

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



Facultad de Ingeniería en Electricidad y Computación

**“IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD EN
CONFORMIDAD CON LA NORMA ISO 27002 PARA EL ÁREA
DE SIS GSI BILLING PARA UNA EMPRESA DE
TELECOMUNICACIONES”**

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

JOSÉ MIGUEL CHICA DURÁN

GUAYAQUIL – ECUADOR

AÑO

2.018

AGRADECIMIENTO

Principalmente agradezco a Dios por la salud recibida, por tener la familia, y amigos que tengo, por sus bendiciones diarias.

A mis padres, por el apoyo constante, por el cafecito de la media noche, por su constante respaldo, gracias totales.

A mi hija, que con su amor supo darme ánimos para seguir adelante en este proyecto.

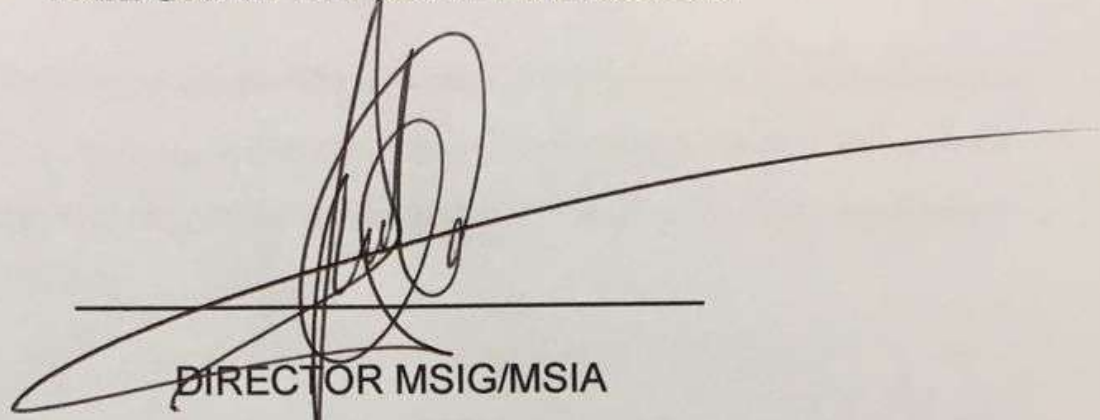
A mis maestros, quienes se esforzaron para compartir sus conocimientos y experiencias, enriqueciendo así mi parte profesional y humana.

A mis amigos, que estuvieron pendientes que se concluya este trabajo, por dedicarme sus consejos y tiempo.

DEDICATORIA

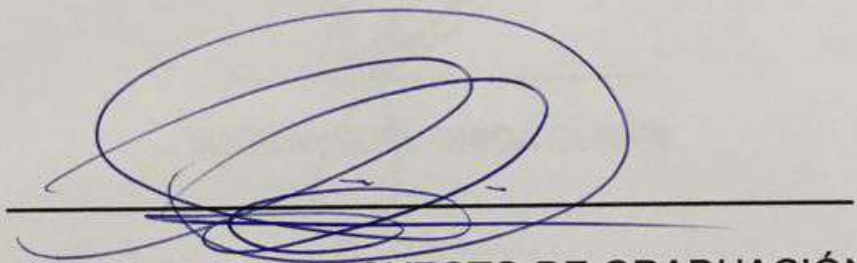
Dedicado especialmente a mis padres, sin ellos nada de esto hubiera sido posible, a mi hija y mi tutor que con paciencia logramos terminar este proyecto.

TRIBUNAL DE SUSTENTACIÓN



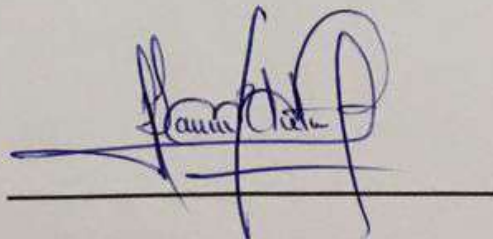
DIRECTOR MSIG/MSIA

ING. LENÍN FREIRE



DIRECTOR DEL PROYECTO DE GRADUACIÓN

ING. FABIÁN BARBOZA

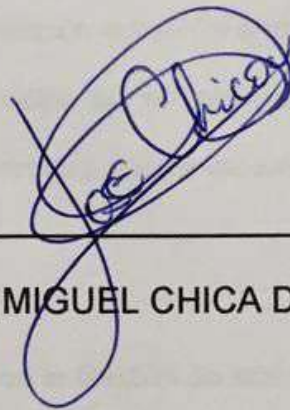


MIEMBRO DEL TRIBUNAL

ING. LAURA URETA

DECLARACIÓN EXPRESA

"Declaro de forma expresa que todo el contenido de esta Tesis de Grado es de mi completa autoría y responsabilidad, por lo que doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"



JOSÉ MIGUEL CHICA DURÁN

RESUMEN

El presente trabajo busca solucionar los problemas de seguridad informática encontrados en el área de GSI Billing, aplicando un esquema de seguridad ISO 27002:2005; con este análisis se pretende minimizar los riesgos de posibles amenazas a la información.

Se realizó un profundo análisis a la situación actual del área y se encontraron falencias en cuanto al manejo de la seguridad de la información, por tal motivo se trabajó en implementar un esquema de seguridad que permita reducir, controlar y mitigar las amenazas.

Se aplicaron políticas relacionadas con la Gestión de activos, Gestión de Accesos y Gestión de incidentes, estas políticas fueron levantadas con el apoyo del Jefe del área, así como el personal involucrado en cada proceso.

A más de establecer los controles que ayuden a mejorar la confidencialidad, integridad y disponibilidad de la información, se propuso presentar un front end que ayudará a que la revisión de estos controles sea vista de una manera más oportuna y directa; anteriormente la revisión de estos controles era analizada a través de queries directamente en la Base de Datos.

ÍNDICE GENERAL

DEDICATORIA.....	iii
DECLARACIÓN EXPRESA	v
ÍNDICE GENERAL.....	vii
ÍNDICE DE FIGURAS	xii
ÍNDICE DE TABLAS	xiv
ABREVIATURAS Y SIMBOLOGÍA	xv
INTRODUCCIÓN	xvi
CAPÍTULO 1	1
INFORMACIÓN GENERAL.....	1
1.1 ANTECEDENTES DE LA INVESTIGACIÓN	1
1.2 SOLUCIÓN PROPUESTA.....	6
1.3 OBJETIVO GENERAL.....	9
1.4 OBJETIVOS ESPECÍFICOS	9
1.5 ALCANCE	10
1.6 METODOLOGÍA.....	10
CAPÍTULO 2	11
MARCO TEÓRICO	11
2.1 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA.....	11
2.2 INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN.....	14

2.3 OBJETIVOS DE LA SEGURIDAD INFORMÁTICA	15
2.3.1 INTEGRIDAD	15
2.3.2 CONFIDENCIALIDAD	15
2.3.3 DISPONIBILIDAD	16
2.3.4 NO REPUDIO	16
2.4 CONCEPTO DE INFORMACIÓN.....	16
2.5 AMENAZAS A LA SEGURIDAD DE LA INFORMACIÓN	18
2.6 DELITOS INFORMÁTICOS	28
2.6.1 TIPOS DE DELITOS INFORMÁTICOS	28
2.6.2 CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS.....	29
2.6.3 ADMINISTRACIÓN DE LA SEGURIDAD INFORMÁTICA.....	30
2.6.4 NORMA ISO 27001.....	31
2.6.5 ANÁLISIS Y EVALUACIÓN DE RIESGOS.....	38
2.6.6 IMPLEMENTACIÓN DE CONTROLES	41
2.6.7 DEFINICIÓN PARA EL TRATAMIENTO DE RIESGOS.....	41
2.6.8 NORMA ISO 27002.....	46
2.6.9 POLÍTICA DE SEGURIDAD	47
2.6.10 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN....	48
2.6.11 GESTIÓN DE ACTIVOS	49
2.6.12 SEGURIDAD HACIA EL RECURSO HUMANO	50
2.6.13 SEGURIDAD FÍSICA Y AMBIENTAL	51
2.6.14 GESTIÓN DE COMUNICACIONES Y OPERACIONES	52
2.6.15 CONTROL DE ACCESO	52
2.6.16 GESTIÓN DE INCIDENTES	53
2.6.17 GESTIÓN DE CONTINUIDAD DE NEGOCIO.....	54

2.6.18 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	56
2.6.19 CUMPLIMIENTO LEGAL	57
2.7 ANÁLISIS DE RIESGO UTILIZANDO LA METODOLOGÍA MAGERIT	58
CAPÍTULO 3	72
ANÁLISIS DE LA SITUACIÓN ACTUAL.....	72
3.1 METODOLOGÍA.....	73
3.2 TIPOS DE INVESTIGACIÓN.....	74
3.3 ESTRUCTURA ORGANIZACIONAL	75
3.4 ANÁLISIS FODA DEL ÁREA DE SIS GSI BILLING.....	76
3.5 RECOLECCIÓN DE DATOS.....	76
3.5.1 DESCRIPCIÓN de las principales funciones del área de SIS GSI Billing.....	77
3.6 ÁREAS PRINCIPALES DENTRO DE SIS GSI BILLING	79
3.6.1 BILLING FIJO.....	79
3.6.2 CONFIGURACIÓN DE PRODUCTOS Y OFERTAS COMERCIALES. (RATING Y CONFIGURACIÓN)	80
3.6.3 FACTURACIÓN	84
3.6.4 FACTURACIÓN EN LÍNEA (PREPAGO)	84
3.6.5 FACTURACIÓN BASADA EN SERVICIOS CONTRATADOS (POSTPAGO) – SECTOR MASIVO	85
3.6.6 FACTURACIÓN BASADA EN SERVICIOS CONTRATADOS (POSTPAGO) – SECTOR CORPORATIVO.....	86
3.6.7 CRONOGRAMA DE FACTURACIÓN	88
3.6.8 PROCEDIMIENTOS ALMACENADOS EN UNIX PARA FACTURACIÓN.....	89
3.6.9 MEDIACIÓN E INTERCONEXIÓN	90

3.7 VISIÓN DEL ÁREA DE SIS GSI BILLING.....	90
3.8 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN.	90
3.9 VALORACIÓN DE LOS ACTIVOS	93
3.10 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES.....	95
3.11 PLAN DE IMPLEMENTACIÓN.....	99
CAPÍTULO 4.	101
IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD BASADO EN LA NORMA ISO 27002	101
4.1 GESTIÓN DE ACTIVOS.....	102
4.2 CONTROL DE ACCESO.....	114
4.3 GESTIÓN DE INCIDENTES.....	122
CAPÍTULO 5.	130
DESARROLLO DEL ESQUEMA DE SEGURIDAD PROPUESTO	130
5.1 CONTROL DE ACCESO	134
5.2 GESTIÓN DE ARCHIVOS.....	136
5.3 GESTIÓN DE CAMBIOS	137
CAPÍTULO 6	141
ANÁLISIS DEL ESQUEMA DE SEGURIDAD PROPUESTO.....	141
6.1 CREACIÓN DE UN PLAN COMERCIAL (DISPARADORES).....	144
6.1.1 ROLES QUE INTERVIENEN EN EL PROCESO	147
6.2 CARGA DE CRÉDITO O DÉBITO (NO REPUDIO).....	150
6.2.1 ROLES QUE INTERVIENEN EN EL PROCESO	152

CONCLUSIONES Y RECOMENDACIONES.....	156
BIBLIOGRAFÍA	160
ANEXOS	164
ANEXO 1 SOA 27001	164

ÍNDICE DE FIGURAS

FIGURA 2.1 TIPOS DE SEGURIDAD INFORMÁTICA FUENTE: UNIVERSIDAD DE VALENCIA	13
FIGURA 2.2 EVOLUCIÓN INCIDENTES DE SEGURIDAD FUENTE: [6] SARA BURSZTEIN • 19/12/2016	23
FIGURA 2.3 EVOLUCIÓN INCIDENTE DE SEGURIDAD DEL 2014 AL 2015 FUENTE: [6] SARA BURSZTEIN • 19/12/2016.....	24
FIGURA 2.4 EVOLUTIVO DE CERTIFICACIONES ISO 27001 POR AÑO FUENTE: AUTOR... 33	
FIGURA 2.5 TOP PAÍSES CERTIFICADOS EN ISO 27001:2005 FUENTE: AUTOR.....	34
FIGURA 2.6 MODELO PDCA FUENTE: AUTOR.....	35
FIGURA 2.7 CÁLCULO RIESGO INHERENTE FUENTE: AUTOR	40
FIGURA 2.8 CÁLCULO DE RIESGO RESIDUAL FUENTE: AUTOR	40
FIGURA 2.9 FORMAS DE TRATAR EL RIESGO FUENTE: AUTOR.....	42
FIGURA 2.10 GESTIÓN DE RIESGO DE ACUERDO A LA NORMA ISO 31000 FUENTE: MAGERIT	59
FIGURA 2.11 GESTIÓN DE RIESGO FUENTE: MAGERIT	63
FIGURA 2.12 ELEMENTOS DE UN ANÁLISIS DE RIESGOS. FUENTE: MAGERIT	65
FIGURA 3.13 GRÁFICO SOBRE LOS SERVICIOS OFERTADOS FUENTE: AUTOR.....	72
FIGURA 3.14 GRÁFICO SOBRE LOS CICLOS DE FACTURACIÓN FUENTE: AUTOR	72
FIGURA 3.15 ESTRUCTURA ORGANIZACIONAL FUENTE: AUTOR	75
FIGURA 3.16 ANÁLISIS FODA FUENTE: AUTOR	76
FIGURA 3.17 DOCUMENTO DE LA CREACIÓN O ACTUALIZACIÓN DEL PLAN CELULAR FUENTE: AUTOR	81

FIGURA 3.18 MÓDULO PARA LA CREACIÓN DE PLANES POSTPAGO FUENTE: AUTOR ..	82
FIGURA 3.19 DOCUMENTO DE CONFIGURACIÓN PARA LA FACTURACIÓN EN LÍNEA FUENTE: AUTOR	83
FIGURA 3.20 CRONOGRAMA DE FACTURACIÓN FUENTE: AUTOR.....	88
FIGURA 3.21 EJEMPLO DE PROCEDIMIENTOS ALMACENADOS FUENTE: AUTOR.....	89
FIGURA 3.22 ACTIVOS PARA EL ÁREA DE GSI BILLING FUENTE: AUTOR.	92
FIGURA 3.23 CRONOGRAMA PARA LA PUESTA EN PRODUCCIÓN DEL ESQUEMA DE SEGURIDAD ISO 27002 FUENTE: AUTOR	100
FIGURA 4.24 GRÁFICA PARA LA CREACIÓN DE USUARIOS EN WINDOWS. FUENTE: AUTOR.....	116
FIGURA 4.25 DIRECTIVA DE CONTRASEÑAS. FUENTE: AUTOR.....	117
FIGURA 5.26 INGRESO AL SISTEMA GSI BILLING FUENTE: AUTOR	131
FIGURA 5.27 MENÚ DE OPCIONES DEL SISTEMA GSI BILLING FUENTE: AUTOR	133
FIGURA 5.28 FRONT END SISTEMA GSI BILLING FUENTE: AUTOR	134
FIGURA 5.29 CONTROL DE ACCESO DE USUARIOS FUENTE: AUTOR	135
FIGURA 5.30 DETALLE DE REGISTRO DE UN USUARIO FUENTE: AUTOR.....	135
FIGURA 5.31 GESTIÓN DE ARCHIVOS GSI BILLING FUENTE: AUTOR	136
FIGURA 5.32 ASIGNACIÓN EQUIPO GSI BILLING FUENTE: AUTOR.....	139
FIGURA 5.33 CRITERIOS DE CONSULTA FUENTE: AUTOR	140
FIGURA 5.34 TABLAS MÁS CONSULTADAS POR USUARIO FUENTE: AUTO.....	140
FIGURA 5.35 SITUACIÓN INICIAL SIS BILLING FUENTE: AUTOR	143

ÍNDICE DE TABLAS

TABLA 1 INCIDENTES DE SEGURIDAD POR AÑO.....	22
TABLA 2 CERTIFICACIONES POR AÑO EN NORMA ISO 27001	33
TABLA 3 EVALUACIÓN DE RIESGO	39
TABLA 4 CONTROLES DE LA NORMA ISO 27002:2005	46
TABLA 5 CRITERIO DE VALORACIÓN CON RESPECTO A SU CONFIDENCIALIDAD	70
TABLA 6 CRITERIO DE VALORACIÓN CON RESPECTO A SU INTEGRIDAD	71
TABLA 7 CRITERIO DE VALORACIÓN CON RESPECTO A SU DISPONIBILIDAD	71
TABLA 8 DETALLE DE ACTIVOS UTILIZADOS EN EL PROCESO DE FACTURACIÓN.....	91
TABLA 9 VALORACIÓN DE ACTIVOS.....	93
TABLA 10 CLASIFICACIÓN RIESGO VS AMENAZAS	96
TABLA 11 RESUMEN DE LA CLASIFICACIÓN RIESGO VS AMENAZAS.....	97
TABLA 12 CALIFICACIÓN DE ACTIVOS Y SUS RIESGOS.....	97
TABLA 13 CLASIFICACIÓN DE LA INFORMACIÓN DE ACUERDO AL CONFIDENCIALIDAD	107
TABLA 14 CLASIFICACIÓN DE LA INFORMACIÓN DE ACUERDO A LA DISPONIBILIDAD.	108
TABLA 15 CLASIFICACIÓN DE LA INFORMACIÓN DE ACUERDO A LA INTEGRIDAD.....	109
TABLA 16 ETIQUETADO Y MANEJO DE LA INFORMACIÓN.....	113
TABLA 17 CONTROLES APLICADOS PARA LOS CASOS DE ESTUDIO.....	149
TABLA 18 CONTROLES APLICADOS PARA CARGA DE CRÉDITO O DÉBITO.....	154

ABREVIATURAS Y SIMBOLOGÍA

E.T.	Empresa de Telecomunicaciones
F.B.I.	Buró Federal de Investigaciones
PWC.	Servicios de auditoría y asesoramiento, consultoría y fiscalidad por sus siglas en inglés (Audit and assurance, consulting and tax services)
FBI	Federal Bureau of Investigation
SGSI.	Sistema de gestión de la seguridad de la información
SEC.	Sección
TH.	Talento Humano

INTRODUCCIÓN

El presente trabajo fue realizado en base a la norma ISO 27002:2005, realizando un profundo análisis a los procesos que maneja el área de Facturación para una empresa de telecomunicaciones.

En el primer capítulo se trata acerca de la situación inicial de la empresa, en base a la observación de sus procesos se encontraron debilidades a nivel de la seguridad informática, en ella se pudo constatar problemas a nivel de ingresos del personal de apoyo, problemas de acceso a los sistemas de información, problemas para realizar auditorías en los cambios realizados a nivel de producción.

En el segundo capítulo se detallan conceptos acerca de la seguridad de información, brevemente se toca el tema de la norma ISO 27001:2005, ISO 27002:2005 y la metodología Magerit que sirvió para realizar la investigación de los riesgos y como se deben tratar para minimizar las posibles afectaciones que puede tener la información de la organización.

En el tercer capítulo se aborda al detalle la composición del área de facturación, realizando un análisis FODA, así como especificando en resumen las tareas asignadas por grupos, que son: Facturación de productos Fijos y móviles, Configuración de ofertas comerciales, Mediación e interconexión, así como también la misión y visión del área de Facturación.

Se realizó una valoración de los activos que se utilizan en estos procesos, esto gracias a la ayuda de la Jefatura, se pudo evaluar la importancia de la información realizando una calificación en orden ascendente de los mismos.

En el capítulo cuatro se mencionan los controles aplicados en este trabajo, esto gracias al análisis realizado en los procesos del área, el esquema propuesto consideró los siguientes controles: Gestión de Activos, Gestión de Accesos y Gestión de incidentes.

En este capítulo se levantó un listado de controles que deben ser aplicados con el fin de reducir los problemas encontrados en el análisis inicial, esto mejorará a garantizar la confidencialidad, integridad y disponibilidad de la información.

En el capítulo cinco, se presentó un front end que ayudará a automatizar algunos procesos que eran llevados a mano, así como ayudara en el control y seguimiento de las tareas que realiza el personal de apoyo, reduciendo el No repudio en sus actividades.

Permitirá realizar una mejor auditoría en los cambios realizados a las tablas de producción, así como también un seguimiento en línea de las actividades que realiza cada ingeniero.

Finalmente, en el capítulo seis, se mencionan dos casos en los que se encontraron problemas de seguridad informática, en base a ello se presentaron los respectivos controles a ser aplicados para mitigar dichos problemas.

