normativas, procedimientos y estándares que son parte del SGSI en el sistema MAI.
- Mantener evidencias y/o registros de las acciones realizadas en torno al proceso del SGSI.
- Compromiso de la Dirección y de todos los usuarios involucrados en el SGSI.
- Asistir a las diferentes capacitaciones que se brindarán en torno al SGSI y el BCP.

4.2.7. Experiencia y Discusión

“No hay nada más difícil de emprender, ni más dudoso de hacer triunfar, ni más peligroso de manejar que el introducir nuevas leyes. El innovador se transforma en enemigo de los que se beneficiaban con las leyes antiguas y no se granjea sino la amistad tibia de los que se beneficiarán con las nuevas. Nicolás Maquiavelo.”
(Maquiavelo, 1513)

Después de la investigación realizada sobre temas de manejo de personal, ejecución de ideas e innovación empresarial, se ha citado muchas veces la frase del famoso Nicolás Maquiavelo y cada vez se concluye que a pesar de haber sido escrita por los años 1500 es una conclusión verdadera y aplicable aun en el siglo XXI.

En verdad, es muy fácil hacer que los seguidores desistan de las ideas de quienes los guían, muy complicado mantener y tener vigente las nuevas leyes, ya que implican sacrificio, trabajo constante e incansable.

4.2.8. Introducción

Con esta meditación se da inicio a la discusión del presente trabajo porque hay que reconocer que en cada realización y ejecución de proyectos siempre nos tropezaremos con serias dificultades que solo con gran valor pueden ser superadas y los cuales una vez en ejecución, la dificultad se centra en la mantención y marcha.

En base a la experiencia obtenida al desarrollar este trabajo y de acuerdo a la fase del proyecto, se ha palpado que fue realmente sencillo aplicar:

- Lo que solicita y exige la norma para la evaluación de requisitos y controles en la auditoría realizada,
- Seguir pasos establecidos y estandarizados en cuanto a validaciones sobre el sistema de gestión de seguridad de la información,
- aplicar metodologías de acuerdo a visiones propias de la empresa sin mayor dificultad.

Sin embargo, lo ciertamente complicado fue evaluar el SGSI con la transición que implica la gestión operativa rutinaria con los cambios que se estaban presentando por la gestión estratégica que la empresa estaba implementando.

En esta transición se evidenciaron factores que se iban visualizando desde diferentes niveles jerárquicos en la empresa, tales como:

- Desmotivación y desconocimiento sobre el proyecto.
- Falta de compromiso tanto de la alta gerencia y los niveles siguientes.
- Resistencia al cambio.
- Falta de concienciación y esperanza de adquirir conocimiento sobre el tema.

Si bien estos factores son los que cualquier empresa puede experimentar al ejecutar un cambio, adaptación y adopción de nuevos procesos; en esta parte se revisará en referencia a la realidad de la empresa, de acuerdo a la naturaleza de la corporación y a la manera en como fue concebida la organización en el transcurrir del tiempo y la actual situación.

4.2.9. Antecedentes

En el capítulo 3, sección 3.1.1 se habló sobre la empresa CNT EP, en resumen se mencionó su nacimiento en el año 2008 como corporación con la fusión de las extintas sociedades anónimas Andinatel y Pacifictel. En enero del año 2010 se convirtió en empresa pública y al poco tiempo oficializó su fusión con la empresa de telefonía móvil TELECSA.

Como se observa en apenas dos años la corporación sufrió cambios importantes con poco tiempo de adaptación para sus colaboradores.

La unión de dos o más sociedades preexistentes, en la que una puede subordinar a la otra o pueden obtener el mismo grado de participación bajo una nueva sociedad, implicó el desarrollo e implementación de proyectos en plazos muy cortos para la adaptabilidad del personal con la nueva situación.

Este proceso de transformación, transición e integración que facilita oportunidades y avances para el crecimiento y fortalecimiento de una empresa, también trae un alto riesgo de amenazas para la misma; es así como respuestas asociadas a estas situaciones generan: caos, desorganización, cambios radicales y miedos.

La unión de dos o más culturas organizacionales podrían ser en ciertos casos contraproducentes sino son tratadas de la forma adecuada; el clima organizacional podría verse afectado si la sensibilización de la situación no fue difundida a tiempo, e

incluso podría resarcirse hasta varios años después, mientras no se logre el compromiso del personal que aun no acoge este cambio, y sigue sintiendo en peligro su estabilidad, su modo de trabajar rutinario con su horario inflexible, sin aportar un esfuerzo adicional en pro a la mejora de la situación actual.

4.2.10. Situación actual y objetivo de la discusión

En las dos fases de la auditoría interna realizada al SGSI de la CNT EP, la mayor parte de no conformidades detectadas se centran en el tema de capacitación, sensibilización, competencia y compromiso de la dirección. Se analizará los resultados de la Auditoría AI1.

De los hallazgos encontrados en febrero, el mayor porcentaje atenta contra el requisito 5.2.2 Capacitación, sensibilización y competencia, seguido en un menor pero importante porcentaje con el requisito 5.1 Compromiso de la Dirección, el restante es la sumatoria de requisitos y controles los cuales abarcan no conformidades menores y oportunidades de mejora que no afectan mayoritariamente a la recomendación de certificación por lo cual no serán objeto de nuestro estudio.

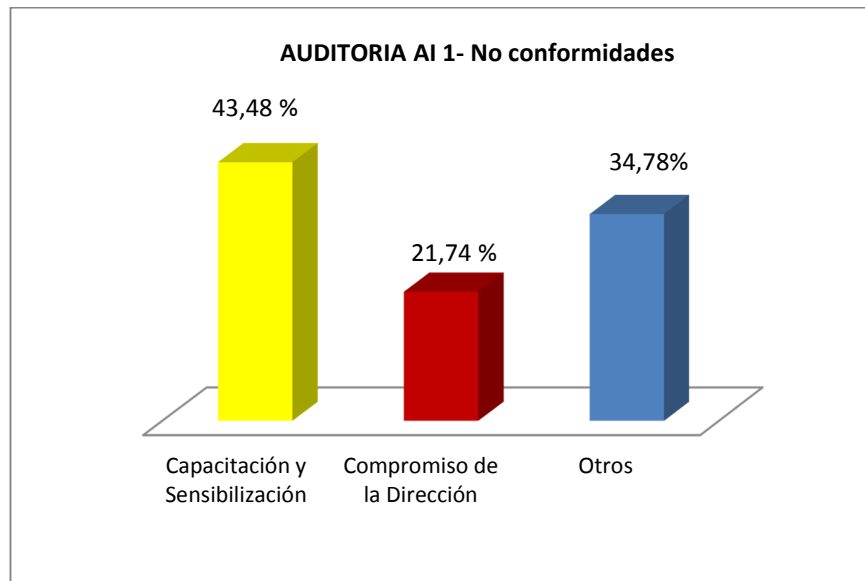


Gráfico 4. No conformidades AI1

De las variables indicadas, los puntos de preocupación son representados con las barras amarillas y rojas en el Gráfico 4., lo cual lleva a cuestionar:

- ¿por qué a pesar de haber sido cerradas observaciones encontradas con Deloitte se siguen presentando los hallazgos más importantes al cumplir con el requisito seis de la norma?; Y mas aún después de un tratamiento de seis meses para el cierre de las mismas.

En la evaluación realizada, se pudo observar que en un porcentaje del 80% los entrevistados no se encontraban comprometidos con su rol en el proceso a ser auditado. De las veinte entrevistas realizadas, se registró al menos una reflexión en el ambito personal del colaborador; la percepcion por parte del equipo auditor fue igual, los entrevistados no estaban dando la debida importancia al tema de seguridad de la

información, incluso no le daban importancia a la auditoría misma, comprometiéndola a faltas, tardanzas e incluso cancelaciones. Es decir, con un SGSI implementado hace más de un año, con una auditoría realizada para evaluar el estado situacional de la empresa, con planes de acción ejecutados y observaciones cerradas, aun la corporación no estaba conciente sobre lo que significaba tener sistema de gestión de seguridad de la información y el trabajo que conllevaba mantener el mismo.

En el momento de realizar los hallazgos con tantas observaciones sobre el tema surge una nueva pregunta: ¿Qué estaba sucediendo?, la respuesta a esta cuestión se la obtuvo en la presentación del informe de auditoría, muchos representantes de la alta dirección no asistieron en la exposición realizada en el mes de febrero.