CAPÍTULO 1

INFORMACIÓN GENERAL

1.1 ANTECEDENTES DE LA INVESTIGACIÓN

XYZ, Empresa de Telecomunicaciones líder en el mercado ecuatoriano ofrece tecnología de punta, calidad y calidez en la atención de las necesidades de los clientes. Siendo una empresa joven, busca contar con los más altos estándares de servicio, garantizando a nuestros clientes el compromiso de mantenerlos comunicados dentro o fuera del Ecuador. Actualmente cubre el 96% del territorio Nacional, ofreciendo productos a nivel de telefonía fija y móvil con la más avanzada tecnología.

Para XYZ, la preferencia de los clientes hacia sus servicios los mantiene en un constante reto para buscar la excelencia, retornándoles servicios innovadores deseando cubrir sus necesidades y garantiza la privacidad de las comunicaciones, ya que es la razón de ser de la industria. La responsabilidad de preservar la privacidad no sólo se centra en comunicaciones de voz sino también en la comunicación de datos, los datos o información que son transmitidos por nuestra red. En la Ley Orgánica de Telecomunicaciones [1], capítulo II numeral 13, menciona que se debe "Garantizar el secreto e inviolabilidad de las comunicaciones cursadas a través de las redes y servicios de telecomunicaciones, sin perjuicio de las excepciones establecidas en las leyes."

La empresa cuenta con un manual de procedimiento en base a la norma ISO-27001, en la que se reflejan las buenas prácticas sobre la seguridad de la información, pero debido a la vertiginosidad con la que se desenvuelve el negocio, muchas prácticas se pierden, quedan obsoletas o son excluidas. Todo lo antes mencionado deja en evidencia debilidades en los sistemas actualmente utilizados en el área y la poca difusión que debe existir sobre la aplicación de seguridades sobre la información sensible de la empresa.

DESCRIPCIÓN DEL PROBLEMA

En la actualidad uno de los principales riesgos para las empresas es la fuga de información, así como también el acceso no autorizado a sus instalaciones, que puede ocasionar la interrupción en sus operaciones por daño en sus sistemas, alteración en su información, etc.

Para el análisis de este estudio, se observaron durante 2 meses las actividades que giraban en torno al departamento de Facturación (SIS GSI Billing) de la empresa de Telecomunicaciones XYZ; de esta observación se determinaron muchas debilidades en la seguridad tanto física como lógica.

Entre estas debilidades y posibles riesgos que preocupan al área de Facturación se detallan:

- Ingreso no autorizado del personal de apoyo.
- Acceso al sistema de Facturación por personal de apoyo.
- Fuga de información.
- Posibles errores operativos por desconocimiento de los procesos.
- Interrupción de procesos por mala manipulación de las bases de datos.

- Eliminación de archivos sensibles que se encuentran en las estaciones de trabajo.
- Dificultad para realizar auditorías en los cambios que se realizan en el sistema.
- Daño en la reputación y buen nombre de la empresa por errores operativos.

Estos potenciales riesgos pueden violentar la confidencialidad, integridad y disponibilidad de la información, ocasionando un incidente grave en el sistema de información, de tal forma que pueden perjudicar económicamente a la empresa y así su prestigio como marca.

Para reducir estos riesgos, se ha decidido generar normas internas que ayuden a regular los procesos y el correcto manejo de la información.

Debido a que la empresa de Telecomunicaciones sigue los lineamientos de la norma ISO 27001:2005; a la seguridad del área de Facturación se la reforzará con las buenas prácticas y controles de la norma ISO 27002:2005.

Es importante que se tenga en consideración que las amenazas a las que se ve expuesta una organización pueden ser:

Amenazas externas: que son generadas fuera del entorno de red.

Amenazas internas: pueden ser generadas por colaboradores de la empresa por desconocimiento (sin intención), con conocimiento (intencionales). Realizando un breve análisis se ha detectado posibles vulnerabilidades que pueden afectar la seguridad de la información, se detectó lo siguiente:

Confidencialidad:

- Las sesiones del personal interno son usadas por el personal a cargo, sean estos internos o de apoyo.
- No existe controles de registro del personal de apoyo al momento de cubrir su turno.
- El área cuenta con una herramienta de código abierto para gestionar las contraseñas de los aplicativos; la contraseña de la esta herramienta no ha sido cambiada desde la instalación.

Integridad:

- Se utilizan cuentas de súper usuarios para realizar modificación de data sensible a nivel de base de datos; aún existen tablas que no cuentan con una tabla de auditoría.

Disponibilidad:

- Se utilizan estaciones de trabajo como servidores de archivos.
- No existen procesos que respalden de manera cíclica los archivos con código fuente (Shells) en los servidores.

No repudio:

- No existe un proceso para auditar la gestión en línea de los ingenieros.
- No existe una bitácora de cambios realizados en los programas actualizados.

1.2 SOLUCIÓN PROPUESTA

De acuerdo al análisis planteado y las vulnerabilidades encontradas en los procesos de control y manejo de la información dentro del área de Facturación, se plantean los siguientes puntos de mejora a ser implementados:

Confidencialidad:

- Elaborar, implementar y difundir un esquema que permita definir una política de seguridad a la información, recursos tecnológicos y humanos tanto interno como externo.
- Aplicar el estándar Internacional ISO 27002 con las mejores prácticas en los dominios a nivel de organización, Gestión de Activos, Control de acceso, Gestión de incidentes en la seguridad de la información, Gestión en la Continuidad del negocio. La norma 27002 ayudará a mejorar la seguridad de la información, permitirá conocer posibles vulnerabilidades de los activos, análisis y tratamiento de riesgos.

Integridad:

- Restringir el acceso al código fuente para evitar robos, alteraciones o aplicación de ingeniería inversa por parte de personal no autorizado, con el fin de evitar cualquier daño al código fuente.

Disponibilidad:

- Realizar semanalmente respaldo de archivos (código fuente), con el fin de garantizar que el proceso continúe en caso de algún sabotaje al archivo principal.
- Una vez realizado el respaldo de la información, se tendrá que realizar una prueba en pre producción para garantizar que la versión de los archivos sea la correcta.
- Llevar a cabo un sistema de control de cambios, es decir construir bitácoras (disparadores a nivel de Base de datos) que almacene hora, usuario, y el cambio realizado con el fin de realizar la auditoría necesaria

No repudio:

- Identificar los riesgos relacionados a personal externo que tiene acceso a la base de datos y servidores.

Los Beneficios que se esperan alcanzar son:

- Mayor control en el personal de apoyo al momento de cubrir el turno.
- Garantizar una adecuada segregación de funciones, a través de la implementación de controles de accesos.
- Mayor control en las tablas de producción, se podrá tener una auditoría al día sobre los cambios realizados.

- Se tendrá mayor conocimiento sobre los cambios realizados en Shells a ser ejecutados.
- Se tendrá mayor conocimiento sobre las rutas de respaldo de archivos sensibles.
- Se podrá controlar el acceso a los aplicativos de una forma segura, utilizando el gestor de contraseñas aplicando una normativa de cambio de clave cada 3 meses.
- Se podrá reducir la posible fuga de información.

1.3 OBJETIVO GENERAL

Analizar e implementar un Esquema de Seguridad en Conformidad con la Norma ISO 27002 destinado para la Empresa de Telecomunicaciones XYZ, enfocado a su área de facturación (SIS GSI Billing).

1.4 OBJETIVOS ESPECÍFICOS

A. Diseñar un esquema de seguridad informática, en base a los controles de la norma ISO 27002, con el fin de implementar políticas necesarias para asegurar la información.

- B. Analizar y desarrollar los componentes para la autenticación, conexión a la base de datos y servidores, generar una bitácora para llevar control de cambios hacia la base de datos.
- C. Implementar y difundir la política y procedimientos basados en la norma ISO 27002.

1.5 ALCANCE

Se ha definido como alcance de este estudio el análisis e implementación de controles a nivel de la gestión de activos, control de acceso y gestión de incidentes; conforme a la norma ISO 27002:2005.

De tal forma que el área de SIS GSI Billing podrá contar con una guía de buenas prácticas que deberán ser consideradas para un mejor control en el acceso a los aplicativos, acceso a las estaciones de trabajo.

Priorizando los pilares de la seguridad de la información que son: confidencialidad, integridad, disponibilidad y no repudio.

1.6 METODOLOGÍA

La metodología que se aplicará en este trabajo será Descriptivo - Analítico, es decir, se describirán situaciones y eventos para evidenciar la realidad del área y sus procesos [2].

CAPÍTULO 2

MARCO TEÓRICO

2.1 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA.

Seguridad informática o también conocida como Ciberseguridad, es un conjunto de normas, herramientas, métodos de gestión de riesgos y mejora continua en procesos de seguridad informática, que se encarga de precautelar la integridad y privacidad de los activos de una organización y de su estructura computacional.

No hay proceso o norma que garantice la seguridad informática al 100%, lo más seguro es que no hay sistema seguro, sin embargo, es importante aplicar una metodología que reduzca al mínimo las posibles amenazas que puede tener la organización.

Con la aplicación de un esquema de seguridad informática, se evita que personas no autorizadas tengan acceso a los sistemas de cómputo, a sus bases de datos, información de clientes, empleados, proveedores, etc.

El concepto de Ciberseguridad se enfoca a la seguridad en internet y los medios electrónicos, en la actualidad son miles de transacciones que se realizan a través de la red de redes; personas, empresas, países inclusive pueden ser víctimas de un ciberataque.

Un ciberataque es cualquier acción realizada por criminales (personas u organizaciones) con el fin de: destruir, modificar, robar o publicar información sensible como:

- Robo de información corporativa
- Robo de tarjetas de crédito.

- Robo de datos médicos.
- Robo de credenciales.
- Ataques destructivos a organizaciones.

En la siguiente figura se detallan los 3 tipos de seguridad informática que deben ser considerados.



Figura 2.1 Tipos de Seguridad informática¹ fuente: Universidad de Valencia

¹ Extraído de la página de la Universidad Internacional de Valencia.

2.2 INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN.

Se considera como seguridad de la información a la protección de los sistemas de información y de la información contenidos o circulante en ellos, para que no sean interceptados, destruidos o divulgados por terceros.

La información puede estar contenida o presentada en cualquier formato, como:

- Impresa
- Dispositivos electrónicos (Discos duros, USB, CD, DVD)
- Escrita en papel
- Audio (conversación)
- Video

La Seguridad de la información se caracteriza por cumplir con los siguientes objetivos:



Figura 2.2 Objetivos de la Seguridad informática fuente: autor

2.3 OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

2.3.1 INTEGRIDAD

Consiste en garantizar que la información almacenada no ha sido modificada por personal no autorizado.

La información debe ser confiable y consistente.

2.3.2 CONFIDENCIALIDAD

Consiste en garantizar que la información esté disponible para el personal autorizado, es decir, alguien sin autorización no podrá tener acceso a dicha información.

2.3.3 DISPONIBILIDAD

Consiste en garantizar que la información esté disponible en todo momento sólo para el personal autorizado.

2.3.4 NO REPUDIO

Consiste en garantizar que las partes que realizan la comunicación, emisor y receptor no puedan negar el origen o el destino de la información.

2.4 CONCEPTO DE INFORMACIÓN

La información es un conjunto de datos procesados y organizados entre sí, que tienen un valor intangible para el propietario.

Se puede llamar a administración de la información como el conjunto de procedimientos, técnicas, actividades que están destinados a controlar el acceso a los sistemas, uso de la información y del almacenamiento del mismo, por parte de los colaboradores de la compañía.

Para una empresa de Telecomunicaciones, el mantener una buena administración de información es de vital importancia, ya que de ello depende el giro del negocio.

El prestigio, y éxito de la compañía no solo gira con el correcto uso de sus recursos (materiales, humanos); sino también del manejo de sus activos intangibles (el know-how o conocimiento ambiente empresarial, su marca, permanencia y preferencia de sus clientes).

En una organización, se puede clasificar la información por su valor, de acuerdo a [5]:

Valor administrativo. - La Dirección o Gerencia puede tomar decisiones.

Valor Operacional. - Cuando la información apoya a la gestión realizada de forma rutinaria.

Valor documental. - Sirve de soporte para las actividades realizadas en la organización.

Valor Histórico. - Información de actividades o eventos realizados y que sirven para realizar o planificar actividades en el futuro.

2.5 AMENAZAS A LA SEGURIDAD DE LA INFORMACIÓN

Se debe considerar como amenaza a la seguridad de la información todo aquello que puede interrumpir el correcto funcionamiento de los procesos.

Algunas de estas amenazas son:

- Virus informático
- Espionaje
- Sabotaje
- Fuga de información
- Suplantación de identidad
- Denegación de Servicio (DoS)
- Ataques de fuerza bruta
- Alteración de información

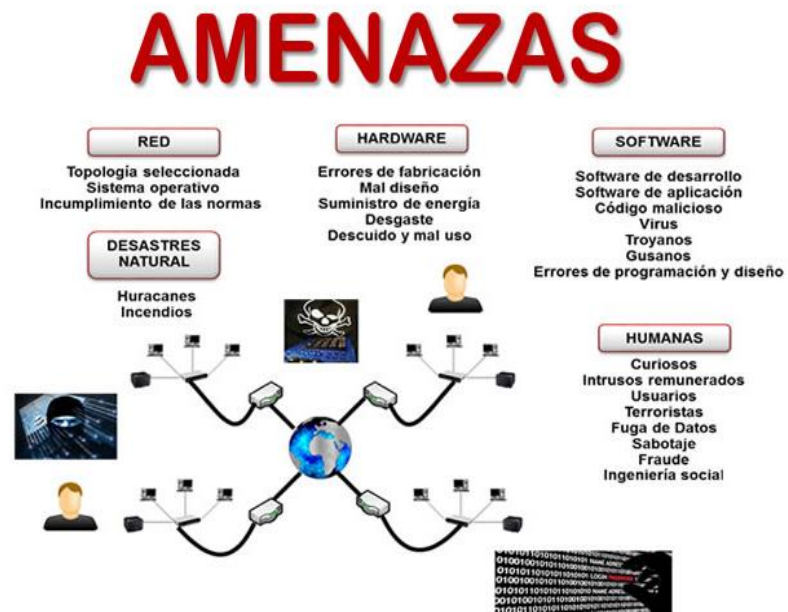


Figura 2.5 Tipos de amenazas

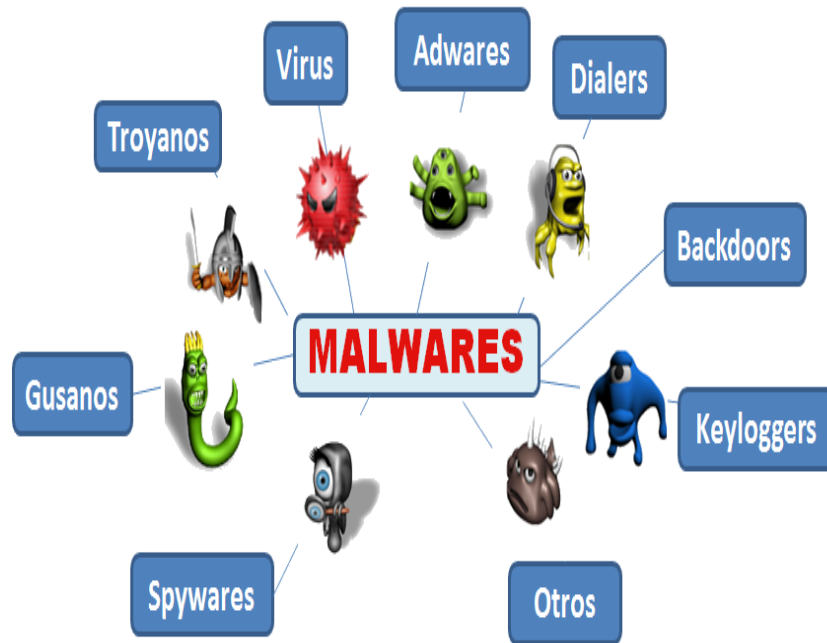


Figura 2.3 Tipos de Malware fuente: Internetlab

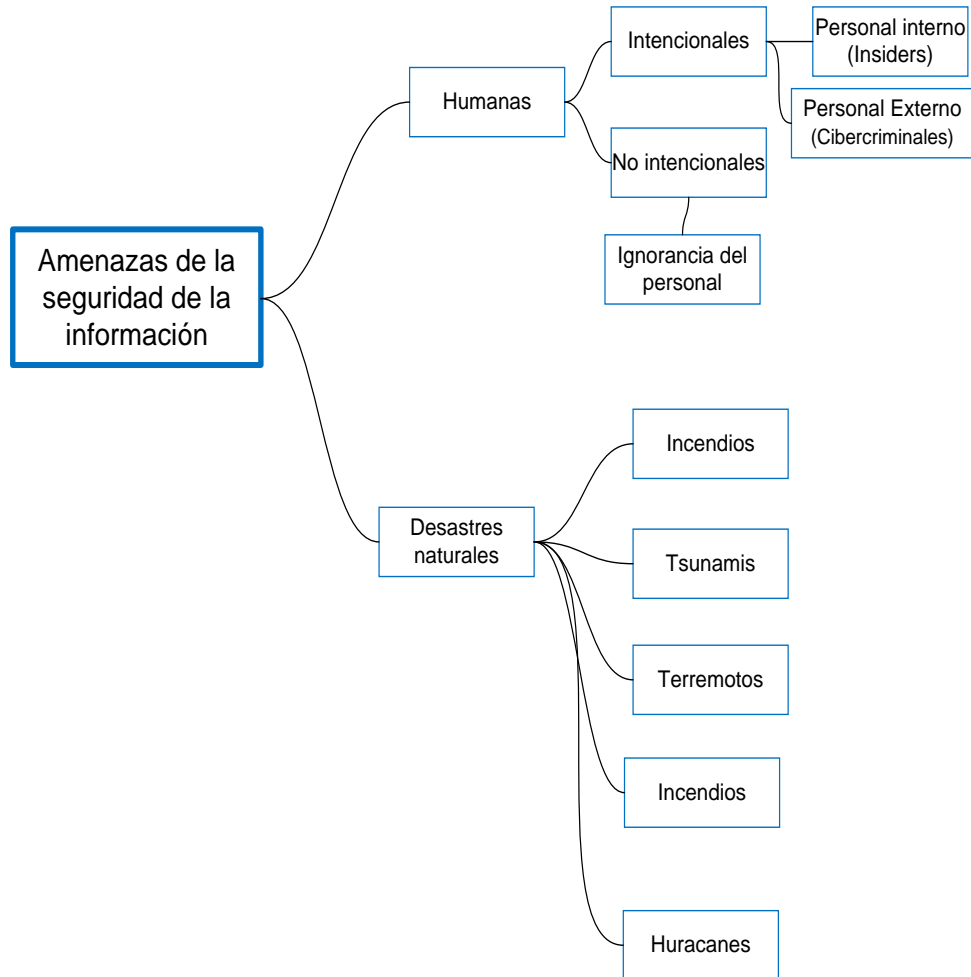


Figura 2.4 Clasificación de amenazas fuente: autor

De acuerdo a un estudio realizado por PWC [6] en una Encuesta Global sobre la seguridad de la Información entre los años 2009 y 2015, se evidencia un crecimiento de incidentes entre los años 2013, 2014 y 2015

Los incidentes fueron considerados en millones:

Tabla 1 Incidentes de seguridad por año

Año	Incidentes	Variación
2009	3,4	176,47%
2010	9,4	141,49%
2011	22,7	9,69%
2012	24,9	20,08%
2013	29,9	43,48%
2014	42,9	38,00%
2015	59,2	

En el siguiente gráfico consta la evolución de incidentes, con un crecimiento del 38% entre los años 2014 – 2015, cifra que preocupa a las organizaciones.

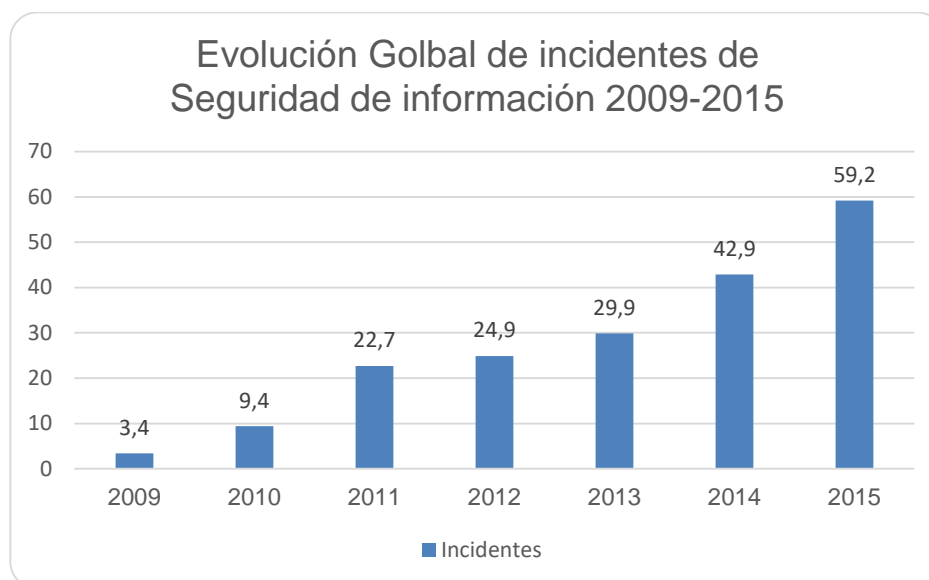


Figura 2.2 Evolución Incidentes de Seguridad Fuente: [6] Sara Bursztein •

19/12/2016

Los incidentes de seguridad van cambiando con el tiempo, esto se debe al cambio constante en las tecnologías, en el hardware, software y las técnicas de penetración que se van perfeccionando por parte de los ciberdelincuentes.