El objetivo después de cumplir con el requisito seis era: proponer a la corporación para una evaluación externa y así obtener una certificación internacional ISO/IEC 27001:2005.

Luego de la evaluación realizada en febrero, la empresa de certificación se presentó para realizar una auditoría externa de primera fase a la corporación, la expectativa era pasar esta evaluación en la primera fase pero salieron a la luz estas falencias y la recomendación del auditor externo fue cerrar las mismas observaciones determinadas ya, en las dos últimas auditorías internas y en la de pre-certificación. El hallazgo encontrado por la empresa auditora externa fue la no recomendación para la certificación internacional.

Después de estas auditorias, el plan de acción se enfocó en su mayoría en planes de capacitación, sensibilización y concienciación. El método a ser utilizado fue el tradicional: plan de capacitaciones ejecutadas en semanas programadas a los cuales el personal debía asistir para instruirse sobre temas de seguridad de la información; lastimosamente después de la primera semana de capacitaciones y de acuerdo a la realidad como empresa no se estaba utilizando el método correcto para concienciar a los colaboradores sobre temas de seguridad, en la primera semana de capacitaciones asistieron 55 colaboradores de los 300 involucrados en este proceso.

4.2.11. Metodología

La empresa CNT EP, como fue mencionado en el capítulo 3, sección 3.1.1, presta varios servicios y cada vez innova con nuevos productos para sus clientes, esto demanda a su personal un trabajo constante con resultados inmediatos para satisfacer a sus clientes, encontrándose esta exigencia en todas las áreas de la empresa: sean las técnicas, de sistemas, de servicio al cliente, o las de operación.

Al analizar el por qué la falta de asistencia a las capacitaciones se encontró lo siguiente:

- **Falta de tiempo por parte de los colaboradores:** el trabajo bajo presión no les permite ausentarse de su puesto de trabajo por algo tan trivial como una capacitación.
- **Falta de interés sobre el tema de seguridad de la información:** el personal por desconocimiento no deseaba saber las nuevas tendencias

sobre seguridad de la información; “por qué modificar mi forma de cuidar la información si siempre he trabajado así y no ha sucedido nada?. Este tema es delicado por que implica temas como:

- El perfil del colaborador en cuanto a educación se refiere,
- Los años de prestación de servicios por temas de fusión de empresas,
- Colaboradores con resistencia al cambio.
- **Falta de colaboración de jefaturas:** el trabajo excesivo que se tiene en ciertas áreas de la empresa, los turnos rotativos, la exigencia de atención 7x24, causa que no todos los colaboradores puedan asistir a las capacitaciones impartidas. Las opciones de las jefaturas fueron: el colaborador que desea puede asistir fuera de los horarios de trabajo o solamente se limitaron a enviar uno o dos representantes del grupo de trabajo.
- **Lugar donde se realiza la capacitación:** el lugar que la empresa destina para las capacitaciones es bastante alejado de los lugares de trabajo de los colaboradores por lo que el traslado y el regreso a las oficinas es difícil, lo que genera que los colaboradores opten por no asistir.
- **Cantidad de horas de capacitación:** para muchos asistir a una capacitación de cuatro horas es bastante tedioso y mas aún si es obligatorio.

Tras haber realizado este análisis, de manera reactiva y de acuerdo a las situaciones encontradas inmediatamente se comenzó con la difusión de los temas de

seguridad de la información explotando los recursos que la empresa posee, para de esta manera intentar cerrar las novedades mencionadas, y se lo hizo así:

- **Por la falta de tiempo de los colaboradores:** En el canal de comunicación interno que llega a nivel nacional, se comenzó a difundir pequeños tips de seguridad de la información, el medio de difusión utilizado fue el correo electrónico. Cuando se comenzó con la campaña, se enviaban diariamente tips de seguridad de la información en un periodo de aproximadamente dos meses. Actualmente la campaña continua y se encuentra en el calendario de difusión que la gerencia de comunicación e imagen corporativa mantiene, ahora la difusión se realiza los martes de cada mes.
- **Falta de interés sobre el tema de seguridad de la información:** con las difusiones realizadas por el canal de comunicación interno, se generó interés incluso con los colaboradores más reacios, el hecho de revisar los tips sobre canales oficiales y masivos, causó que del grupo detectado en un 40% se inclinarán a conocer más sobre el tema.