Es importante analizar estos incidentes y descubrir sus orígenes con el fin de poder determinar la forma de mitigar dichos incidentes, en el estudio realizado por PWC (The Global State of Information Security® Survey 2016); se determinaron los siguientes puntos:

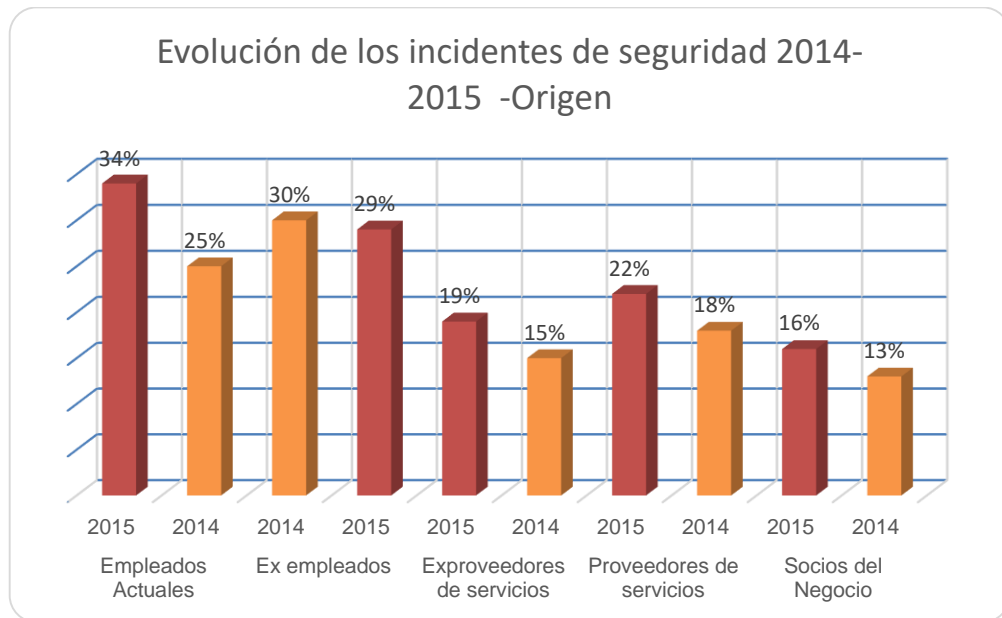


Figura 2.3 Evolución incidente de seguridad del 2014 al 2015

Fuente: [6] Sara Bursztein • 19/12/2016

Como se observa, el origen de los incidentes de seguridad tiene como actores principales a empleados actuales y ex empleados, alcanzando un 34%-25% y un 30%-29% respectivamente, lo que significa que, pese a que en las empresas se apliquen normas y controles en este aspecto, el factor humano sigue siendo el eslabón más débil de la cadena.

En mayo del 2014, la empresa Sony Pictures fue blanco de cibercriminales que afectó a 47 mil personas [7], el F.B.I. sostenía que Corea del Norte estuvo detrás del ciberataque; sin embargo, la empresa de seguridad Norse que fue contratada

para realizar la investigación afirmó que fue un ex empleado quien causó el ataque.

El estudio realizado por Norse determinó que el ataque fue perpetrado por personas de Estados Unidos, Canadá, Singapur y Tailandia.

¿Cómo mitigar esta problemática?

- Identificar las cuentas con privilegios de administrador
- Eliminar las cuentas que ya no estén en uso
- Realizar un constante seguimiento con el área de TH y actualizar el sistema de empleados.

En tercer y cuarto lugar del este estudio, se ubican los ex proveedores y proveedores de servicio; esto es un claro aviso a las empresas que por abaratar costos recurren a la tercerización de empresas que ofrecen varios servicios, esto implica que una persona ajena a la organización tendrá acceso a: operar, manipular, los sistemas informáticos; llegando a ocasionar incidentes de seguridad informática, sino se lleva una política adecuada este punto puede

ocasionar un gran dolor de cabeza para los administradores de la seguridad informática.

¿Cómo mitigar esta problemática?

- Realizando un acuerdo de confidencialidad de la información.
- Conociendo el perfil del personal de apoyo.

Conocer el ambiente al que la empresa tercerizada presta sus servicios.

Como último punto en este estudio, se tienen los incidentes ocasionados por Socios del negocio, esto hace referencia a los intercambios de información que existen entre los involucrados, por desconocimiento de la confidencialidad de la información que manejan, no siempre se respeta este punto, siendo un punto negativo para la empresa.

¿Cómo mitigar esta problemática?

- Informar a los socios el tipo de información que reciben e instruirlos sobre los efectos que pueden ocasionar su pérdida o difusión no autorizada.

A continuación, se definirán los tipos de amenazas a la seguridad de la información más comunes [8]:



Figura 2.7 Tipos de amenazas más comunes fuente: autor

2.6 DELITOS INFORMÁTICOS

Se puede definir como delito informático o ciberdelito a toda característica o acción ilícita y culpable que por medio de internet, se tiene acceso no autorizado a sistemas informáticos, con el fin de alterar, robar o destruir dispositivos electrónicos, computadores, y redes. [10]

Gracias a internet y al constante desarrollo de la tecnología, los criminales han encontrado una nueva forma de delinquir, el uso de herramientas tecnológicas ha permitido que se comentan robos, fraudes, chantajes, interceptación ilegal de datos, etc.

2.6.1 TIPOS DE DELITOS INFORMÁTICOS

En este punto es necesario diferenciar los diferentes tipos de delitos informáticos que existen [11]:

- Delitos Computacionales
- Delitos Informáticos

Delitos computacionales. - actividades delictivas realizadas a dispositivos conectados a redes locales, nacionales o globales con el fin

de impactar bienes de las personas u organizaciones; estas acciones pueden ser: robo de cuentas bancarias, robo de información privada para luego ser utilizadas como medios de extorsión, etc.

Delitos Informáticos. - acciones delictivas en contra del sistema, es decir, que el ataque es dirigido a los programas o la forma lógica de los sistemas, como ejemplo se puede considerar la intromisión de virus, gusanos a través del sistema.

2.6.2 CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS.

Se pueden identificar los delitos informáticos por las siguientes características [12]:

- Delitos cometidos de forma remota, no es necesario estar en el sitio donde residen los equipos informáticos.
- Son muchos los casos, pero pocos deciden denunciarlos, por ello no se tiene una estadística real.
- No se necesita de una inversión grande, únicamente herramientas y dispositivos electrónicos.

- Para probar un delito informático, es necesario tener un alto conocimiento en esta rama de la informática.
- Se necesita un alto conocimiento en tecnología para poder llevar a cabo estos delitos.
- Estos delitos pueden ser cometidos también por organizaciones delictivas con un alto grado de conocimientos en informática.
- Tienen como fin el factor económico, o reconocimiento.
- Tienden a incrementarse cada vez.
- Provocan considerables afectaciones económicas.
- Son acciones realizadas de oportunidad.

2.6.3 ADMINISTRACIÓN DE LA SEGURIDAD INFORMÁTICA.

Sin lugar a duda, la administración de seguridad informática es de real importancia para las organizaciones, ya que la información ha sido, es y será el activo intangible más importante.

Es necesario implementar correctamente políticas y los controles necesarios para mitigar posibles ataques al sistema de información.

En el pasado, las organizaciones protegían su información confidencial de amenazas externas, a través de firewalls, sin embargo, en la actualidad las amenazas no sólo son externas sino también podrían ser internas (colaboradores inconformes, desleales llamados insiders).

Cuando no se tiene un plan de continuidad del negocio, un simple fallo en la seguridad puede comprometer el futuro y la reputación de la organización, por tal motivo el tener una buena administración de la seguridad minimiza los posibles fraudes, fugas de información, alteración de datos, etc.

2.6.4 NORMA ISO 27001

La ISO 27001, es una norma emitida por la Organización Internacional de Normalización (ISO), describe la forma de gestionar la seguridad de la información, en el 2005 fue publicada como una actualización de la norma británica BS 7799-2 [11].

La norma 27001 puede ser aplicada en cualquier tipo de organización; sean estas empresas públicas o privadas, grandes o pequeña; la norma cuenta

con la participación de especialistas en seguridad de la información a nivel mundial.

Una empresa puede certificarse con esta norma, lo que implica que la información que es procesada, almacenada y transmitida en esa organización; cumple con los estándares internacionales sobre la seguridad de la información.

Cumplir con los lineamientos que sugiere la ISO 27001 es de gran importancia para las empresas, ya que protegen uno de sus activos más preciados, la información; a diferencia de otros documentos de la serie 27000, la 27001 es certificable, es decir, que las empresas pueden demostrar su compromiso con la protección de datos e información.

Una empresa certificada en la norma ISO 27001 no elimina en su totalidad el riesgo de que su información está protegida, sin embargo, cada año las empresas muestran su interés en ser certificadas, de tal forma que demuestran el interés que tienen en resguardar su información.

De acuerdo a un estudio realizado por ISO Survey [12] indica el detalle de las certificaciones en la norma ISO realizadas por diferentes países a nivel mundial, desde el lanzamiento de su primera versión 2005 hasta la versión más reciente 2013.

A continuación, se muestra la tendencia de certificaciones realizadas por año, desde el lanzamiento de la primera versión hasta el 2015, podemos notar un incremento en certificaciones en los últimos 3 años; en el 2013 se registraron 21604, 2014 existió un incremento del 6%, mientras que en el 2015 se registraron 27536 certificaciones, un incremento del 20% con respecto al 2014.

Tabla 2 Certificaciones por año en norma ISO 27001

Año	Total	Variación
2013	21.604	-
2014	23.005	6%
2015	27.536	20%



Figura 2.4 Evolutivo de Certificaciones ISO 27001 por año
Fuente: Autor

Es importante detallar qué países lideran el top 10 en realizar la certificación ISO 27001, gracias a la encuesta realizada por ISO, se tiene acceso al siguiente detalle:

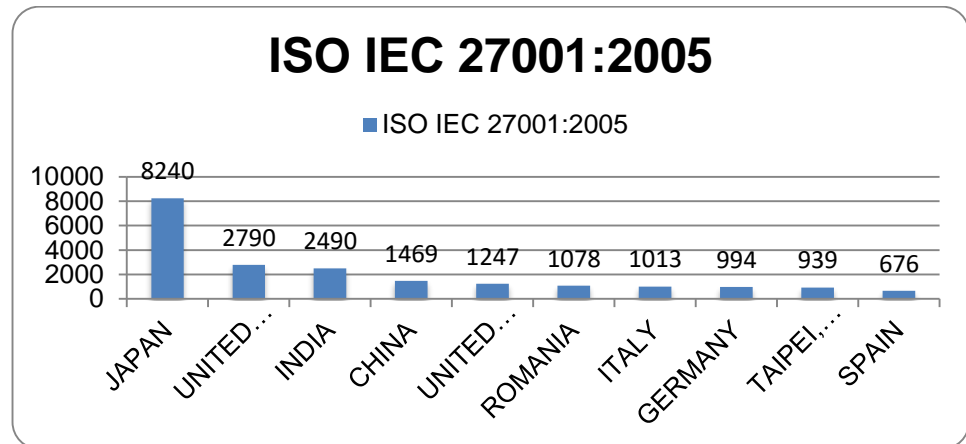


Figura 2.5 Top países Certificados en ISO 27001:2005
Fuente: Autor

Ecuador se encuentra en el puesto 52 con 11 certificaciones en la norma ISO 27001 [20], pese a que pocas empresas han buscado certificarse, existen muchas que siguen estos lineamientos, entre ellas la empresa de Telecomunicaciones XYZ.

La ISO 27001 tiene como modelo fundamental el PDCA (del inglés plan-do-check-act) que significa Planear-Hacer-Chequear-Actuar, el cual propone ser aplicado en todos los modelos SGSI.

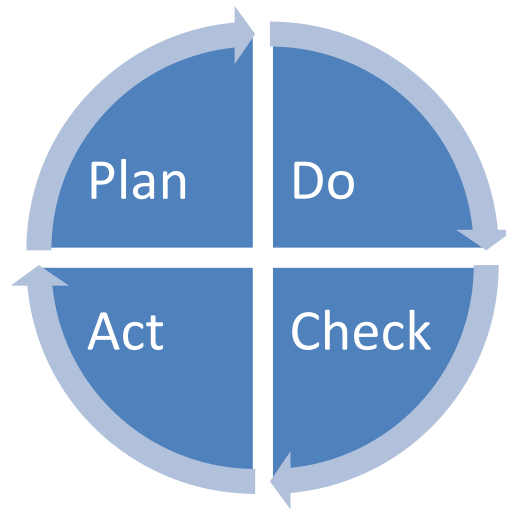


Figura 2.6 Modelo PDCA
fuente: Autor

Planear.

Establece políticas, procesos, procedimientos y objetivos SGSI para mejorar la seguridad de la información, de tal forma que se pueda entregar resultados a fines a las políticas generales de la empresa.

Hacer.

Aplicar y procesar las políticas, procesos y controles y procedimientos SGSI.

Chequear.

Revisar los procesos a los cuales se han implementado los controles de la seguridad de la información y determinar una evaluación integral, con el fin de realizar reportes a la gerencia sobre los resultados obtenidos.

Actuar.

Este punto es uno de los más importantes ya que permitirá tomar decisiones preventivas y correctivas, basados en informes obtenidos; de tal forma que se pueda tener un control y mejora continua de todos los procesos.

Funcionamiento de la ISO 27001.

El eje principal de la norma ISO 27001, es la protección de la confidencialidad, integridad, y disponibilidad de la información, en una empresa sea esta grande, mediana o pequeña. Para conocer cuáles son los potenciales problemas que podrían afectar la seguridad de la información es necesario evaluar los riesgos, una vez evaluados.

Por tal motivo la evaluación de riesgos: determinar dónde se presentan los riesgos y como tratarlos de forma sistemática, es la principal filosofía de la ISO 27001[13].

Los controles a implementarse se presentan en forma de políticas a ser implementadas, generalmente estas políticas suelen ser aplicadas tanto en equipos como en sus sistemas, de tal forma que se minimice el impacto que puede tener un fallo en la seguridad.

La gestión de la seguridad no siempre está vinculada al hardware o software (ejemplo firewalls, anti virus, etc.), también debe relacionarse a los procesos, la administración del recurso humano, así como la protección legal y jurídica.

Para implantar un SGSI en base al sistema PDCA, la ISO 27001 establece los siguientes puntos [14]:

- Análisis y evaluación de riesgos.
- Implementación de controles.
- Definición para el tratamiento de riesgos.

- Alcance.
- Procesos de la organización.
- Partes involucradas.
- Objetivos alcanzables y medibles.
- Documentación del proceso.
- Auditorías internas y externas.

2.6.5 ANÁLISIS Y EVALUACIÓN DE RIESGOS.

Se considera al riesgo a la medida de daño que puede ocurrir en un sistema, determinando el impacto de las amenazas sobre activos, el riesgo es considerable de acuerdo al impacto y la frecuencia con la que suceden.

Para valorar los riesgos se utiliza la fórmula matemática: $\text{Riesgo} = \text{probabilidad de amenaza} \times \text{magnitud del daño}$.

Es importante calificar los riesgos para poder considerar la importancia de la información en un posible fallo de la seguridad que comprometa la pérdida de la confidencialidad, integridad, y disponibilidad de la información, a más

de analizar los riesgos, es necesario también evaluar las consecuencias que puede tener.

ALTA

Tabla 3 Evaluación de Riesgo

IMPACTO	Riesgo medio	Riesgo Alto
	Bajo Riesgo	Riesgo Medio
	BAJA	ALTA

PROBABILIDAD

Riesgo Medio = Alto impacto baja probabilidad

Riesgo Alto = Alto impacto alta probabilidad

Riesgo bajo = Bajo impacto baja probabilidad

Riesgo Medio = Bajo impacto alta probabilidad

Tipos De Riesgos

Riesgo inherente: Riesgo propio de la actividad del negocio sin considerar los controles.



Figura 2.7 Cálculo riesgo inherente fuente: Autor

Riesgo residual: Riesgo residual después de aplicar los controles

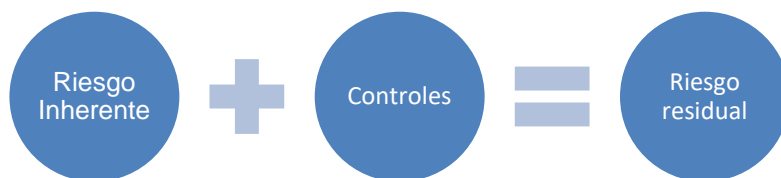


Figura 2.8 Cálculo de Riesgo Residual fuente: Autor

2.6.6 IMPLEMENTACIÓN DE CONTROLES

Luego de realizar el análisis del riesgo que puede presentarse, es necesario planear los controles que deben ser implementados en la empresa, estos controles deben ser verificables y auditables.

En la norma ISO 27001:2005 se tienen 133 controles y dependerá de cada empresa si debe implementar en su totalidad o de forma parcial los controles.

2.6.7 DEFINICIÓN PARA EL TRATAMIENTO DE RIESGOS.

Luego de realizado el análisis del riesgo se debe crear un esquema de mejora a los procesos luego de que se tenga en cuenta los potenciales riesgos a los que se ve amenazada la seguridad de la información.

A continuación, se detallan las formas de tratar los riesgos:

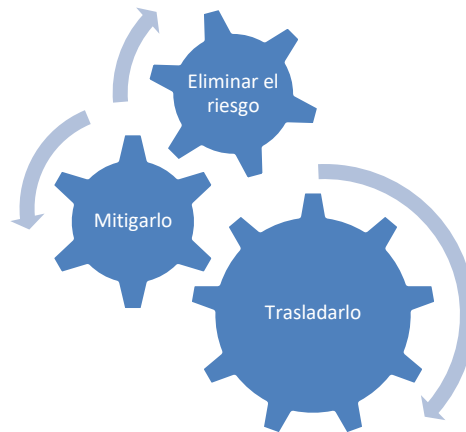


Figura 2.9 Formas de Tratar el riesgo Fuente: Autor

Eliminar el riesgo.

Si se conoce que el riesgo puede ocasionar daños críticos a la información de una empresa, se debe destinar todos los recursos para eliminar el riesgo en su totalidad.

Mitigarlo.

En algunas ocasiones el riesgo no puede ser eliminado en su totalidad, ya sea porque para la empresa es técnicamente imposible resolverlo o porque el riesgo no es considerado como crítico, por tal motivo no se lo elimina, sino que sólo se lo controla.

Trasladarlo.

Se tiene la alternativa de trasladar el riesgo cuando se hace uso de una empresa que dé el contingente para este tipo de eventos, por lo general se trata de empresas aseguradoras que compensen la inversión de contratarlas con el posible deterioro de la información.

Alcance.

El alcance puede establecerse por línea de negocio, es decir, la empresa puede decidir si otorga más recursos al área de servicio al cliente o de facturación, siendo el segundo un área crítica para la empresa.

Se podría detallar el alcance de acuerdo al área que puede ser más vulnerable ante fallos en la seguridad de la información.

Procesos de la organización.

Es importante conocer los procesos de la organización, ya que así se puede realizar un análisis integral y determinar los problemas internos y externos, así como sus debilidades, amenazas, fortalezas y oportunidades.

Partes involucradas.

Es importante conocer el contexto de la organización y así poder determinar las partes involucradas en el giro del negocio.

Siendo parte del negocio:

- Clientes internos
- Proveedores
- Clientes externos
- Sociedad en General

Objetivos alcanzables y medibles.

Para las empresas es importante fijarse objetivos a corto, mediano o largo plazo; estos objetivos deben ser claramente mediable.

Para alcanzar los objetivos, es necesario se involucre a todo el personal de la organización, ya que es necesario que todo el personal se sienta

identificado con que tienen un objetivo en común, en este sentido, el talento humano debe conocer aspectos también en seguridad de la información.

Documentación del proceso.