De: [] CONTIGO CNT
Para: [] CONTIGO CNT
CC:
Asunto: TENDENCIAS 2014: PÉRDIDA DE PRIVACIDAD EN INTERNET Enviar

Seguridad de la información

Tendencias 2014: Pérdida de Privacidad en Internet





A partir de la masificación de Internet el tema de la privacidad de la información comenzó a adquirir mayor trascendencia para la comunidad en general y ya no sólo para los expertos del área de seguridad informática o las empresas.

Si bien, los problemas relacionados a la seguridad y privacidad de los datos almacenados en Internet existen a partir del momento en que esta tecnología comenzó a masificarse, lo acontecido con la NSA provocó que sea mayor la cantidad de usuarios que se preocupan por este tema. Entre las estadísticas que corroboran este aumento, es posible mencionar:

"La falta de concientización sigue siendo uno de los principales obstáculos al momento de proteger adecuadamente la información y privacidad del usuario en Internet. En una primera instancia es la propia persona quien decide cuál información publicar y qué no, por ende, también puede aumentar o disminuir el nivel de su privacidad

Imagen 32. Captura de pantalla de boletín interno Medio de Difusión CONTIGO CNT- Seguridad de la Información.

- **Falta de colaboración de jefaturas:** El hecho de poder recibir tips de información en el mismo lugar de trabajo, sin dejar de realizar las tareas diarias, facilitó a las jefaturas el inconveniente de ausentar recursos y retardar la atención requerida en el área. Para poder reforzar estos temas se comenzó a colocar material en carteleras de las diferentes areas y jefaturas sobre seguridad de la información, su politica y tips adicionales para que el colaborador al ingresar o salir de las instalaciones pueda leer y recordar lo revisado a través del canal de difusión. Tambien se crearon ayudas memoria publicadas en el Sistema de gestión documental y del cual las gerencias tenían el deber de difundir entre los colaboradores.
- **Lugar donde se realiza la capacitación:** en algunos casos fue necesario formar grupos de capacitacion dirigidos para cada área por periodos determinados, al final se determinó un nuevo sitio oficial para capacitación, el cual se centró en las instalaciones donde se encontraba el mayor número de ausentismos.
- **Cantidad de horas de capacitación:** el tiempo de capacitación fue reducido a dos horas realizandose por fases, donde se ampliaron las semanas de capacitación y la asistencia de colaboradores fue considerablemente alta.

Todo este plan de acción tardó en ejecutarse entre cuatro y cinco meses incluyendo todos los temas de gestión interna que se realiza para oficializar tanto las difusiones por medios masivos como las capacitaciones realizadas.

Para conocer si en verdad surtió efecto la gestión, se realizó una evaluación para comprobar la efectividad del plan ejecutado, esta nueva revisión volvió a demostrar que aún no se podía cerrar con éxito las observaciones de capacitación, sensibilización y concienciación. Sin embargo y con alegría se pudo decir que se habían resuelto en un 75% el tema de capacitación, sensibilización y competencia al igual que el compromiso de la dirección, pero aun seguía siendo un inconveniente que atentaría a una recomendación de no certificación. Todavía se tenía que buscar formas de concienzar sobre seguridad de la información en la corporación.

Con el apoyo de la alta gerencia y su disposición se procedió a generar una capacitación obligatoria la cual debía ser aprobada por todos los involucrados en el proceso del SGSI en un tiempo determinado.

Este curso realizado por el canal interno oficial de capacitaciones, tuvo como estrategia enviar un mail personalizado a cada colaborador para que ejecute el curso de seguridad de la información de manera obligatoria, la no ejecución de la misma sería sancionada ejecutando el reglamento interno de talento humano de la corporación.

The screenshot shows the CNT EP internal application interface. At the top, there is a navigation menu with icons for Agenda, Cursos, Biblioteca, Comunidad, Opciones, and Salir. Below the menu, the course title 'Curso : SEGURIDAD DE LA INFORMACION' is displayed. The main content area is a table titled 'Unidades' with the following data:

Tipo	Unidad	Estado	Fecha fin
Abc	Capítulo 1. Introducción a la Seguridad de la Información	terminado	24-sep-2013
Abc	Evaluación del Capítulo 1 Introduccion a la seguridad de la Información	terminado	24-sep-2013
Abc	Capítulo 2. La Seguridad de la Información no es solo tecnología	terminado	24-sep-2013
Abc	Evaluación del Capítulo 2 La Seguridad de la Información no es solo tecnología	terminado	24-sep-2013
Abc	Capítulo 3. Sistema de gestión de seguridad de la información SGSI	terminado	24-sep-2013
Abc	Evaluación del Capítulo 3 Sistema de gestión de seguridad de la información SGSI	terminado	24-sep-2013
Abc	Capítulo 4. Mejores prácticas de Seguridad de la Información	terminado	24-sep-2013
Abc	Evaluación del Capítulo 4. Mejores prácticas de Seguridad de la Información	terminado	24-sep-2013

Imagen 33. Captura de pantalla Curso: Seguridad de la Información. Aplicación interna CNT EP.

4.2.12. Evaluación de resultados.

La prueba de fuego sobre todo el trabajo realizado en los meses anteriores al cerrar las no conformidades mencionadas, fue sin duda la Auditoria de Septiembre AI2, realizando una revision de la misma se encontró:

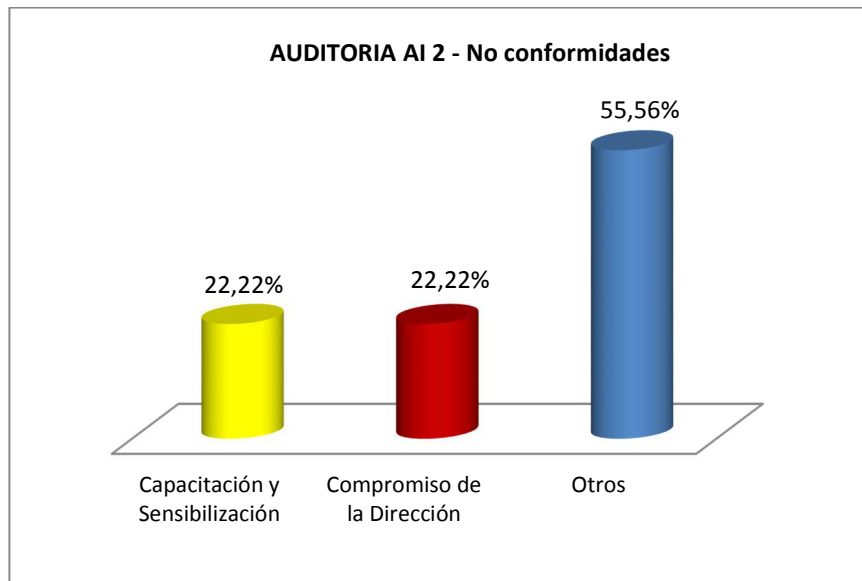


Gráfico 5. No conformidades AI2

El tema de preocupación sobre Capacitación, Sensibilización y Competencia llegó al 22% de los hallazgos encontrados y en idéntico porcentaje el tema de Compromiso de la Dirección, evidenciando que se ha reducido en más del 50% las no conformidades encontradas en febrero. Al realizar una comparación gráfica de los resultados obtenidos en la auditoría de febrero y septiembre, se puede ver con más claridad la diferencia en el cierre de no conformidades con respecto a este tema.

La gráfica indica que la incidencia que venía repitiéndose por casi un año fue superada con gran éxito al culminar la auditoría interna AI2 como cumplimiento del requisito número seis de la norma.