La ISO 27001 hace énfasis en que la organización debe tener sus procesos, procedimientos, políticas debidamente documentadas.

La documentación puede ser presentada en diferentes formatos:

- Archivos de texto
- Documentos impresos
- Hojas de cálculo
- Archivos de audio o video
- Etc.

Auditorías internas y externas.

Para un correcto funcionamiento de un SGSI es necesario llevar a cabo auditorías internas cada cierto tiempo, de tal forma que se pueda garantizar que el sistema, proceso se encuentran controlados.

Tipos de Auditorías internas:

- Controles: Se auditan los controles aplicados por la organización, por lo general es realizado por personal experto y puede realizarse en diferentes años.
- Gestión: Se auditan el liderazgo, procesos, el contexto de la organización, etc.

2.6.8 NORMA ISO 27002

El enfoque principal de este proyecto es la aplicación de la gestión de la seguridad de la información por medio de la norma ISO 27002:2015, el cual presenta políticas de control más claras

Cabe indicar que se eligió la norma ISO 27002 versión 2015 porque extiende la información de los anexos contenidos en la norma ISO 27001:2005, ya que actualmente la organización sigue estos lineamientos.

A continuación, se detallan los controles a los que hace referencia la norma ISO 27002:2005

Tabla 4 Controles de la norma ISO 27002:2005

ISO 27002:2005
5. Política de Seguridad de la información
6. Organización de la seguridad de la información
7. Gestión de activos
8. Seguridad de los Recursos humanos
9. Seguridad Física y entorno
10. Gestión de comunicaciones y operación
11. Control de Acceso
12. Adquisición, desarrollo y mantenimiento de sistemas de información
13. Gestión de incidentes Sistemas de información.
14. Gestión de continuidad de negocio
15. Cumplimiento

2.6.9 POLÍTICA DE SEGURIDAD

Las políticas de seguridad forman parte de las instrucciones generales utilizadas por la organización para generar estrategias bien establecidas, con la finalidad de presentar objetivos específicos y generales en temas de seguridad. Estas políticas se establecen como reglas que cumplan las necesidades de las áreas internas, aplicándolos por medio de controles fundamentados en mejorar la gestión de las mismas.

Dentro de la estructura utilizada para la elaboración de éstas políticas, se encuentran los siguientes puntos:

- Resumen
- Introducción
- Ámbito de aplicación
- Objetivos
- Principios
- Responsabilidades
- Resultados
- Políticas Relacionadas

2.6.10 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.

La importancia de los aspectos organizativos es la de lograr una correcta administración de los posibles riesgos de fuga de información por parte de personal que debe acceder a data sensible de la organización por diversos medios, ya sean internos o externos. Todo esto genera la necesidad de aplicar controles por medio de la coordinación y asignación de áreas de seguridad de la información y establecimiento de funciones y responsabilidades. La colaboración multidisciplinaria, incluyendo desde la dirección de la organización y expertos en materia de seguridad debe

generar un mejor enfoque en la aplicación de normas claras, estableciendo roles de seguridad de manera general. El apoyo externo por parte de expertos en el área de seguridad forma parte fundamental de la implementación de estos controles, permitiendo la evolución de las políticas ya establecidas y logrando mitigar al mínimo los nuevos riesgos en materia de seguridad de la información.

2.6.11 GESTIÓN DE ACTIVOS

La gestión de activos enfocada al esquema de la seguridad de la Información se basa en definir claramente todos los activos que presenta la organización para poder lograr una correcta administración de los mismos. La clasificación debe ser basada en varios aspectos fundamentales, como su funcionalidad, que tan crítico es para la organización y cuán sensible puede llegar a ser, para identificar como se deben aplicar las mejores prácticas de protección de dichos activos. Es importante recalcar que la metodología de clasificación de activos debe ser analizada de manera clara, para no generar procesos complejos de control que conllevaría riesgos adicionales para la organización.

Se puede definir como activos los siguientes:

- Recursos de información, donde se consideran la data contenida en documentos, manuales, procedimientos, planes utilizados para migraciones, contingentes, bases de datos, data almacenada, etc.
- Recursos de software; todos los aplicativos utilizados dentro de la organización, aplicaciones tanto internas como externas de uso diario, lenguajes de programación utilizados por áreas de proyectos, sistemas operativos, etc.
- Activos físicos; todo equipo tecnológico utilizado (computadoras, servidores, etc.), medios de almacenamiento tanto interno como externo, equipos varios como mobiliarios, etc.
- Servicios; estos pueden ser tanto informáticos como los básicos.

2.6.12 SEGURIDAD HACIA EL RECURSO HUMANO

Los recursos humanos dentro de la organización es el activo más importante de la organización y a su vez, el punto más sensible dentro del mismo. Desde el ingreso del personal a la empresa, se genera una gran cantidad de transferencia de conocimiento que puede conllevar a riesgos importantes si no se delimitan responsabilidades y controles de seguridad respectivos. Las buenas prácticas para el manejo de la información, seguridad y sanciones impuestas en caso de incumplimientos de las normas deben ser transmitidas de manera continua para poder minimizar:

errores involuntarios, actos ilícitos, incorrecto uso de información, recursos e instalaciones, entre otros. Los acuerdos de confidencialidad deben ser incluidos en todo reclutamiento de personal, adicionando las políticas de seguridad e incluyendo dentro de las funciones establecidas para cada recurso, el compromiso inherente de mantener a salvo información importante que esté a su cargo y las posibles amenazas que existen.

2.6.13 SEGURIDAD FÍSICA Y AMBIENTAL

El objetivo principal de diseñar esquemas de seguridad de la información es primordialmente para mitigar errores en procesos y tratar de disminuir los posibles riesgos de pérdida o mal uso de la data almacenada o los procedimientos operativos ejercidos dentro de la organización. Se deben establecer diferentes límites de acceso a información que puede considerarse crítica y la detección de intrusiones de usuarios a la misma. Adicionalmente a esto, el control de almacenamiento físico debe ser salvaguardado por procedimientos documentados para la recuperación efectiva de la información en caso de ser necesario. Los riesgos inherentes del acceso a la información deben ser analizados de acuerdo a su ubicación, en caso de que se encuentren fuera de la organización o si está almacenado por medio de terceros.

2.6.14 GESTIÓN DE COMUNICACIONES Y OPERACIONES

La tecnología actualmente permite la transferencia de información de manera continua, por lo cual el esquema de gestión de la seguridad de la información abarca el análisis de todos los métodos de comunicación de la organización, tanto interna como externa, para que pueda ser protegida de terceros. Es importante que dentro de este análisis se apliquen límites sobre el traspaso de información, considerando cualquier implicación legal necesaria para para el efecto. Todo tipo de información que sea transferida fuera de la empresa, debe pasar por rigurosos controles de seguridad, aplicando políticas que estén amparadas por la ley en caso de existir fuga de información.

2.6.15 CONTROL DE ACCESO

Los controles de acceso son importantes para la organización, principalmente el acceso a la información sensible dentro de la misma. La implementación de procesos que imponga las restricciones y roles para los usuarios debe incluir el acceso a la base de datos, documentación existente, procesos y procedimientos proporcionados por el departamento de Organización y Métodos, entre otros. Se debe considerar educar al personal del buen uso de las contraseñas para cada acceso existente, la

confidencialidad de los datos y todo el equipo que esté a su cargo, durante todo el tiempo que trabaje dentro de la organización.

2.6.16 GESTIÓN DE INCIDENTES

La comunicación de eventos que puedan generar riesgos para salvaguardar la información es de vital importancia y deben ser concientizadas de manera tal que se puedan tomar correctivos a tiempo. Existen muchos activos, tanto físicos como de información, que pueden presentar eventualidades con respecto a su seguridad. Es imprescindible conocer los posibles casos que pueden presentarse para la gestión de incidentes. Todo el personal de la organización debe tener conocimiento de las responsabilidades que se adquieren sobre todos los activos a su cargo, siempre formando parte de entrenamientos continuos para la detección de nuevos riesgos y aplicar las mejores prácticas de la seguridad de la información.

Las mejores estrategias para analizar incidentes conllevan desde el análisis de los antecedentes que lo provocaron hasta definir las conclusiones que se pueden determinar y recomendaciones para evitar que dichos incidentes vuelvan a generarse. La revisión de casos como el

fraude informático, el robo de información, entre otros, permite encontrar las posibles debilidades de la gestión actual, y logra comunicar efectivamente nuevos mecanismos de control para evitar nuevas intrusiones de servicios. Los elementos de comunicación de este tipo de eventos deben ser accesibles y de conocimiento general del personal en la organización.

2.6.17 GESTIÓN DE CONTINUIDAD DE NEGOCIO

Los planes implementados de seguridad de la información suelen ser planteados para un cierto límite de eventos y no suelen ser a todos los activos y procesos de la organización. El verdadero enfoque de los procesos de control de la seguridad de la información debe abarcar toda la vida útil de los todos activos, tanto físicos como intangibles.

El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

Se debería integrar dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativas y/o que estén dispuestos de un modo distinto a la operativa habitual.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos.

Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre.

Minimizar los efectos de las posibles interrupciones de las actividades normales de la organización asociadas a desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos, protegiendo los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Instruir al personal involucrado en los procedimientos de reanudación y recuperación en relación a los objetivos del plan, los mecanismos de coordinación y comunicación entre equipos (personal involucrado), los procedimientos de divulgación en uso, los requisitos de la seguridad, los procesos específicos para el personal involucrado y responsabilidades individuales.

2.6.18 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La implementación de procesos de control de la seguridad de la información se debe aplicar desde el inicio de la compra y desarrollo de todos los procesos y módulos presentes en la organización. Todo debe estar correctamente documentado y analizando los posibles riesgos y

eventos que puedan generarse de acuerdo a la criticidad de los módulos o procesos que sean considerados.

2.6.19 CUMPLIMIENTO LEGAL

Todo sistema interno de la organización debe mantener:

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deberían estar debidamente definidos y documentados.

El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos.

Se debe revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la

política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

2.7 ANÁLISIS DE RIESGO UTILIZANDO LA METODOLOGÍA MAGERIT

La metodología Magerit es utilizada para el análisis y control de riesgos, fue diseñada por el Consejo Superior de administración electrónica Española (CSAE).

El constante uso de los sistemas de información, hace que los ciudadanos consideren necesario que la información que se procese, almacene en estas entidades cuente con un adecuado nivel de gestión que garantice la seguridad de su información.

Para un buen gobierno privado o público, la gestión de riesgos es fundamental por las decisiones que se tomen entorno al conocimiento que los riesgos implican.

Magerit responde a la normativa ISO 31000 [16] en cuanto al Proceso de Gestión de Riesgos, "Implementación de la gestión de Riesgos" sec. 4.4.

Esta metodología se implementa el Proceso de Gestión de Riesgos en un esquema de trabajo para que las áreas de las compañías tomen decisiones considerando los riesgos que se derivan del uso de las tecnologías de información.

La siguiente gráfica muestra el esquema del marco de trabajo para la gestión de Riesgo de acuerdo a la norma ISO 31000.

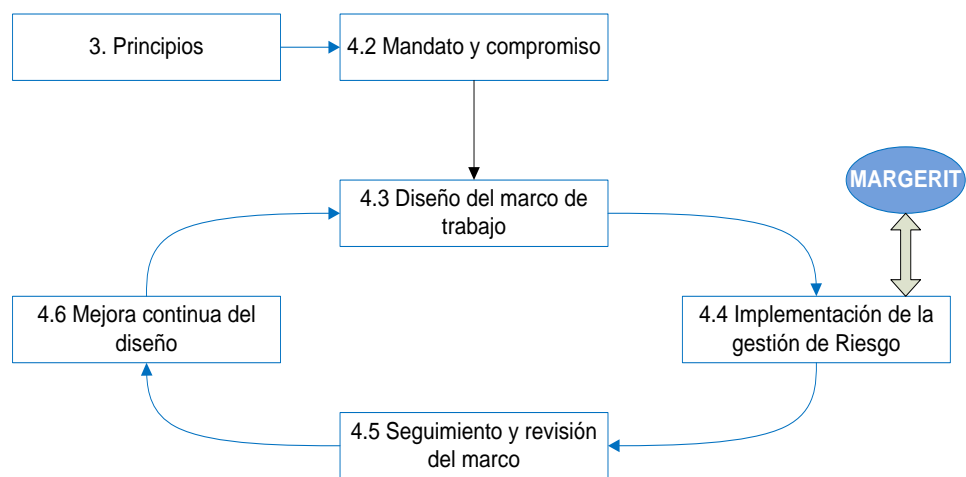


Figura 2.10 Gestión de Riesgo de acuerdo a la norma ISO 31000
fuente: Magerit

Magerit busca los siguientes objetivos que son una aproximación metódica que no deja lugar a la improvisación y no depende de la objetividad del analista.

Directos

- Ofrecer un método sistémico para analizar los riesgos derivados del uso de las tecnologías de la información.
- Concienciar a los directivos de las organizaciones de la existencia de riesgos y de su respectivo control y gestión.
- Ayuda a tener una planificación sobre el tratamiento a tiempo de los riesgos y tenerlos controlados.

Indirectos

- Proyecta a la organización para procesos de auditoría, certificaciones, o acreditaciones según sea el caso.

Los informes presentados utilizando el modelo Magerit contemplan uniformidad en sus descubrimientos y conclusiones en su análisis de riesgo, en función a eso se cuenta con:

Modelo de valor

Dependencia de los activos y el valor que representan para la organización.

Mapa de Riesgos

Muestran a los activos y la relación a las amenazas que están expuestos.

Declaración de aplicabilidad.

Confirman si los controles son aplicables o no al sistema de información o no.

Evaluación de seguridad.

Evalúa si la seguridad es eficiente frente al riesgo que afrontan.

Estado de riesgo.

Considera el riesgo residual, es decir, el riesgo que resulta luego de aplicar los controles aplicados.

Cumplimiento de la normativa.

Confirma si los controles aplicados se ajustan de acuerdo a la norma.

Plan de seguridad.

Esquema de seguridad que permite aplicar los controles necesarios para el tratamiento del riesgo.

Tareas a realizar al momento de aplicar el modelo Magerit:

Análisis de Riesgo.

Permite a la organización analizar el riesgo que existe y estimar los posibles incidentes de seguridad que pueden ocurrir.

Tratamiento de riesgo

Permite a la organización la defensa eficaz minimizando el riesgo presentado, para seguir operando en las mejores condiciones, la Dirección debe estar consciente que una vez que se apliquen los controles necesarios, quedará un riesgo residual que debe ser asumido por ellos.

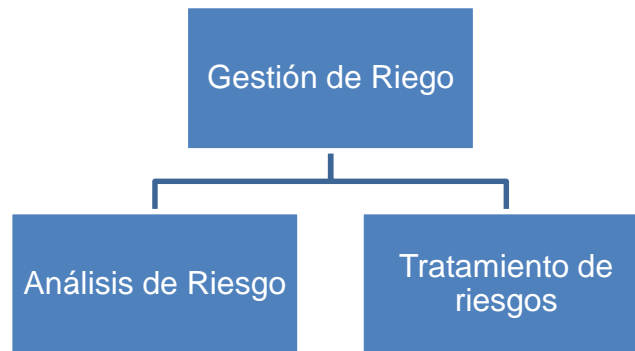


Figura 2.11 Gestión de Riesgo fuente: Magerit

Para el análisis de riesgo se debe considerar:

- **Activos:** elementos de un sistema de información que soportan la gestión de la organización
- **Amenazas:** acciones o eventos que pueden dañar los activos, procesos, sistemas de una organización.
- **Contramedida:** controles que se implementan para que las amenazas no causen el daño estimado.

Una vez se considere estos elementos se podrá definir el impacto que tendría si las amenazas afectan los activos, así como el riesgo de que eventualmente sucedan.

De acuerdo a la metodología Magerit, para realizar un correcto análisis de riesgos, es necesario seguir los siguientes lineamientos:

1. Definir los activos con información relevante para la organización, su valor e interrelación en el sentido de que tan crítico sería su degradación.
2. Definir las amenazas a las que están expuestos estos activos.
3. Definir los controles frente a estas amenazas y comprobar su eficacia frente al riesgo.
4. Evaluar el impacto sobre el activo si se materializa la amenaza.
5. Evaluar el riesgo, que se definió como impacto con su respectiva calificación (posible materialización) de la amenaza.

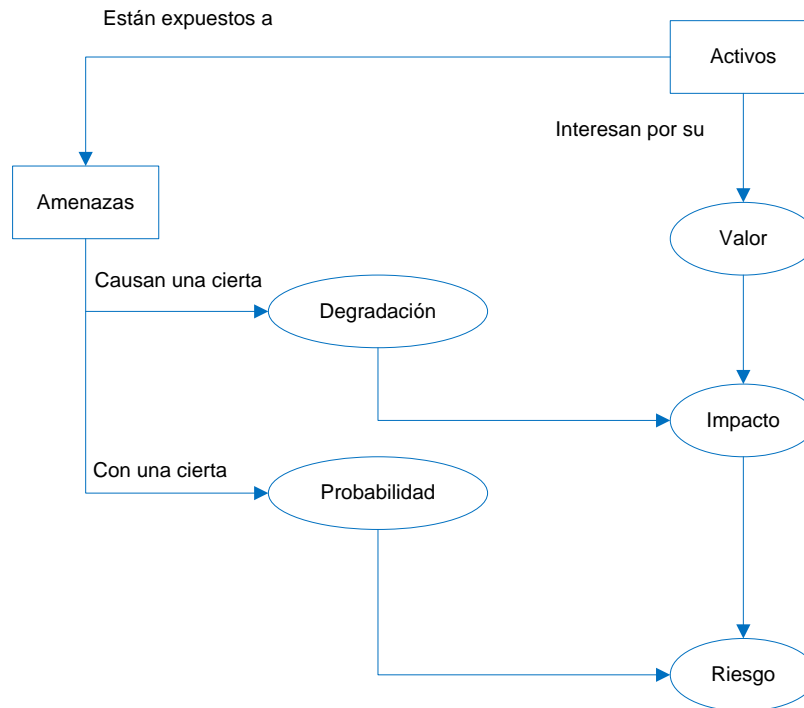


Figura 2.12 Elementos de un análisis de Riesgos. fuente: Magerit

Los activos y sus costos

Para las organizaciones es indispensable determinar el costo de su información, que no es otra cosa que conocer cuál sería el coste de recuperarse ante una incidencia de pérdida parcial o total de su activo, para ello se debe considerar:

Costo por restitución: instalación de nuevos equipos informáticos.

Costo por mano de obra: costo por contratar especialistas para que solucionen el incidente.

Lucro cesante: pérdida del valor económico que no se generó durante el incidente.

Capacidad de operar: confianza del público, proveedores traducidos en una pérdida económica

Sanciones: por incumplimiento en la entrega de algún servicio o bien durante el incidente.

Destrucción de otros activos: propios o no.

Daño a las personas

Daño del medioambiente.

Valoración cualitativa.

La valoración cualitativa (en escalas) permite realizar un análisis con rapidez, posicionando en orden relativo el valor de los activos. Plantear estas escalas como órdenes de frecuencias es muy frecuente para determinar el orden en la magnitud del riesgo.

La limitante que se tiene en las valoraciones cualitativas es que no permiten comparar valores más allá de su orden, en resumen, no permite la suma de valores.

Valoración cuantitativa.

La valoración cuantitativa, requiere de mucho esfuerzo por parte del analista ya que permite sumar valores de forma natural y por ello no es motivo de debates.

En este caso de estudio, la valoración que se debe dar es económica, por ende, se podrá realizar comparaciones entre lo que se invierte vs el valor económico del activo.

Identificación de las amenazas.

Una vez identificado los activos de la organización, el siguiente paso es analizar las posibles amenazas en las que puede verse comprometida la seguridad de la información (activos).

Las amenazas son acciones, eventos que pueden ocurrir y por ello el interés de conocer lo que puede causar a nuestros activos (sistema de información).

Las amenazas pueden ser:

De origen natural

Se consideran a los desastres naturales como terremotos, maremotos, tsunamis, inundaciones, ante esto el sistema de información es víctima pasiva, sin embargo, la administración debe estar consciente el daño que puede ocasionar este tipo de amenazas.

De origen industrial

Amenaza que está relacionada con el entorno de la organización, estos pueden ser: fallas eléctricas, contaminación, etc. Ante estas amenazas el sistema de información es víctima pasiva es necesario estar preparados ante este tipo de amenazas.

Error en aplicaciones

Amenaza que es inherente en el equipamiento propio, se presenta en errores en el diseño e implementación, las consecuencias son potencialmente negativas sobre el sistema. Este tipo de amenaza es considerado como amenaza de tipo técnico.

Ocasionadas por el personal (desconocimiento)

El personal que acceso al sistema puede ocasionar problemas en el procesamiento de la información, por lo general por desconocimiento u omisión del proceso.

Ocasionadas por el personal (de forma intencional)

El personal que tiene acceso al sistema puede ocasionar problemas en el procesamiento de la información de manera intencional con la intención de causar daños a la información que se procesa o almacena en el sistema.

Luego de evaluar las amenazas y el perjuicio que pueden ocasionar a los activos, se debe determinar el peso que tiene en el valor del activo, en los siguientes aspectos:

Degradación.

Cuantificar el daño ocasionado en el valor del activo.

Probabilidad.

Estimar que tan probable es que se materialice la amenaza.

Criterios de valorización de la información

Para la valorización de los riesgos se clasificarán de acuerdo a los pilares de la seguridad de la información [17].

Tabla 5 Criterio de Valoración con respecto a su Confidencialidad

Criterio de Valoración con respecto a su Confidencialidad		
N	Nivel	Descripción
1	Alto	La información debe ser conocida por un grupo limitado de personas
2		La información debe ser clasificada como reservada o confidencial
3		La revelación causaría daño grave
1	Medio	La información sólo debe ser conocida por quienes realicen su gestión
2		Su revelación causaría daño leve
1	Bajo	La información no debe ser conocida por personal de otras áreas
1	Mínimo	La información es de carácter público, lo puede conocer cualquier persona

Tabla 6 Criterio de Valoración con respecto a su Integridad

Criterio de Valoración con respecto a su Integridad		
N	Nivel	Descripción
1	Alto	La información está clasificada con valor histórico
2		La modificación de la información causaría perjuicio a nivel legal
3		La pérdida o alteración ocasionaría un daño considerable imposible de recuperación.
4		La alteración o daño ocasionaría perjuicio a la imagen de la compañía.
1	Medio	La alteración o daño ocasionaría un perjuicio leve a la organización
2		La alteración ocasionaría un daño al prestigio de la organización.
1	Bajo	La alteración o daño es sencillo de solucionar y no causa impacto a la organización
1	Mínimo	Fácilmente reparable

Tabla 7 Criterio de Valoración con respecto a su Disponibilidad

Criterio de Valoración con respecto a su Disponibilidad		
N	Nivel	Descripción
1	Alto (entre 0 y 5 minutos)	El no acceder en el rango de tiempo especificado ocasionaría incumplimiento legal o normativo para la organización
2		La falta de acceso ocasionaría perjuicio en el prestigio de la organización
1	Medio (entre 6 y 60 minutos)	Si la información no estaría disponible habría un efecto en las operaciones, sin embargo se podría continuar con medios alternativos
1	Baja (tolerancia de 1 a 9 horas)	Interrupción parcial de las operaciones, sin embargo las operaciones no están en riesgo
1	Mínimo (más de 9 horas)	Se puede tener demoras en el procesamiento de la información sin embargo no tiene perjuicio sobre el prestigio de la organización

CAPÍTULO 3

ANÁLISIS DE LA SITUACIÓN ACTUAL

La empresa de Telecomunicaciones XYZ, está compuesta por varios departamentos; entre ellos el área de Sistemas y en particular la Unidad de Facturación SIS GSI BILLING. Esta unidad es la encargada de realizar la facturación de todos los servicios móviles y fijos ofrecidos por la compañía; entre los servicios que brinda la empresa son:

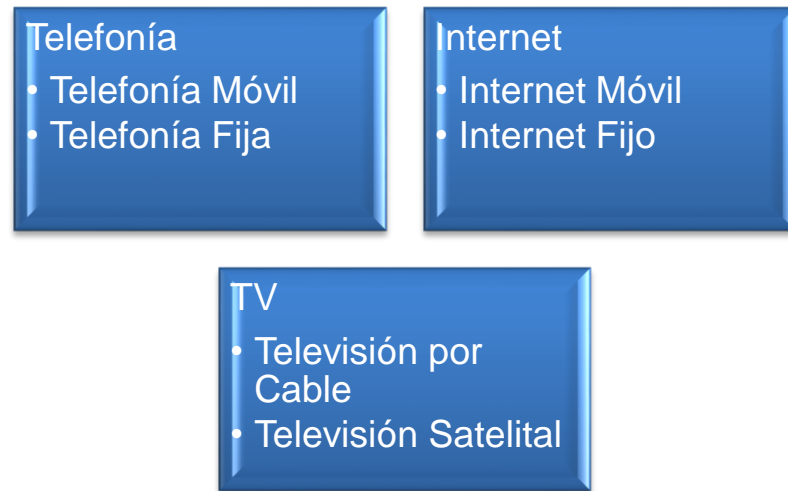


Figura 3.13 Gráfico sobre los Servicios Ofertados Fuente: Autor

Hasta el momento existen 4 ciclos de Facturación, es decir, que el proceso debe ser ejecutado 4 veces por mes:

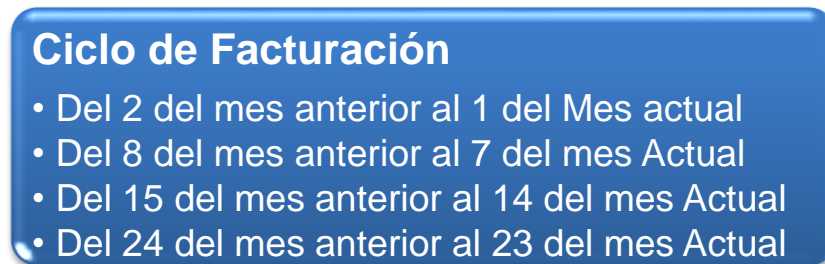


Figura 3.14 Gráfico sobre los ciclos de Facturación Fuente: Autor

Para llevar a cabo el proceso de Facturación, el área hace uso de rutinas a nivel de Base de Datos y de Servidores, a través de Procedimientos y Shell's respectivamente. La información que se procesa es de suma importancia, ya que se tiene el dato preciso de lo facturado por cada uno de los clientes, sean estos particulares o empresariales.

Son varias etapas en diferentes jornadas, existe un equipo destinado a realizar un detallado número de actividades para cumplir con los tiempos de entrega de la factura hacia los clientes, proveedores, ente regulador, etc. El equipo destinado para gestionar este proceso está formado por personal interno y por personal de apoyo (Outsourcing). En este sentido, es indispensable llevar un esquema de seguridad que garantice la integridad, confiabilidad, y disponibilidad de la información; minimizando al máximo las amenazas que conlleva trabajar con un activo sensible (la información).

3.1 METODOLOGÍA

La metodología que fue aplicada para la realización de este proyecto fue el método Descriptivo - Analítico, el cual será presentado a continuación.

3.2 TIPOS DE INVESTIGACIÓN

El uso de este tipo de investigación, el cual permite la adquisición y análisis de datos, genera objetivos más precisos para una solución sistemática óptima. Este se basa claramente en la observación de diferentes escenarios de manera controlada, permitiendo la separación y estructuración del conocimiento; datos primarios y secundarios para un mejor entendimiento de la investigación realizada.

Para el análisis de este proyecto, se utilizaron los siguientes principios:

- Análisis de la metodología utilizada para salvaguardar la información, basados en políticas de seguridad existentes, enfocado principalmente en el estándar Internacional ISO 27002.
- Observación de las vulnerabilidades de los procesos actuales ejecutados en el área de facturación, identificando los riesgos inmediatos que conllevaría.

3.3 ESTRUCTURA ORGANIZACIONAL

El departamento de SIS GSI Billing, está compuesto por 27 personas lideradas por un Jefe y 4 ingenieros Seniors que supervisan las tareas encomendadas a cada ingeniero.

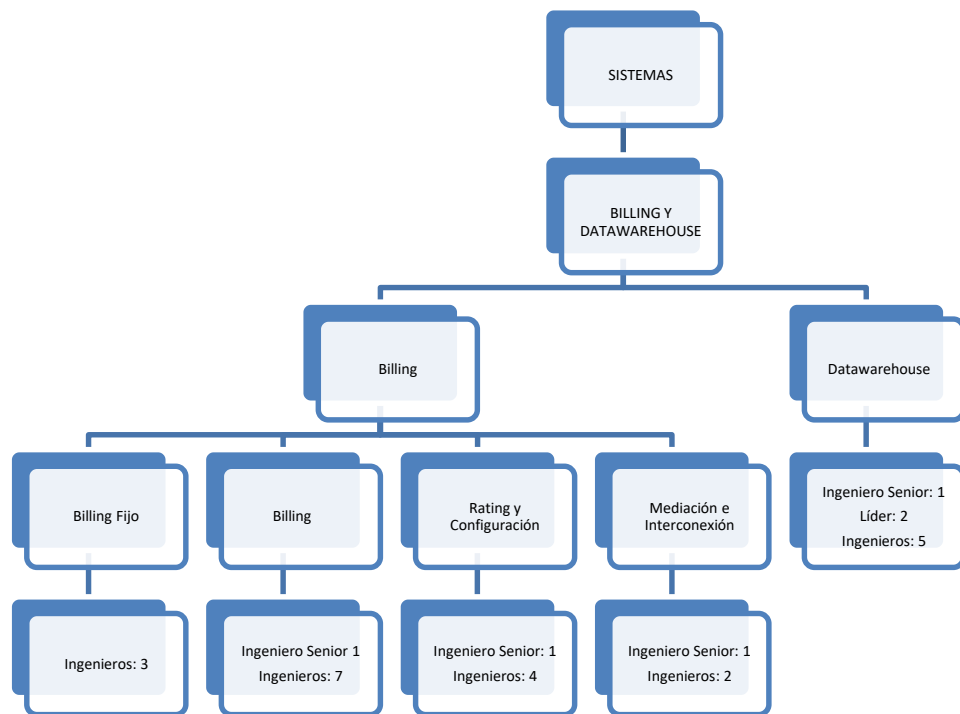


Figura 3.15 Estructura organizacional Fuente: Autor

3.4 ANÁLISIS FODA DEL ÁREA DE SIS GSI BILLING

A continuación, se enlista el FODA del área de Facturación (SIS GSI Billing):



Figura 3.16 Análisis FODA Fuente: Autor

3.5 RECOLECCIÓN DE DATOS

Actualmente la información con que se cuenta para el desarrollo de este proyecto se encuentra parcialmente documentada, incompleta o desactualizada, sobre los procesos realizados dentro de la facturación Postpago y el uso de procedimientos de líneas de comandos en Unix (Shell scripting). Actualmente dichos Shells se

encuentran centralizados en 3 servidores Unix, en donde se ejecutan para los 4 ciclos de facturación existentes. Los pasos necesarios para la ejecución del proceso general de facturación forman parte de un cronograma estructurado en base a acuerdos definidos entre las áreas dentro de la empresa, con límites de tiempos de entrega de información, reportes y archivos necesarios para la continuación de la facturación.

3.5.1 DESCRIPCIÓN DE LAS PRINCIPALES FUNCIONES DEL ÁREA DE SIS GSI BILLING

Entre las principales funciones que tiene el área de facturación (SIS GSI BILLING) se encuentran:

- Cumplir con los ciclos de facturación establecidos por la empresa para los diferentes grupos.
- Programar y coordinar los procesos previos para la correcta ejecución de los ciclos de facturación.
- Ejecutar y controlar los procesos operativos del área (configuraciones - prefacturaciones y facturaciones de servicios)
- Operar la base de datos facturación de Billing, interconexión y roaming para abonados Postpago.
- Diseñar y generar cuadros estadísticos con información generada de la base de datos de facturación y tráfico.

- Dar soporte al área comercial, servicio al cliente y operaciones para el análisis de factibilidad de la facturación de nuevos productos y servicios comercializables.
- Dar soporte al área financiera y comercial en cuanto a análisis de tráfico, supervisión de nuevos y vigentes convenios de interconexión y roaming.
- Dar soporte al área técnica para el análisis y evaluación de nuevas configuraciones y ampliación de la red celular.
- Dar soporte al área de aseguramiento de ingresos y control celular para análisis, diseño y soporte de esquemas para administración de suspended.
- Mantener en archivo los errores que se detecten hasta que se corrijan, realizando seguimiento continuo sobre éstos.
- Llevar controles de calidad requeridos en forma previa y post los procesos de facturación.
- Asegurar que la información generada para las direcciones sea consistente y real de mejoramiento
- Diseñar, desarrollar e implementar productos informáticos necesarios para la labor de mejoramiento continuo de las tareas asignadas
- Evaluar los resultados de los procesos y tendencias de datos críticos e implementa nuevos puntos de control para fortificar la calidad de los resultados.

3.6 ÁREAS PRINCIPALES DENTRO DE SIS GSI BILLING

A continuación, se enlistarán las áreas principales que conforman el área de SIS GSI Billing, las cuales son el área de Billing Fijo, Rating y Configuración, Billing (Postpago) y Mediación e Interconexión. Se dará una breve explicación de las principales funciones y procesos ejecutados.

3.6.1 BILLING FIJO

El área de Billing para productos fijos se encarga de la facturación de servicios tales como televisión por cable, telefonía fija e internet para hogares y para corporativos. El esquema de los procesos aplicados a estos servicios es similar a los utilizados dentro del área de facturación, considerando diferentes ciclos y cronogramas establecidos. La mayor cantidad de funciones realizadas dentro de ésta área están siendo homologadas dentro del área de facturación para Postpago, debido a la centralización de la ejecución de procedimientos en servidores.

3.6.2 CONFIGURACIÓN DE PRODUCTOS Y OFERTAS COMERCIALES. (RATING Y CONFIGURACIÓN)

La creación, desarrollo y ejecución de proceso es llevado a cabo por 4 ingenieros del área de Billing y su función principal es realizar la configuración de las nuevas ofertas comerciales solicitadas por el departamento de Marketing. Las configuraciones solicitadas pueden ser a nivel de la plataforma de facturación (Postpago), plataforma de tasación en línea (prepago y Postpago puro) o modificaciones de las configuraciones existentes.

Para que el requerimiento pueda ser procesado, es necesario que se recpte la información en formatos establecidos (archivos de Excel) y estos son receptados por el área de configuración vía correo electrónico. Este documento debe contener datos básicos para la creación de planes Postpago y considerar muchos atributos necesarios para una correcta configuración en las diferentes plataformas existentes. Cuando se considera que el requerimiento se encuentra completo, se empieza con la configuración de los productos, tanto para prepago como para Postpago. A continuación, se presenta el formato utilizado para la recepción de los requerimientos:

CREACIÓN O ACTUALIZACIÓN DE PLAN CELULAR

Requerimiento No.	999999	Trámite No.	99999999
MOTIVO:	CREACION	Código del Plan:	AB-9999
PRODUCTO	POSTPAGO	Clasificación:	CORPORATIVOS
Segmento Plan:	INDIVIDUAL	Tipo Plan:	DATOS
Tipo Cliente:	ESPECIAL	Categoría Plan:	DATOS
PLAN APLICA CIRCULO CLARO:	SI	Segmento Datos:	ORD
PROMO PREVIA RECARGA	-	CLASIFICACION REGULATORIA	-
Información Básica			
Nombre del Plan	Plan Postpago Multiuso 1	Tarifa Básica VOZ:	0
Tipo de Interconexión	Tarifas planas	Cupo Mensual Final:	3.5
BULK	-	APLICA PARA WEB:	NO
CANTIDAD DE LINEAS:			
Mínimo:	-	Máximo:	-
Nota: El Feature de "Cobro de envío de Estado de Cuenta" se deberá activar cuando el cliente no contrate el feature de "Factura detallada"			
Retenciones / Adendum			
Redirección			

Figura 3.17 Documento de la Creación o Actualización del Plan Celular Fuente: Autor

La tarea se gestionará de acuerdo de lo solicitado; de manera semiautomática (por medio de aplicativos que realizan modificaciones directas en Bases de datos), solicitud de configuración a nivel de la plataforma de tasación en línea y por último, modificación directa a la base de datos.

Creación de Planes

Información Básica Features del Plan Información Costo Tarifa Información de Manejo de Error Tarifas Plan Clon

Creación de Planes Usuario:

Información Básica

Código automatico SI NO Cod Plan Asig.

Código de plan

Nombre Plan asignado

Nombre Corto

Plan

Tipo Plan

Tipo Cliente

Segmento

Toll

Clase

Categoria

Codigo

% Fondo

% Bono

Adendum Finan Plazo Aden

Cant. Min. Linea

Cant. Max. Linea

Cuota Mensual Plan

Tipo plan

Supertel

Segmento

Se reporta

Plan Maestro

SI

NO

Id Subproducto de plan

Figura 3.18 Módulo para la creación de Planes Postpago
Fuente: Autor

Existen configuraciones aplicadas a la facturación en línea (Prepago), las cuales deben ser atendidas por proveedores externos que permiten la funcionalidad de dicho segmento de manera inmediata. A continuación, se presenta el formato utilizado para la configuración de servicios:

CODIGO	DESCRIPCION	SEGMENTO	CANTIDAD	COSTO	COSTO IVA	COSTO ADICIONAL	COSTO ADICIONAL IVA
AB-1	PAQUETE DATOS 1	PREPAGO	10	0	0	0.1000000000	0.114
AB-2	PAQUETE DATOS 2	PREPAGO	20	0	0	0.1000000000	0.114
AB-3	PAQUETE DATOS 3	PREPAGO	30	0	0	0.1000000000	0.114
AB-4	PAQUETE DATOS 4	PREPAGO	40	0	0	0.1000000000	0.114
AB-5	PAQUETE DATOS 5	PREPAGO	50	0	0	0.1000000000	0.114
AB-6	PAQUETE DATOS 6	PREPAGO	60	0	0	0.1000000000	0.114
AB-7	PAQUETE DATOS 7	PREPAGO	70	0	0	0.1000000000	0.114
AB-8	PAQUETE DATOS 8	PREPAGO	80	0	0	0.1000000000	0.114
AB-9	PAQUETE DATOS 9	PREPAGO	90	0	0	0.1000000000	0.114
AB-10	PAQUETE DATOS 10	PREPAGO	100	0	0	0.1000000000	0.114

Figura 3.19 Documento de configuración para la facturación en línea
Fuente: Autor

Todos los pasos antes descritos cambian de manera constantemente y de acuerdo al requerimiento del negocio; existen procesos que son generados diariamente para realizar cambios que no fueron contemplados inicialmente debido a que no existía la funcionalidad solicitada o por cambios en las regulaciones impuestas. Finalmente, luego de que todos los procesos de configuración han terminado, se realizan controles de calidad y validaciones varias dependiendo del tipo de servicio solicitado. En caso de que sean nuevas funcionalidades configuradas, éstas son probadas antes de que los productos salgan a la venta.

3.6.3 FACTURACIÓN

El área de facturación, gestiona, coordina, y audita la facturación de servicios o productos realizada por clientes Postpago y Prepago (en línea). Estos procesos son ejecutados de manera cíclica (Postpago) y es el encargado de administrar diferentes fuentes de información sensible para áreas financieras y técnicas para la continuación y finalización del proceso de facturación del cliente.

Los procesos generados por el área son ejecutados a través de procesos semiautomáticos, es decir, se utilizan aplicativos en entorno Windows, Shells a nivel de sistema operativo y de procedimientos almacenados a nivel de base de datos.

3.6.4 FACTURACIÓN EN LÍNEA (PREPAGO)

La facturación del segmento Prepago se enfoca directamente en la venta y cobro en línea de todos los servicios ofrecidos por la empresa. El control de este cobro es de manera diaria, del cual el área de facturación se encarga de verificar costos en caso de existir problemas reportados por medio de reclamos de clientes. Toda la información generada por este tipo

de segmento es cargada para el área de facturación de manera diaria a nivel de base de datos, dependiendo de los servicios que generen tráfico.

3.6.5 FACTURACIÓN BASADA EN SERVICIOS CONTRATADOS (POSTPAGO) – SECTOR MASIVO

La facturación para el sector Masivo contiene todos los clientes Postpago con planes comerciales, de los cuales se siguen los siguientes pasos para generar su factura:

- Preparación de toda la información maestra de clientes, distribución de valores asignados a los contratos, entre otros. Esta data es almacenada en base de datos, inicialmente transferida desde el servidor maestro hasta el servidor donde se ejecutarán los procesos iniciales. La ejecución de este procedimiento es diaria.
- Ejecución de procesos de control de calidad y análisis de información a ejecutarse; revisión de servicios contratados y fechas de actividad de clientes.
- Inicio de la pre facturación; se validan los procesos antes de la generación de factura. Este paso genera pre facturas cargadas en bases de datos que serán revisadas por procesos internos para la detección de errores y corrección de los mismos.

- Inicio de la facturación; conlleva la ejecución de Shells incluidos en 3 servidores Unix, cerrando el corte de la facturación para áreas como financiero, generando las facturas en diferentes formatos.