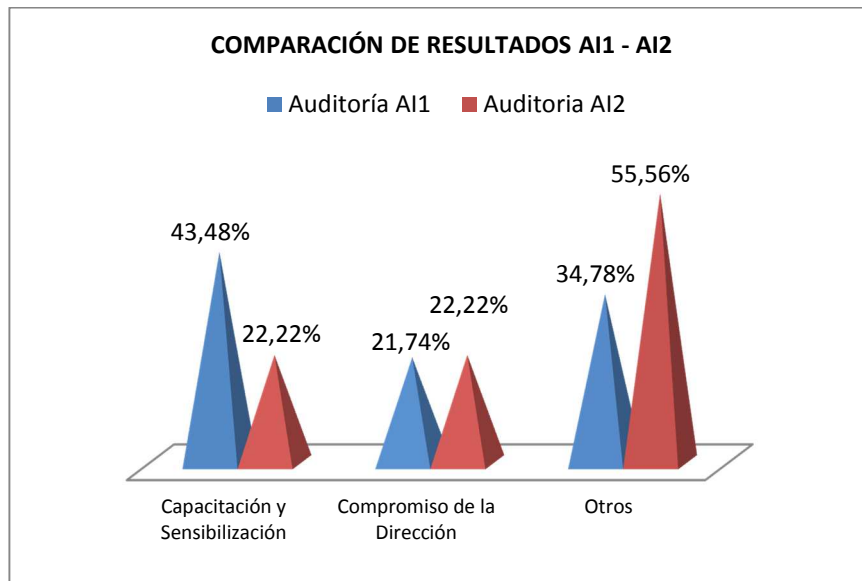


Gráfico 6. Comparación de Resultados entre la Auditoría de Febrero y la Auditoría de Septiembre.

Si bien en la segunda auditoría se registraron hallazgos con referencia a estos requisitos, fueron en menor grado y tratables para llegar a la auditoría externa realizada en la última semana del mes de septiembre.

Al someterse la corporación a la auditoría externa para obtener la certificación, corría el riesgo de que estos hallazgos sean encontrados por el auditor de certificación, tema que preocupó al grupo de seguridad de la información por lo cual para cerrar estas observaciones la corporación tuvo que trabajar arduamente en tres semanas sobre temas de capacitación y difusión de procedimientos. Por supuesto estas acciones se lograron con el apoyo de gerencia ya que los mismos por su importancia debieron ser de cumplimiento obligatorio.

4.2.13. Conclusiones y trabajos futuros

Al realizar las evaluaciones, la mayor dificultad que se encontró; fue la falta de colaboración de los empleados, los cuales no actuaban mientras no tengan una motivación que en este caso se presentó como una disposición de cumplimiento obligatorio. Es imprescindible, trabajar no solo por el objetivo de mantener un SGSI o por que las disposiciones indican o no una forma de actuar determinada. El trabajo debe centrarse en concientizar a los colaboradores del significado de crecer como empresa y prestar servicios de calidad en un tiempo oportuno.

El conocer el camino que emprende la empresa para ser líder en el mercado, implica un orden, disciplina, sacrificio, trabajo arduo e incansable, que solo se logra con el compromiso de todos los que forman parte de la organización. El camino a seguir es lograr un cambio de mentalidad donde se entienda que sin el esfuerzo de todos los colaboradores el avance y crecimiento tardará aún más, porque con el consentimiento o no de todos, el cambio vendrá.

Todos podemos crear y transmitir conciencia, como miembros de un equipo, como parte de una familia, el éxito está en prepararnos, actualizarnos e intentar caminar a la velocidad que lo hace el mundo.

CAPÍTULO 5

5. CONCLUSIONES Y RECOMENDACIONES

En referencia al punto 1.5 Objetivos Generales, se detectaron las no conformidades y oportunidades de mejora en cada una de las auditorías realizadas las cuales fueron difundidas en la empresa y tratadas en el correspondiente plan de acción posterior.

En referencia al punto 1.6 Objetivos Específicos, al realizar las auditorías internas se cumplió con cada uno de los ítems registrados apoyando directamente con la ejecución de las evaluaciones que permitieron cumplir con el requisito seis de la norma que indica que debe realizarse auditorías internas en intervalos determinados.

Tomando como referencia las auditorías realizadas en la corporación, contando la realizada por Deloitte y sobre todo en la auditoria de febrero se determinaron en mayor número no conformidades que abarcaban el tema de Capacitación, sensibilización y competencia las cuales a pesar de haber sido tratadas en el plan de acción descrito por la empresa Deloitte y en el informe de febrero, se volvieron a repetir en la auditoria de septiembre, lo cual lleva a determinar que como en muchas otras organizaciones se tiene miedo al cambio que genera buscar una mejora continua, por varias razones, siendo las principales: la resistencia a dicho cambio, el compromiso que esto implica, persistencia y disciplina que se requiere para la mejora continua y la exigencia de una capacitación permanente.

Al aplicar una táctica diferente en la manera de difundir los conceptos clave sobre seguridad de la información, se generó una clara mejora en los cierres de observaciones sobre el tema de capacitación y compromiso de la dirección, concluyendo que los métodos sugeridos sobre aplicaciones de planes de acción deben variar de acuerdo a la naturaleza de la organización, su situación actual, y las exigencias que requiere para mantenerse en el mercado junto con el estudio previo de su nacimiento como empresa.