3.6.6 FACTURACIÓN BASADA EN SERVICIOS CONTRATADOS (POSTPAGO) – SECTOR CORPORATIVO

La facturación para el sector Corporativo contiene la mayor cantidad de clientes Postpago en contratos masivos, desde 3 clientes hasta más de 4000; el proceso que conlleva la generación de factura, es la siguiente:

- Preparación de toda la información maestra de clientes, distribución de valores asignados a los contratos, entre otros. Esta data es almacenada en base de datos, inicialmente transferida desde el servidor maestro hasta el servidor donde se ejecutarán los procesos iniciales. La ejecución de este procedimiento es diaria.
- Se ejecutan pre procesos de facturación; procesos coordinados que generan subtotal y totales por contrato y cliente. Se involucra el servidor donde se receptaron toda la información maestra, ejecutando Shells de cada proceso y guardando los resultados en tablas almacenadas en base de datos.
- Inicia el control de calidad sobre los pre procesos de facturación (tablas ya generadas), aplicando reglas para clientes especiales.

- Se ejecutan procesos de facturación sobre la data ya normalizada; forma parte del proceso macro de facturación (similar al proceso para Postpago masivo). En este punto, se involucran 3 servidores Unix, 2 bases de datos para el análisis y procesamiento de la información final, terminando dicho proceso en la generación de la factura en varios formatos que serán almacenados para la visualización del cliente final.

3.6.7 CRONOGRAMA DE FACTURACIÓN

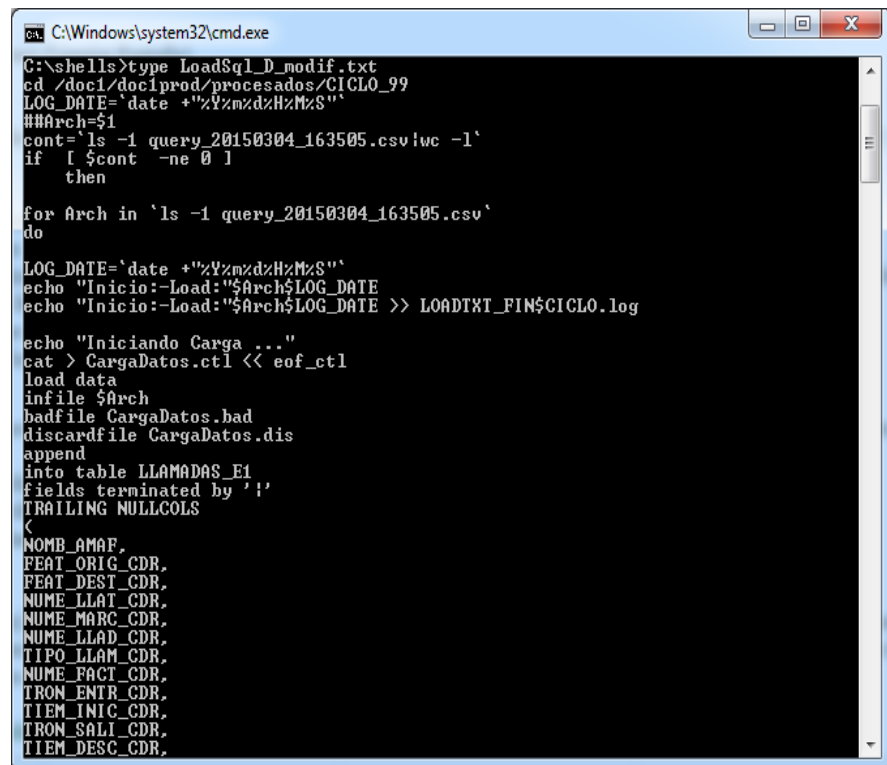
A continuación, se muestra parte del cronograma de facturación para productos corporativos utilizados por el equipo de facturación:

Nombre de tarea	% completado	Duración	Comienzo
31 Renombrar la tabla AUT_BULK_SVA_RTX a AUT_BULK_SVA_RTX_MMDO	100%	1440 mins?	vie 23C
32 Crear la tabla AUT_BULK_SVA_RTX	100%	1440 mins?	sáb 24C
33 Truncar la tabla CL_CONSUMO_TELEFONO	100%	5 mins	dom 25C
34 Respalda la tabla CL_VIDEO_LLAMADA	100%	1440 mins?	dom 25C
35 Verificar todas las tablas vacías y que estén en los tablespaces correctos	100%	5 mins	lun 26C
36 Analizar a tablas de procesos de sumarización	100%	1440 mins?	lun 26C
37 Seguir con el cronograma de actividades diarias	100%	2968 mins	mar 27C
38 EJECUCIÓN DEL SHELL MENU_FACTURACIÓN_BULK_RTXPROD	6%	71726 mins?	mar 22I
39 PROCESO DE FACTURACIÓN	29%	705868 mins?	mar 22I
40 Solicitar a Producción confirmación de cargas BULK SVA hasta el día de corte (DEPENDIENDO DE QUE TERMINE TODO EL FLUJO EN CONTROL-M)	100%	60 mins	sáb 24C
41 Cuentas no Factura que tienen llenadas	100%	15 mins	sáb 24C
42 Ejecutar analize	0%	5 mins	mar 22I
43 Verificar que el proceso de Cargas OCC no haya cargado datos para clientes BUL y TOT (SE REALIZA EN BSCSPROD)	100%	1440 mins?	mar 22I
44 VERIFICAR PROMOCIONES DE CORPORATIVOS (NO EJECUTAR RETARIFICACIÓN SIN VERIFICAR ESTO ANTES)	100%	1440 mins?	mar 22I
45 ESTADÍSTICAS PROMOCIONES DE CORPORATIVOS (NO EJECUTAR RETARIFICACIÓN SIN VERIFICAR ESTO ANTES)	100%	1440 mins?	mar 22I
46 Ejecutar Opción 6 (Retarificación)	0%	1060 mins	mar 22I
47 Sumarizar Consumos y Bonos BULK	0%	240 mins	dom 25C
48 *FREE UNITS	0%	20 mins	dom 25C
49 QC de Verificación de procesamiento de cuentas migradas	0%	1440 mins?	dom 25C
50 Carga de llenadas para ACO	0%	1440 mins	lun 26C
51 Enviar estado de cuentas VIP a ACO	0%	1440 mins?	mar 22I
52 Revisión de Estadísticas de Facturación de Voz BULK	0%	1440 mins?	mar 22I
53 QC Consumos Bulk_Consumo_Mensual Vs Ugr_i_Bulk	0%	5 mins	mar 22I
54 QC tabla BULK_CONSUMO_MENSUAL	0%	20 mins	mié 23I
55 Validación de Promoción de Más Minutos	0%	1440 mins?	mar 22I
56 (*QC de Bono no Aplicado por Cambio de Producto	0%	1440 mins?	mar 22I
57 QC de TB y CP BUL (BUL Y FAM)	0%	20 mins	mié 23I

Figura 3.20 Cronograma de Facturación Fuente: Autor

3.6.8 PROCEDIMIENTOS ALMACENADOS EN UNIX PARA FACTURACIÓN

Se presenta a continuación un ejemplo de los scripts utilizados para la ejecución de procesos internos de facturación:



```

C:\Windows\system32\cmd.exe
G:\shells>type LoadSql_D_modif.txt
cd /doc1/doc1prod/procesados/CICLO_99
LOG_DATE='date +%Y%m%d%H%M%S'
##Arch=$1
cont='ls -l query_20150304_163505.csv!wc -l'
if [ $cont -ne 0 ]
then
for Arch in `ls -l query_20150304_163505.csv`
do
LOG_DATE='date +%Y%m%d%H%M%S'
echo "Inicio:-Load:$Arch$LOG_DATE"
echo "Inicio:-Load:$Arch$LOG_DATE >> LOADTXT_FIN$CICLO.log"

echo "Iniciando Carga ..."
cat > CargaDatos.ct1 << eof_ct1
load data
infile $Arch
badfile CargaDatos.bad
discardfile CargaDatos.dis
append
into table LLAMADAS_E1
fields terminated by '|'
TRAILING NULLCOLS
<
NOMB_AMAF,
FEAT_ORIG_CDR,
FEAT_DEST_CDR,
NUME_LLAT_CDR,
NUME_MARC_CDR,
NUME_LLAD_CDR,
TIPO_LLAM_CDR,
NUME_FACT_CDR,
TRON_ENTR_CDR,
TIEM_INIC_CDR,
TRON_SALI_CDR,
TIEM_DESC_CDR,

```

Figura 3.21 Ejemplo de procedimientos almacenados
Fuente: Autor.

3.6.9 MEDIACIÓN E INTERCONEXIÓN

El área de Mediación e Interconexión se encarga de analizar patrones de comportamiento entre plataformas, formar parte de los ejecutores de nuevas versiones en plataformas de mediación de datos y llevar a cabo funciones de custodios de los registros de cobro de llamadas y servicios para toda la facturación.

3.7 VISIÓN DEL ÁREA DE SIS GSI BILLING

Ser un área referente para toda la compañía, que gestiona y coordina de manera oportuna sus procesos de facturación, procurando reducir al mínimo posibles errores generados durante la ejecución de estos procesos.

3.8 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN.

Para realizar la implementación de controles que aseguren la seguridad de la información, es necesario realizar unos inventarios de los activos y su respectiva valoración de riesgos, para ello se utilizará el modelo de Gestión de Riesgos Magerit [15]. Para el inventario de la información y su respectiva ponderación, se realizó un trabajo conjunto con el propietario de la misma, para el caso del área

de SIS GSI Billing, el propietario de la información que se procesa es el Jefe del departamento.

A continuación, se detallan los activos que se utilizan en el proceso de Facturación.

Tabla 8 Detalle de activos utilizados en el Proceso de Facturación

Área	N°	Activo	Tipo de Activo
FACTURACIÓN	1	Estaciones de trabajo	Hardware
	2	Impresoras	Hardware
	3	S.O servidores	Software
	4	Shells para proceso de facturación	Software
	5	Sistema para reportaría	Software
	6	Correo electrónico	Servicio
	7	Portal para configuración de promociones	Software
	8	Sistema para creación de Productos	Software
	9	Sistema de gestión de tareas	Software
	10	Servicio FTP con proveedores	Servicio
	11	Base de datos	Software
	12	Manuales impresos de usuarios	Soporte documental
	13	Telefonía VOZ/IP	Telecomunicaciones
	14	Red LAN	Telecomunicaciones
	15	Red inalámbrica	Telecomunicaciones
	16	Cámaras de video conferencia	Telecomunicaciones
	17	Ingenieros de planta	Personas
	18	Personal de apoyo	Personas
	19	Capacitadores (líderes de proyectos)	Personas

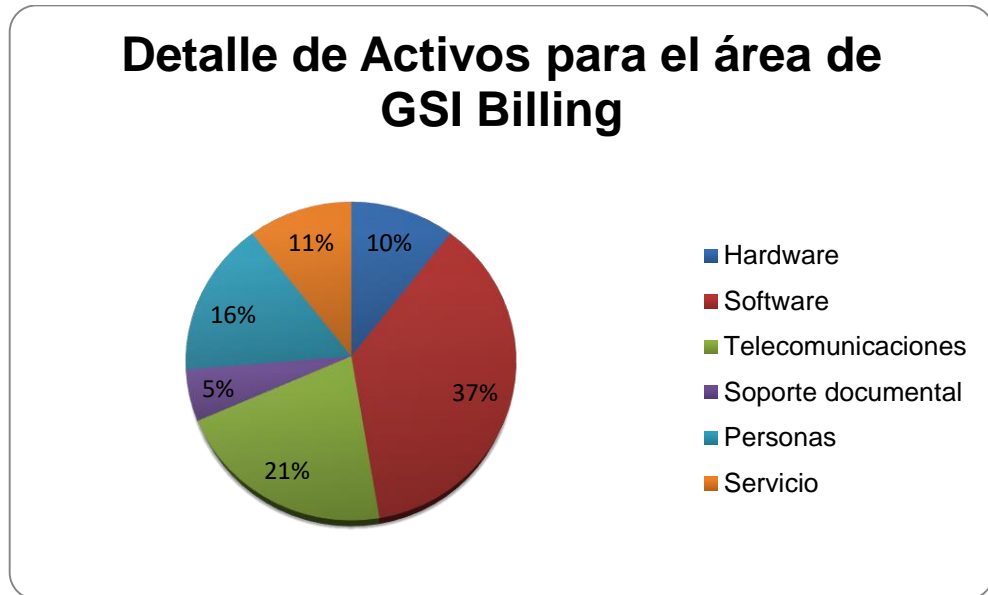


Figura 3.22 Activos para el área de GSI Billing Fuente: Autor.

Como se observa en la gráfica el activo que en su mayoría es manejado por el área de facturación es el software con un 37% en comparación del resto de activos.

3.9 VALORACIÓN DE LOS ACTIVOS

Una vez realizada la identificación de los activos, se debe continuar con la valoración de los mismos; esto debe ser en función de los pilares de la seguridad de información que son: Confidencialidad, Integridad y disponibilidad. La siguiente calificación fue realizada en reuniones con el propietario de los activos.

Tabla 9 Valoración de activos.

Activo	Tipo de activo	Confidencialidad	Integridad	Disponibilidad	Promedio
Estaciones de trabajo	Hardware	2	3	4	3
Impresoras	Hardware	1	1	1	1
S.O servidores	Software	4	4	4	4
Shells para proceso de facturación	Software	4	4	4	4
Sistema para reportería	Software	4	4	4	4
Correo electrónico	Servicio	3	4	3	3,33
Portal para configuración de promociones	Software	3	4	3	3,33
Sistema para creación de Productos	Software	2	2	2	2

Sistema de gestión de tareas	Software	1	1	2	1,33
Servicio FTP con proveedores	Servicio	4	4	4	4
Base de datos	Software	4	4	4	4
Manuales impresos de usuarios	Soporte documental	3	4	2	3
Telefonía VOZ/IP	Telecomunicaciones	3	3	2	2,67

Red LAN	Telecomunicaciones	4	4	4	4
Red inalámbrica	Telecomunicaciones	1	1	1	1
Cámaras de video conferencia	Telecomunicaciones	1	1	1	1
Ingenieros de planta	Personas	3	3	3	3
Personal de apoyo	Personas	4	3	3	3,33
Capacitadores (líderes de proyectos)	Personas	1	1	1	1

3.10 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES.

Las vulnerabilidades es la debilidad que puede ser explotada por una inminente amenaza, una amenaza es vulnerabilidad que tienen los activos o las medidas de protección implementadas que facilitan el éxito de la amenaza.

Es importante reconocer que no todas las vulnerabilidades son idénticas, ya que existen vulnerabilidades que atacan directamente a los activos o bienes de la organización, por lo que su detección y explotación puede significar una gran pérdida económica a la empresa.

Existen vulnerabilidades que afectan a los activos de la empresa, pero no de forma directa, así como existen vulnerabilidades que consiguen informar a los administradores de los sistemas y que pueden ayudar a dar información sobre el atacante.

Se puede recalcar que una vulnerabilidad puede ser crítica si deniega el servicio que da la empresa. Es primordial para la empresa cuando sigue un modelo de seguridad de la información que el trabajo sea realizado; este sea medible y de

igual forma puede ser comparado, caso contrario no se podría evaluar el nivel de evolución real.

En general se debe evaluar al detalle cómo afecta la vulnerabilidad a las funcionalidades del servicio; una vez detectada la vulnerabilidad y si se detecta como crítica se deberá notificar a la brevedad posible para su inmediata corrección.

Para el análisis de vulnerabilidades y amenazas se utilizó como fuente la clasificación basado en Riesgos y amenazas de los sistemas de información geográfica, se consideraron solo las amenazas [18].

Tabla 10 Clasificación Riesgo vs Amenazas

Impacto	10	0	0	0	2	5
	8	0	0	1	6	3
	6	0	0	1	2	0
	4	0	0	1	0	0
	2	0	0	0	0	0
		20%	40%	60%	80%	100%
		Probabilidad				

Tabla 11 Resumen de la clasificación Riesgo vs amenazas

Zona Total: 3	16
Zona Total: 2	4
Zona Total: 1	1

Tabla 12 Calificación de activos y sus riesgos.

Activo	Amenaza	Probabilidad (Porcentaje)	Impacto (Numérico)	Riesgo
Estaciones de trabajo	Corte del suministro eléctrico	60%	4	2,4
	Acceso no autorizado	80%	6	4,8
	Abuso de privilegios de acceso	80%	8	6,4
	Corrupción de la información	100%	8	8
	Destrucción de información	80%	8	6,4
Servidores	Abuso de privilegios de acceso	100%	8	8
	Acceso no autorizado	100%	10	10
	Alteración de la información	100%	10	10
	Caída del sistema por sobrecarga	80%	8	6,4
	Corrupción de la información	80%	10	8
	Errores de configuración	100%	10	10
	Errores de los usuarios	100%	10	10
	Fuga de información	100%	10	10
	Introducción de falsa información	100%	8	8
Shells para proceso de facturación	Alteración de la información	80%	8	6,4
	Abuso de privilegios de acceso	60%	8	4,8
	Robo	80%	8	6,4
	Corrupción de la información	60%	6	3,6

	Destrucción de información	80%	8	6,4
	Errores de configuración	80%	6	4,8
Base de datos	Abuso de privilegios de acceso	80%	10	8
	Alteración de la información	100%	10	10
	Caída del sistema por sobrecarga	40%	4	1,6
	Corrupción de la información	60%	8	4,8
	Destrucción de información	100%	10	10
	Errores de configuración	80%	8	6,4
	Errores de los usuarios	80%	6	4,8
	Fuga de información	80%	6	4,8
	Impresoras	Corte del suministro eléctrico	20%	2
Errores de configuración		20%	2	0,4
Errores de mantenimiento / actualización de equipos (hardware)		60%	2	1,2
Errores del administrador		40%	4	1,6

3.11 PLAN DE IMPLEMENTACIÓN.

Una vez presentada la propuesta para implementar el esquema de seguridad basado en la norma ISO 27002:2005 se espera obtener como resultados:

- Levantar un manual de procedimientos sobre buenas prácticas en el manejo de la seguridad de la información.
- Segmentar las tareas y roles que intervienen en el proceso de Facturación y configuración.
- Concienciar tanto al personal de planta como al personal de apoyo la importancia de conocer, los riesgos a los que se tiene expuesta la información que se procesa.
- Minimizar al máximo los errores operativos.
- Hacer que el personal reporte por medio del correo o del aplicativo los incidentes de seguridad presentados y la solución que fue encontrada.

Para poner en funcionamiento esta propuesta, se ha presentado un cronograma con las tareas a realizar en un plazo no mayor a 10 días.

CAPÍTULO 4.

IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD BASADO EN LA NORMA ISO 27002

El desarrollo de las Políticas de Seguridad informática, basado en la norma ISO 27002 para el área de SIS GSI Billing, es producto del análisis de la situación presente del área, se realizó un estudio de sus procesos, encontrando puntos débiles y sus respectivos controles para mejorar esta situación

A continuación, se detallan los controles con los cuales se realizaron las Políticas de Seguridad para el área de Facturación (SIS GSI Billing), para ello se consideraron los siguientes controle:

- Control de acceso.
- Gestión de incidentes.
- Gestión de Activos.

Las políticas desarrolladas en este trabajo están siendo revisadas por la dirección de Sistemas con carácter confidencial, es decir, que pueden ser objeto a modificaciones y ajustes necesarios para que se alineen con las políticas de seguridad generales.

Una vez se tenga la aprobación del documento, este será custodiado por el departamento de Sistemas, área de GSI Billing.

4.1 GESTIÓN DE ACTIVOS.

Objetivo: "Lograr y mantener una apropiada protección de los activos organizacionales."

Todo activo es de propiedad de la empresa de Telecomunicaciones XYZ, desde el punto de vista de la seguridad de la información debe ser registrado y clasificado para su respectivo control, adicional se debe nombrar a su respectivo propietario.

El propietario de la información deberá ser el custodio de la misma, aplicando según su criterio los controles necesarios para asegurad la integridad, confidencialidad y disponibilidad.

Es importante para una organización inventariar todos sus activos y conocer cuáles son los controles que se aplican de acuerdo a su nivel de importancia.

Por temas de confidencialidad, los activos a ser mencionados no corresponden exactamente a la organización de estudio.

Clasificación de los activos:

La información debe ser protegida a lo largo de su ciclo de vida, desde su creación, procesamiento y mantenimiento, en este sentido es importante tener en consideración la clasificación de la información por su nivel de sensibilidad e importancia.

Activos de información

Se considera activo de información a todo aquello que tenga valor para la organización, por tal motivo debe protegerse; un activo de información es todo aquello que almacena, manipula, transmite información.

Se puede considerar como activos a:

Tangibles: Routers, computadores, archivadores, dispositivos de almacenamientos, etc.

Intangibles: nombre de la empresa, imagen de la empresa, base de datos de cliente, base de datos de proveedores, empleados, etc.

Inventario de los activos

Identificar los activos de información para una organización debe ser de vital importancia, ya que de esta manera se busca clasificar a los activos que requieren mayor atención y protección, de tal forma que se conozcan sus características y rol que tiene en los procesos del negocio.

A más de identificar los activos, estos deben ser documentados; el inventario de los activos ayudará a la organización a incluir la información necesaria y relevante para poder recuperarse de un desastre, es importante que esta información se encuentre en una bitácora y que tenga: ubicación del activo, tipo de activo, información que servirá de respaldo, valor económico, formato del activo.

Propiedad de los activos.

El propietario de la información es el Jefe del área de Facturación, quién deberá llevar el inventario actualizado de la información que maneja su área, este inventario debe incluir:

- Bases de datos que maneja
- Servidores a los que tienen acceso
- Estaciones de trabajo
- Manuales de procesos.
- Archivos
- Contratos
- Documentación del sistema.
- Documentación del facturador.
- Personal que tiene acceso a estos activos.
- Materiales de capacitación
- Aplicaciones para la configuración de Ofertas

- Utilitarios.
- Teléfonos VOZ/IP.
- Impresoras

Custodio de la información

Los custodios de la información serán los Supervisores que tendrán que ser los responsables de los accesos a las bases de datos, servidores; de acuerdo a la gestión que realicen los ingenieros que tienen bajo su supervisión.

El custodio de la información será definido por el Jefe del área quien otorgará los permisos necesarios para el procesamiento de la actividad encargada.

Acceso

Ingenieros: serán quienes tengan acceso al sistema a nivel del servidor, base de datos, previo a la división de funciones (de acuerdo a la gestión que realicen: facturación, configuración de ofertas, etc.) obtendrán los permisos para editar, transformar, conservar o eliminar información que se deposite en los sistemas.

Clasificación de la información.

Clasificar la información tiene como objetivo dar a conocer la importancia que tiene el activo y el nivel de protección adecuada que se debe aplicar. De acuerdo al nivel de importancia y características singulares requerirá un especial manejo.

Para una empresa de Telecomunicaciones el identificar su información de acuerdo a los pilares de la seguridad de la información permitirá a mitigar de manera eficaz alguna eventualidad presentada, por ellos se clasificará de la siguiente manera.

Clasificación de la Información de acuerdo a la Confidencialidad.

La confidencialidad establece que la información no debe ser revelada ni debe estar disponible a personas de otras áreas, personal externo, entidades o procesos que no han sido autorizados.

Tabla 13 Clasificación de la información de acuerdo al confidencialidad

Clasificación de la información de acuerdo al confidencialidad	
Información Reservada	<p>Información disponible únicamente para los procesos internos de área de Facturación</p> <p>La divulgación de esta información puede afectar a los procesos o controles internos del área</p> <p>Puede comprometer una sanción de tipo económica por el ente regulador de las Telecomunicaciones</p> <p>Como información reservada se tiene: Detalle de clientes, valor facturado por mes, detalle de llamadas, etc.</p>
Información Clasificada	<p>Información disponible para los ingenieros del área, es utilizada para los procesos internos del área de Facturación.</p> <p>Esta información puede ser conocida por otros procesos previo autorización del Jefe del área.</p> <p>Como información clasificada se considera: Código fuente de Shells, manuales de configuración, tablas para el procesamiento de información, reporteras, etc.</p>

Información Pública	<p>La información del área o de los procesos ha sido aprobada por la Jefatura del área para su revelación dentro o fuera del área.</p> <p>La divulgación de esta información no afectará al área o a los procesos internos que maneje</p> <p>Información sobre promociones, ofertas comerciales de planes, etc.</p>
No Clasificada	Activos de información que aún no han sido incluidos en el inventario de información, se requiere del análisis para proceder a inventariarlos.

Clasificación de la Información de acuerdo a la Disponibilidad.

De acuerdo a la norma ISO 27001, la información debe estar disponible en el momento y lugar que se requiera por el personal autorizado o por el proceso que requiera del acceso a la misma.

Se realizará una clasificación de acuerdo al nivel de importancia: Alta, media, baja.

Tabla 14 Clasificación de la información de acuerdo a la disponibilidad

Clasificación de la información de acuerdo a la disponibilidad	
Alta	<p>Si la información NO está disponible, puede ocasionar multas por parte del ente regulador de Telecomunicaciones y la imagen de la organización se verá afectada.</p> <p>Se pueden considerar información como: Detalle de facturas, detalle de llamadas, información de precios, costo de productos, etc.</p>
Madia	Si la información NO está disponible, puede ocasionar impacto negativo en cuanto a su imagen, o puede ser objeto de multas moderadas por parte del ente regulador

	Se pueden considerar información como: detalle de equipos en la web, costo de nuevos servicios, etc.
Baja	Si la información no está disponible, puede ocasionar problemas en el procesamiento de las operaciones a nivel interno, no ocasiona impacto legal o económico. Se puede considerar: Gestor de tareas no está en línea, detalle de horarios, etc.

Clasificación de la Información de acuerdo a la Integridad.

La información debe estar íntegra, es decir, no debe sufrir modificaciones, debe ser coherente y precisa; en otras palabras, la información no debe ser modificada por personal no autorizado.

Se realizará una clasificación de acuerdo al nivel de importancia: Alta, media, baja.

Tabla 15 Clasificación de la información de acuerdo a la integridad

Clasificación de la información de acuerdo a la integridad	
Alta	La información que no conserve su integridad puede ocasionar un gran impacto a nivel legal y económico. Si la información no se encuentra íntegra el resultado de la misma no será presentada a los clientes de manera correcta, puede generar pérdida de la imagen de la organización y desconfianza de los clientes. Ejemplo: Facturas con valores incorrectos, mal cobro en servicios, etc.

Media	La información que no conserve su integridad puede ocasionar un impacto moderado a nivel legal y económico. Ejemplo: información engañosa en los medios donde se ofertan los productos.
Baja	La información que no conserve su integridad puede ocasionar un impacto no significativo a nivel legal y económico.

Etiquetado y manejo de la información.

Una vez realizada la clasificación de la información es necesario etiquetarla bajo estos criterios, si bien es cierto existen activos físicos, los cuales podrán ser etiquetados de forma física no obstante los activos electrónicos, necesariamente se tendrá que hacer uso de una aplicación para poder realizar el correcto etiquetado.

Los elementos que deben ser considerados para el etiquetado pueden ser: documentos impresos, guías de usuario, medios de almacenamiento (memorias USB, discos portables, CD, DVD, etc.), correos electrónicos, base de datos, servidores, etc.

De acuerdo a la clasificación se tendrá que definir el tipo de control a ser aplicado que incluyen: almacenamiento, procesamiento, transmisión y hasta destrucción segura del activo.

En este etiquetado también se debe considerar la cadena de custodia; así como la bitacorización de cualquier evento presentado durante el ciclo de vida del activo.

A continuación, se detallarán los campos que debe tener el etiquetado:

Código: Su valor será secuencial y será único, de esta manera se identificará al activo.

Proceso: Se deberá detallar que proceso estará utilizando el activo, es decir, para el caso del área GSI Billing se detallará si el proceso es de Facturación, Configuración, o Tasación, etc.

Nombre del activo: Se definirá si nombre del activo corresponde dentro del proceso al que pertenece.

Observación: Se definirá brevemente la descripción del activo y su uso dentro del proceso al que pertenece.

Tipo: Se definirá si el activo corresponde a hardware, Software, Telecomunicaciones, soporte documental, personas, etc.

Ubicación: Se detallará la ubicación lógica del activo, en el caso de las tablas de trabajo se definirá la base de datos a la que pertenece.

Si el activo se tratara de un bien físico, se detallará la ubicación en la que se encuentra ubicado.

Clasificación: Se definirá de acuerdo a su nivel de importancia considerando su confidencialidad, integridad, y disponibilidad de la información.

Criticidad: Es el cálculo que se realizará cuando se estime el valor del activo, de acuerdo a la clasificación de la información: alta, media o alta.

Propiedad: Se detallará quien es el responsable del activo, en el caso del área de Facturación se deberá indicar como propietario al jefe del departamento de Facturación.

Tabla 16 Etiquetado y manejo de la información

Código	Proceso	Nombre Activo	Observación	Tipo	Ubicación	Confidencia	Integridad	Disponibilidad	Criticidad	Responsable
1	Facturación	Tabla de productos	Almacena el detalle de los productos ofertados por la empresa	Base de datos	BD Fact	Alta	Alta	Alta	Alta	Jefe de Facturación
2	Facturación	Tabla de Clientes	Almacena el detalle de clientes por corte de facturación	Base de datos	BD Fact	Alta	Alta	Alta	Alta	Jefe de Facturación
3	Facturación	Tabla de servicios adicionales	Almacena el detalle de servicios adicionales contratados por los clientes	Base de datos	BD Fact	Alta	Alta	Alta	Alta	Jefe de Facturación
4	Facturación	Tabla de números celulares	Almacena el detalle de contratos por número celular	Base de datos	BD Fact	Alta	Alta	Alta	Alta	Jefe de Facturación
5	Configuración	Tabla de promociones	Almacena el detalle de promociones por mes	Base de datos	BD Conf.	Alta	Alta	Alta	Alta	Jefe de Facturación

4.2 CONTROL DE ACCESO.

Control.

"Se tendrá que establecer, documentar y revisar periódicamente la política de control de acceso de acuerdo a los requerimientos de la organización".

Los controles de acceso son considerados tanto físicos (a nivel de infraestructura) como lógicos (a nivel de sistema), el acceso debe estar establecido tanto para personal interno, personal de apoyo, proveedores de algún servicio.

Para la creación de esta política se deberá considerar el control de acceso tendrá que considerar:

- Creación de perfiles con ciertos privilegios de acceso para las diferentes aplicaciones, servidores y bases de datos.
- Requerimiento de seguridad para cada uno de los sistemas que almacenen información.

Administración de acceso a usuarios.

El área de GSI Billing, a través del Jefe del área establecerá los respectivos procedimientos para la asignación de roles a los usuarios bajo su mando para que tengan acceso a los diferentes sistemas, servicios de información que manejan.

Creación de usuarios.

El jefe del área solicitará a las diferentes áreas (Técnico, seguridad informática, Redes) la creación de un nuevo usuario con su respectivo rol.

Estas áreas tendrán entre sus funciones la creación, modificación o eliminación de usuarios, previo requerimiento del Jefe de Facturación, ellos deberán aplicar los cambios o eliminación de manera inmediata.

Se sugiere que el personal de apoyo tenga una cuenta de usuario creada, ya que por lo general ellos se conectan a la red utilizando sesiones del personal de apoyo, de esta manera ejecutan procesos o realizan modificaciones en las tablas de trabajo y su identificación y auditoría se complica.

Los datos necesarios para acceder a los sistemas deberán estar compuestos por: nombre de usuario, contraseña, una breve descripción del rol que tendrá la persona.

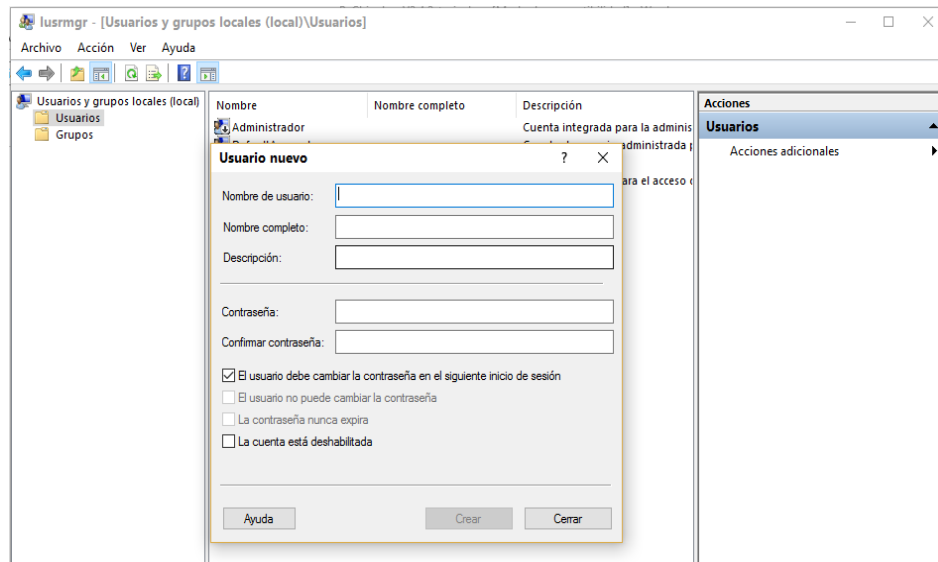


Figura 4.24 Gráfica para la creación de usuarios en Windows. Fuente: Autor

Cuando el personal interno o de apoyo deje de laborar, se deberá comunicar de manera inmediata al departamento de seguridad informática para que la sesión sea inactivada, y se quiten los privilegios de acceso de todos los sistemas de información.

Administración de contraseña de usuarios (Políticas de contraseñas).

Las contraseñas deben tener un mínimo de 8 caracteres.

Las contraseñas deben tener combinaciones de letras mayúsculas, minúsculas, caracteres especiales y números.

La vigencia de cada contraseña debe ser mínimo de 3 meses y no debe permitir el uso de contraseñas históricas.

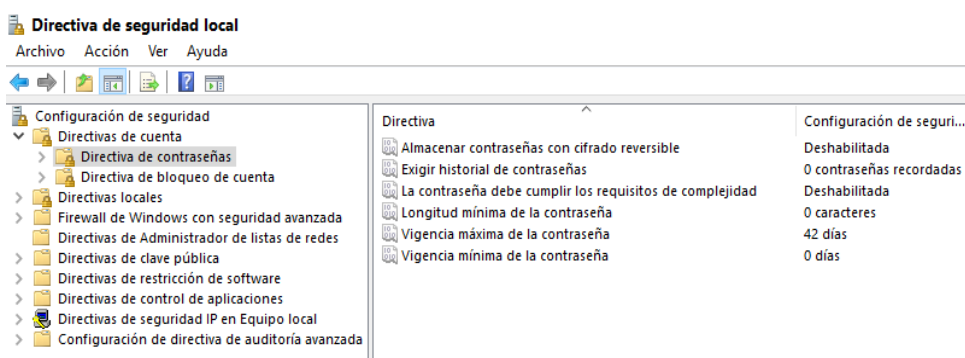


Figura 4.25 Directiva de contraseñas. fuente: Autor.

Uso de contraseñas.

Tanto el personal de planta como personal de apoyo debe cumplir con los siguientes requisitos para el uso de contraseñas.

- Las contraseñas deben ser difíciles de adivinar, pero fáciles de recordar para los ingenieros.
- En el caso de robo, pérdida de las contraseñas se deberá reportar de inmediato al Jefe del departamento.
- Las contraseñas no deben ser basadas en nombres de familiares, fechas de nacimientos, etc.
- Las contraseñas no deben ser compartidas.
- Las contraseñas no deben ser escritas en lugares de fácil acceso.

Estaciones de trabajo desatendidas.

Si el usuario de una estación de trabajo tiene que ausentarse del lugar de trabajo, deberá activar el bloqueo del computador para que terceras personas no tengan acceso a su computador.

Si el sistema detecta inactividad de la sesión en un periodo de 5 minutos, automáticamente deberá bloquearse por time out, y finalizará la sesión del usuario

Oficina cero papeles.

Se debe inculcar al personal sobre la cultura de oficina cero papeles, que consiste en:

- En el puesto de trabajo deben tener documentación que sirva para la gestión de la tarea encomendada.
- Los escritorios deben permanecer cerrados con llave.
- No se debe dejar documentos con información sensible a la vista.
- No se debe utilizar hojas para anotar las contraseñas de acceso.
- Se debe mantener el puesto de trabajo ordenado.
- Todas las estaciones de trabajo deberán ser apagadas al término de la jornada laboral, salvo excepciones especiales y bajo autorización de Gerencia podrán dejarlas encendidas.

Control de autenticación y de identificación de usuarios.

Todos los usuarios sin excepción deberán contar con su respectiva sesión, sean estos: personal de apoyo, personal de planta, programadores, personal técnico.

Esto ayudará a proteger la confidencialidad, integridad de la información ya que de esta manera se evitará el no repudio y la auditoría de la gestión será más eficiente.

Sistema de administración de contraseñas.

Se debe contar con un sistema de administración de contraseñas, que permita:

- Las contraseñas deben ser cifradas
- Se debe configurar el sistema para que permita la actualización de la contraseña una vez se entregue el nuevo usuario.
- Las contraseñas deben ser modificadas en un plazo no mayor a 3 meses.
- El uso de usuarios y contraseñas permitirá determinar responsabilidades en el caso de algún incidente en la seguridad de la información.

Conexiones con límites de tiempo.

Las conexiones remotas deben estar controladas y deben se debe establecer horarios en las conexiones, el acceso al sistema vía remota contempla riesgos significativos, por ello se debe considerar:

- Limitar el tiempo de conexión remota, en horario de oficina, al no existir de forma expresa una orden para la extensión de horarios.

- Se debe llevar una bitácora con el personal que se conecta luego del horario normal de oficina para que se evidencie la autorización de conexión.

Autenticación de usuarios para conexiones remotas.

La autenticación a la red vía remota deberá ser autorizada por el Jefe del departamento de Facturación.

Control de conexión a redes.

La conexión a la red será a través de redes seguras, el personal autorizado tendrá acceso a VPN, o APN según corresponda.

Estos accesos deberán ser actualizables por el área encargada por un periodo de mayor a 3 meses.

4.3 GESTIÓN DE INCIDENTES.

Objetivo: Se debe aplicar un esquema consistente y eficiente para la gestión de posibles incidentes en la seguridad de la información.

Para una empresa de Telecomunicaciones el contar con una eficaz respuesta ante posibles fallas de seguridad, ayudará a la mejora continua de los procesos y a la vez a la protección de sus activos.

Clasificación de incidentes.

La política de gestión de incidentes deberá utilizar un esquema que clasifique los sucesos en la seguridad de la información, la clasificación permitirá elaborar estadísticas para la toma de decisiones a corto o largo plazo.

Al momento de implantar un esquema para la clasificación de incidentes se deberá considerar lo siguiente:

Severidad:

El impacto se podrá medir en factor económico, es decir, cuánto costaría el incidente a nivel monetario, o se podrá determinar el impacto a través de escalas

estas podrían ser alta, media, baja; todo dependerá de la afectación de los servicios.

Tipo:

Se podrá clasificar en categorías que identifiquen las características o funciones que tienen estos activos para los procesos de la organización, estos pueden ser:

- Infección por virus o malware.
- Denegación de servicios.
- Ataques externos o internos
- Acceso no autorizado a los sistemas.
- Revelación de información sensible
- Fuga de información.
- Daño de la información.
- Información no actualizada.
- Mala gestión del conocimiento.
- Uso Indebido de Software.
- Uso Indebido de Usuarios.
- Suplantación de Identidad.
- Modificación no autorizada.
- Perdida o daño de la documentación.

Evento de la seguridad de la información.

Todo suceso presentado en un sistema, servicio de red, que puede presentar una inminente violación a la política de seguridad de la información.

Toda falla a las medidas de seguridad o situación desconocida debe ser considerada como un evento que puede ser relevante a la seguridad.

Incidente de la seguridad de la información.

La ocurrencia de sucesos en la seguridad de información, se ha materializado de tal forma que ocasiona efectos negativos para la organización o para el departamento de facturación.

Ejemplo: robo de código fuente, suplantación de cuentas de usuarios para la realización de un proceso, ejecución de código malicioso a nivel de servidores, etc.

Reportes de incidentes.

Es responsabilidad del personal reportar de manera inmediata cualquier incidente de seguridad que se presente, para ello puede hacer uso de:

- Correo electrónico.
- Intranet (mesa de ayuda).
- Notificación verbal al jefe del área.
- Notificación escrita.
- Notificación vía telefónica

Incidentes de accesos lógicos.

El acceso a los sistemas de información, uso de servicios, uso de equipos de forma no autorizada deberá ser considerada como un incidente de acceso lógico.

- Uso sin autorización de la estación de trabajo.
- Bloqueo imprevisto de la sesión.
- Ejecución de procesos utilizando mi sesión de trabajo.
- Alguien puede conocer mi usuario y contraseña.

En el caso de evidenciar uno de estos eventos se deberá informar al Jefe inmediato con copia al departamento de seguridad informática para que se tomen

los correctivos necesarios y minimizar los posibles fallos en la seguridad de acceso lógico.

Incidente por virus o código malicioso.

Si un servidor o estación de trabajo ha sido infectado por virus, y el funcionamiento del mismo no es el correcto; el personal que tenga conocimiento de este evento deberá reportarlo inmediatamente al departamento de seguridad informática con el fin que se solucione el inconveniente.