A lo largo de este proyecto se pudo determinar que el haber implementado un Sistema de gestión de seguridad de la información en la empresa y su posterior revisión, ha implicado un forzoso cambio de cultura organizacional para obtener el éxito final. Este cambio modificó la forma de trabajar de la empresa, haciéndolo pensar en la mejora continua tras la búsqueda de la calidad de todas las actividades que realizan, siendo conscientes que mejorar no implica solamente tratar de hacer mejor lo que se ha venido haciendo, sino que es necesario mejorar de manera continua aplicando sus conocimientos, creatividad e innovación.

Con lo mencionado en el punto anterior se puede evidenciar la fortaleza de CNT al efectivizar las recomendaciones en un promedio del 80%; en un tiempo que permitió a la empresa, cerrar observaciones importantes, lo cual contribuyó que la Corporación Nacional de Telecomunicaciones adquiriera la certificación internacional bajo la norma ISO/IEC 27001:2005:2005, convirtiéndola en la primera empresa estatal

de telecomunicaciones con Certificación internacional sobre la seguridad de su información.

Como recomendaciones para la empresa, se indica que no es posible eliminar los riesgos de seguridad de la información pero sí podemos reducir su probabilidad de ocurrencia mediante la incorporación en nuestro actuar de prácticas seguras para el uso responsable de los recursos de información de la CNT EP.

Es fundamental tomar en cuenta que para la implementación de un Sistema de Gestión de la Seguridad de la Información basado en ISO/IEC 27001:2005, los requisitos impuestos por dicha norma deben ser implementados al 100%, y, uno de estos requisitos es tener una metodología de evaluación de riesgos, de modo que, la seguridad de la información sin una evaluación de riesgos, es incompleta, disfuncional y muy probablemente no tenga los resultados deseados por la dirección. En vista de lo anterior, una de las diferencias fundamentales entre un equipo de “seguridad informática” y un equipo de “seguridad de la información” es la habilidad y experiencia para aplicar una metodología válida para evaluar los riesgos de seguridad de la información. La recomendación es que el Oficial de Seguridad de la Información debe conocer e impulsar el uso de una metodología de evaluación de riesgos en la organización.

Contar con personal especializado en la familia de normas 27000 permitirá a la organización incursionar, implantar y adoptar éstas normas, en este punto es

importante reconocer que uno de los pilares lo constituye el personal por lo cual mejorar la cultura organizacional sin duda permitirá conseguir dicho objetivo empresarial. La recomendación es que, la organización debe monitorear su evolución en materia de seguridad de la información, así como su evolución en gestión de riesgos, además de comprometer al personal para que participe activamente.

Cada vez existen más riesgos de seguridad y con impacto mayor, por lo que se debe estar atento a las nuevas tendencias, siendo alternativos con la manera de proceder y responder con prudencia a los sucesos repentinos que puedan dañar los activos. La seguridad de la información de la corporación la hacen todos, comenzando por la gerencia, y sus niveles. Es importante que se recuerde que la cadena de la seguridad de la información se rompe por medio del eslabón más débil.

El personal debe estar atento a las iniciativas de seguridad que en el corto plazo tendrán lugar en la corporación, la participación de todos lo que conforman la organización será fundamental.

BIBLIOGRAFÍA

(s.f.).

27001:2005, E. I. (15 de 10 de 2005). Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requerimientos. España.

CNT EP. (2012). Inventario de activos de información. Quito, Pichincha, Ecuador.

CNT EP. (2012). Mapa de procesos telecomunicaciones-Confidencial. Quito, Pichincha, Ecuador.

CNT EP. (2012). Normativa de auditores internos del SGSI. Quito, Pichincha, Ecuador.

CNT EP. (2012). Procedimiento de Acciones correctivas y Acciones preventivas. Quito, Pichincha, Ecuador.

CNT EP. (2013). Informe Auditoría Interna Septiembre 2013. Quito, Pichincha, Ecuador.

CNT EP. (2013). Plan de Auditoria Interna. Quito, Pichincha, Ecuador.

CNT EP. (01 de 02 de 2012). Alineación Estratégica del SGSI. *Alineación Estratégica del SGSI*. Quito, Pichincha, Ecuador.

CNT EP. (2012). Declaración de aplicabilidad. Quito, Pichincha, Ecuador.

CNT EP. (2012). Informe de aceptación del riesgo residual. Quito, Pichincha, Ecuador.

CNT EP. (2012). Informe de Auditoría Deloitte. Quito, Pichincha, Ecuador.

CNT EP. (2012). Informe de tratamiento de riesgos. Quito, Pichincha, Ecuador.

CNT EP. (2012). Metodología de Evaluación de Riesgos. Quito, Pichincha, Ecuador.

CNT EP. (01 de 02 de 2012). Objetivos del SGSI. Quito, Pichincha, Ecuador.

CNT EP. (2012). Planeación Estratégica. Quito, Pichincha, Ecuador.

CNT EP. (01 de 2013). Informe Auditoría Interna Enero 2013. Quito, Pichincha, Ecuador.

CNT EP. (2013). Normativa para auditorias internas al SGSI. Quito, Pichincha, Ecuador.

CNT EP. (2013). Procedimiento de auditorias internas. Quito, Pichincha, Ecuador.

- Corletti. (s.f.). *www.revista-ays.com/Normas/*. Obtenido de *www.revista-ays.com*:
<http://www.revista-ays.com/DocsNum22/Normas/Corletti.pdf>
- Corporación Nacional de Telecomunicaciones CNT EP. (2013). *Página Pública*. Recuperado el 01 de 07 de 2013, de <http://www.cnt.com.ec/>
- Deloitte. (2012). Informe TMT Predicciones 2012 de Deloitte. Quito, Pichincha, Ecuador.
- EY. (s.f.). *www.ey.com/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras*. Obtenido de *www.ey.com*:
[http://www.ey.com/Publication/vwLUAssets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/\\$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf](http://www.ey.com/Publication/vwLUAssets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf)
- ISO, C. (2012). *www.iso27001certificates.com*. Obtenido de *www.iso27001certificates.com*: <http://www.iso27001certificates.com/>
- ITGLOBAL. (2011). *ITGLOBAL_SGSI*. Recuperado el 2013, de Seguridad de la información: <http://www.itglobal.es/sgsi.php>
- Legal, I. (2013). Informática Legal imagen. <http://www.informaticalegal.com.ar>. Obtenido de <http://www.informaticalegal.com.ar>
- Maquiavelo, N. (1513). *Philosophia/Maquiavelo*. Obtenido de Philosophia:
<http://www.philosophia.cl/biblioteca/Maquiavelo/El%20pr%EDncipe.pdf>
- S.A., S. d. (2012). Curso de Formación de Auditor Líder ISO/IEC 27001:2005:2005. *Curso de Formación de Auditor Líder ISO/IEC 27001:2005:2005*.
- SGS. (2012). Curso de formación para Auditor/Auditor jefe SGS ISO/IEC 27001, 2012.
- SN. (03 de 2009). *seguridad-de-la-informacion/sgsi-virtuales.html*. Obtenido de *seguridad-de-la-informacion.blogspot.com*: <http://seguridad-de-la-informacion.blogspot.com/2009/03/sgsi-virtuales.html>
- SN. (2010). *blog.iso27001standard.com/auditoria-interna/*. Obtenido de *blog.iso27001standard.com*: <http://blog.iso27001standard.com/es/tag/auditoria-interna/>
- SN. (21 de 07 de 2012). *blog.iso27001standard.com/cuatro-beneficios-clave-de-la-implementacion-de-la-norma-iso-27001*. Obtenido de *blog.iso27001standard.com*:
<http://blog.iso27001standard.com/es/2010/07/21/cuatro-beneficios-clave-de-la-implementacion-de-la-norma-iso-27001/>

sociedaddelainformacion.wordpress.com/Auditoría interna de un SGSI. (2006). Obtenido de sociedaddelainformacion.wordpress:
<http://sociedaddelainformacion.wordpress.com/2006/11/12/auditoria-interna-de-un-sgsi-iso-27001/>

Telconet. (2013). *Telconet la fibra del ecuador*. Recuperado el 01 de 06 de 2013, de Telconet: <http://www.telconet.net/>

TELEFÓNICA. (2013). *Telefónica*. Recuperado el 02 de 06 de 2013, de <http://www.telefonica.com.ec/>