Si luego de eliminarlo, el virus o código malicioso reaparece deber ser considerado como una nueva amenaza, el procedimiento deberá ser el mismo.

Incidente por acceso físico.

Es responsabilidad de todo el personal que labora en el área de facturación reportar si identifica el ingreso de personal no autorizado a las instalaciones del área o de toda la organización.

El acceso a las instalaciones de forma no autorizada puede ocasionar graves afectaciones a los equipos que ahí se encuentran, por ello es indispensable que se reporte al área de seguridad del edificio.

Responsabilidades y procedimientos.

El jefe del área de facturación es el responsable de los activos de información que maneja y por ende es el responsable de su protección, conservación, transmisión y comunicación.

Sin embargo, es responsabilidad de todo el personal reportar los incidentes de seguridad al departamento de Seguridad informática.

El responsable de atender el incidente de seguridad deberá categorizar el suceso presentado como:

- Revelación de información sensible
- Fuga de información.
- Daño de la información.
- Información no actualizada.

- Mala gestión del conocimiento.
- Uso Indebido de Software.
- Uso Indebido de Usuarios.
- Suplantación de Identidad.
- Modificación no autorizada.
- Perdida o daño de la documentación.

Bajo este contexto se establecen los respectivos niveles de escalamiento de los incidentes de acuerdo con su criticidad.

Aprender de los incidentes de la seguridad de la información.

Se debe contar con una bitácora dónde se lleve un historial de los eventos presentados y de los controles implantados para mitigar estos incidentes.

Así como una realimentación a todo el personal sobre estos incidentes y la capacitación para prevenir este tipo de incidentes.

El área de Facturación procesa información muy sensible y la probabilidad que existan incidentes de seguridad es muy alto, por ello se debe concienciar a todo el personal para una correcta mejora continua.

CAPÍTULO 5.

DESARROLLO DEL ESQUEMA DE SEGURIDAD PROPUESTO

Como una mejora a la gestión de la seguridad de la información se ha sugerido la puesta a producción de un portal que ayuda a monitorizar la gestión del personal interno y de apoyo.

Este portal Web ayudará a bitacorizar los cambios realizados en las tablas de trabajo, así como monitorizar los accesos realizados a las distintas bases de datos que maneja el área de GSI Billing.

Como fase inicial, el personal de apoyo tendrá que hacer uso de un usuario y contraseña proporcionado por el Jefe del área de facturación, esto con el fin de mejorar la auditoría en los procesos.

A continuación, se explicará la funcionalidad de esta herramienta y los beneficios que se obtendrán al usarlo dentro de la gestión.

Cómo requisito inicial al portal Web, se deberá ingresar usuario y contraseña por el ingeniero del departamento.



Figura 5.26 Ingreso al Sistema GSI Billing Fuente: Autor

Una vez ingresado el usuario y contraseña (mínimo de caracteres 8, con variación de caracteres especiales), se tendrá acceso al portal Web.

Existirán dos tipos de usuarios, Administrador y Usuario invitado, el usuario Administrador tendrá la potestad de realizar:

- Creación/modificación/Eliminación de usuarios
- Ingreso de horarios para los diferentes turnos de facturación.
- Ingreso de incidencias registradas en los procesos realizados.
- Carga de archivos
- Consulta de bitácoras de auditorías.
- Ingreso de noticias.

El usuario invitado tendrá acceso a:

- Consulta de horarios
- Consulta de archivos (manual de operaciones, manual de procesos, etc.)
- Consulta de novedades

La siguiente imagen muestra la interfaz gráfica.

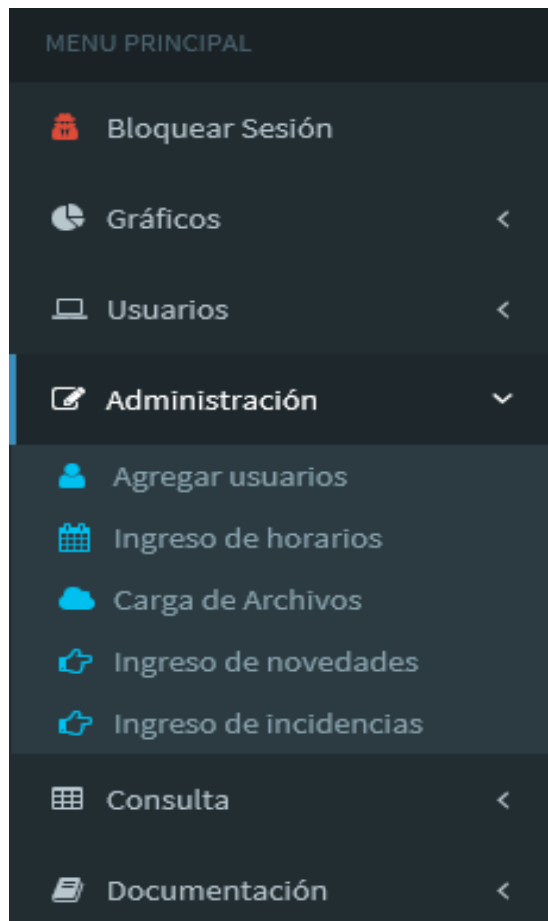


Figura 5.27 Menú de Opciones del Sistema GSI Billing Fuente: Autor

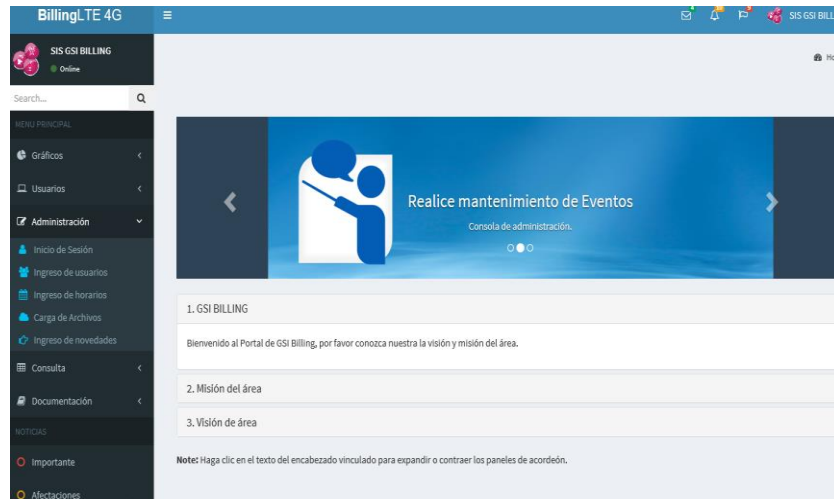


Figura 5.28 Front End Sistema GSI Billing Fuente: Autor


Controles aplicados.

5.1 CONTROL DE ACCESO

El contar con una herramienta en entorno Web ayudará a la administración llevar un control de la hora de ingreso, salida, y seguimiento de las acciones que realiza el personal sobre las tablas de trabajo.

Personal GSIBilling				
#	Nombre	Apellido	Nombre_usuario	Filter
1	JCHICAD	SIS	TEST@MSIA	
2	Jacob	Thornton	TEST1@MSIA	
3	Larry	the Bird	TES2@MSIA	

Figura 5.29 Control de acceso de usuarios Fuente: Autor


Q

Gestion:	SIS Billing
Ingreso:	06/23/2011
Fecha nacimiento:	01/24/1986
User:	XXXX
Género:	Masculino
Dirección:	Guayas, Guayaquil
Email:	test@msia.com
Teléfono de contacto:	0423213445(Casa) 0976232311(Móvil)

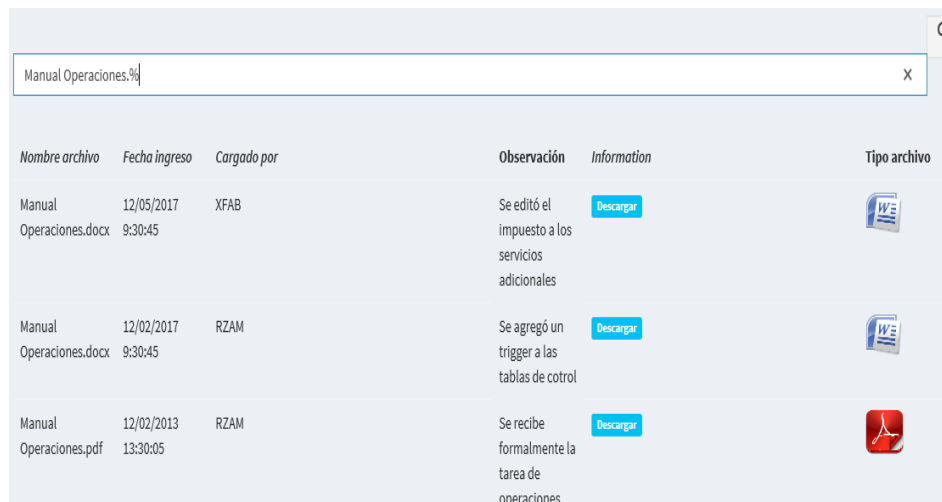
[Regresar](#)

Figura 5.30 Detalle de Registro de un usuario Fuente: Autor

5.2 GESTIÓN DE ARCHIVOS

Una de las mejoras que se realizó fue la creación de un servidor de archivo de tal forma que los diferentes documentos del área no estarán dispersos o en correos de usuarios, ahora estarán en un solo repositorio.

El archivo y su versionamiento será cargado por el Jefe o supervisor del área, una vez cargado se llevará un control de cambios en los archivos, así como la fecha y usuario de carga.






Nombre archivo	Fecha ingreso	Cargado por	Observación	Information	Tipo archivo
Manual Operaciones.docx	12/05/2017 9:30:45	XFAB	Se editó el impuesto a los servicios adicionales	Descargar	
Manual Operaciones.docx	12/02/2017 9:30:45	RZAM	Se agregó un trigger a las tablas de control	Descargar	
Manual Operaciones.pdf	12/02/2013 13:30:05	RZAM	Se recibe formalmente la tarea de operaciones	Descargar	

Figura 5.31 Gestión de Archivos Gsi Billing Fuente: Autor

5.3 GESTIÓN DE CAMBIOS

En este apartado, se explicarán los controles aplicados a nivel de base de datos, ya que fue necesario contar con la aplicación de auditorías a las tablas de trabajo.

Uno de los problemas más comunes que se presentaban en la gestión y procesamiento de facturación electrónica era la aplicación de cambios en registros de las tablas que se utilizan para estos procesos, el personal de apoyo no contaba con una sesión propia y realizaba el uso de sesiones de ingenieros de planta, ocasionando serios problemas al momento de realizar el seguimiento respectivo a la gestión.

Se crearon disparadores en dos tablas de uso cotidiano y que conserva información sensible para el procesamiento de la información, estos disparadores indican si los registros fueron eliminados, modificados o insertados.

Gracias a estos controles se puede identificar el usuario que lo realizó, la dirección IP que lo ejecutó, así como la fecha y hora del cambio.

Si el personal de apoyo, aún no tiene su propio usuario y contraseña, al momento de ingresar al turno, se le destinará una máquina; la asignación de la misma estará a cargo del supervisor.

En el registro contará con la siguiente información:

- Nombre del equipo asignado.
- Fecha y hora del ingreso.
- Nombre de la persona que ingresa a cubrir el turno.

Este registro ayudará a tener un mayor control con los cambios realizados en las tablas de trabajo, de tal forma que se evitará el NO repudio.

En el momento de detectar una anomalía en la actualización, eliminación, o ingreso de un registro se podrá determinar el usuario y la dirección IP de la

máquina que lo ejecutó, así como el propietario de la sesión o en su defecto el personal de apoyo que durante esas horas utilizó el equipo.







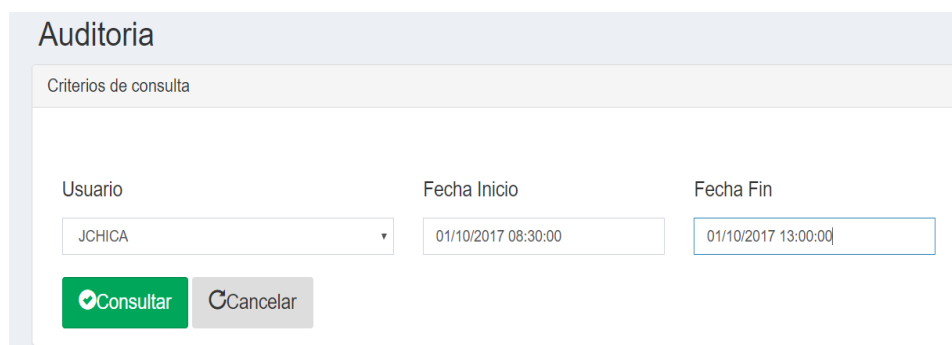
Asignación de Equipo							
IP asignada	Nombre	Estado	Fecha_ingreso	Observac	Fecha_Salida	Tiempo Uso	Acciones
192.168.1.5	PLAR/	Ocupada	10/04/2017 08:30:00	Cubre turno de factur		8:00:29	 
192.168.1.2		Liberar	10/04/2017 08:27:28		10/04/2017 16:30:00	8:02:32	 
192.168.1.6		Libre	10/04/2017 15:27:28		10/04/2017 16:30:00	10/04/2017 14	 

Figura 5.32 Asignación Equipo GSI Billing Fuente: Autor

Una vez que se asegura que el personal de apoyo cuenta con una máquina asignada, el sistema de forma interna capturará las consultas que realice a nivel de base de datos.

Se podrá conocer las tablas que más visita y el tipo de acciones que realiza, con ello se podrá monitorear en línea las actividades que realiza y de esta manera se minimiza la posible fuga de información.

A continuación, se muestra el formulario que facilitará las consultas.



The screenshot shows a web interface titled 'Auditoria'. Below the title is a section labeled 'Criterios de consulta'. It contains three input fields: 'Usuario' with a dropdown menu showing 'JCHICA', 'Fecha Inicio' with the value '01/10/2017 08:30:00', and 'Fecha Fin' with the value '01/10/2017 13:00:00'. At the bottom of the form are two buttons: a green 'Consultar' button with a magnifying glass icon and a grey 'Cancelar' button with a circular arrow icon.

Figura 5.33 Criterios de consulta Fuente: Autor



Figura 5.34 Tablas más consultadas por usuario Fuente: Auto

CAPÍTULO 6

ANÁLISIS DEL ESQUEMA DE SEGURIDAD PROPUESTO

En la actualidad ningún mecanismo de seguridad puede asegurar que se eliminen los riesgos de sufrir ataques cibernéticos o fuga de información, el aplicar controles en sus procesos ayudarán a mitigar en lo posible que la información de la organización se vea comprometida.

El desarrollar un esquema de seguridad basándose en la norma ISO 27002 ayudará a complementar los lineamientos de seguridad que actualmente sigue la empresa.

En reuniones que se han tenido con el Jefe del departamento de Facturación, se han verificado ciertas brechas de seguridad que deben ser corregidas con el fin de reducir los posibles riesgos.

- El área no cuenta con un instructivo de seguridad de la información.
- En los procesos que se siguen para la gestión de facturación no cuenta con un plan de contingencia en caso de errores operativos.
- Es importante que se difunda a todo el personal del área el acuerdo de confidencialidad que existe con las empresas Outsourcing, de esta manera todos serán responsable de que el acuerdo se respete.

Antes de proponer el esquema de seguridad no se tenía control del personal de apoyo y de las actividades asignadas, por ello la necesidad de aplicar estos controles. Para comprobar la efectividad de los controles se expondrán los problemas encontrados en el área, posibles riesgos y la situación mejorada luego de los controles.

PROBLEMA	POSIBLE RIESGO
El personal de apoyo no cuenta con una sesión de usuario configurada, por lo que tiene que "prestar" al personal de plata y de esa manera poder realizar su gestión	Borrado de archivos sensibles en el servidor Alteración de registros en las bases de datos. Envío de correos sin autorización Fuga de información
No existe un sistema de registros para el ingreso del personal de apoyo.	Puede ingresar personal no autorizado Puede realizarse una suplantación de identidad
No existen auditorías en las tablas de trabajo	Borrado de la información y alteración de la información Dificultad para realizar una correcta auditoría
No se cuenta con un sistema para bitacorar cambios en los procesos de Facturación	Errores operativos al ejecutar procesos no actualizados (uso de shells a nivel de servidor) Posibles errores operativos al ejecutar procesos no actualizados a nivel de Base de datos. Errores operativos al ejecutar procesos deshabilitados o en desuso por cambios en las políticas
El área no cuenta con un sistema que alerte amanzas por de 0 days	Pérdida de información por la NO actualización de los sistemas

Figura 5.35 Situación inicial SIS Billing Fuente: Autor

Aplicación de Esquema de Seguridad en Base a la norma ISO 27002:2005	
Software	
	Política para el control de acceso para el control del personal de apoyo Disparadores a nivel de Base de datos para bitacorizar cambios en los registros Política para la autorización o restricción de usuarios a los distintos sistemas
Servicios	
	Plan de contingencia para la continuidad de negocio en caso de errores operativos Política para prevenir los ataques de 0 days
Hardware	
	Política para el control de acceso al área de Facturación. Política para coordinar el mantenimiento de los equipos con el dpto de PCs.

Figura 5.40 Esquema de seguridad Fuente: Autor

A continuación, se describirán 3 casos puntuales en los cuales se ven inmersos los problemas presentados en el área de Facturación, y cuáles son los controles propuestos para corregir y mitigar los posibles fallos de seguridad o errores operativos.

6.1 CREACIÓN DE UN PLAN COMERCIAL (DISPARADORES).

- Actores
- Departamento de MKT
- Supervisor de la unidad de Configuración.
- Ingeniero de Billing.

- Herramientas
- Aplicativo para la creación del plan
- Base de datos para la Configuración.

Para la creación de un plan comercial se cuenta con una secuencia de procesos que son:

- a) Luego de realizar un estudio de mercado, el departamento de MKT crea un nuevo producto (plan celular) y ellos se encargan de diseñar las promociones vinculadas a este plan, es decir, a más de tener una configuración estándar (minutos, SMS, Mb) se añaden ciertos componentes para su comercialización.
- b) El requerimiento es enviado al departamento de SIS Billing a través de un correo electrónico.
- c) El requerimiento es revisado por el supervisor de la unidad de Configuración, quien da su aval para proceder a la configuración del nuevo plan.

- d) Uno de los problemas que se presentan es la falta de definición en los costos de los servicios, estos pueden ser:
- Costos de llamadas
 - Costos por la navegación adicional
 - Falta de definición de las promociones.
- e) Si el requerimiento no está claro, se realiza la devolución del mismo al departamento de MKT.
- f) Una vez MKT realiza la corrección del plan, envía nuevamente el requerimiento vía correo electrónico.
- g) El requerimiento nuevamente es revisado por Supervisor del área y este es aprobado, se asigna un ingeniero de Billing para la configuración del plan.
- h) Para la creación estándar del plan se utiliza un aplicativo de entorno Windows.
- i) El problema encontrado, es que si el plan tiene una característica no contemplada en la forma (aplicativo) el ajuste se tendrá que realizar a nivel de base de datos.

- j) Una vez configurado el plan comercial, se tendrá que añadir distintos componentes antes de liberar el plan comercial.
- k) El problema encontrado es que el añadir estos componentes como: promociones de Mb, SMS, minutos deberán ser añadidos de forma manual a nivel de Base de datos.
- l) Una vez configurado el plan comercial, se libera el detalle al departamento de MKT para que dé su aprobación y el plan sea liberado en producción.
- m) El problema presentado es que no existen auditorías en las tablas de configuración, una vez realizado el plan MKT suele pedir cambios en sus componentes lo que es posible que se realicen esos cambios y no se encuentre quién los realizó.

6.1.1 ROLES QUE INTERVIENEN EN EL PROCESO

Analista de Producto (MKT)

- Realizar estudios de mercado para la creación de nuevos productos.
- Diseñar la estructura para los nuevos planes comerciales.

- Enviar los requerimientos al departamento de SIS GSI Billing respetando los acuerdos de servicios.
- Revisar y aprobar los planes, ofertas comerciales configurados por la unidad de Configuración.

Supervisor de la unidad de Configuración (SIS).

- Revisar los requerimientos enviados por las diferentes áreas.
- Establecer tiempos de respuesta para nuevos requerimientos por parte de MKT.
- Analizar la factibilidad de las nuevas configuraciones solicitadas por el área de MKT.
- Coordinar con los ingenieros la disponibilidad de tiempo para la configuración de las ofertas.
- Administrar al personal de apoyo asignados al proceso de configuración.
- Cumplir con los acuerdos de servicio entre áreas.
- Ingeniero de Billing (unidad de configuración SIS)
- Analizar el requerimiento asignado por el supervisor de la unidad de configuración.
- Validar el requerimiento y notificar si existen novedades no contempladas en el proceso de configuración.

- Realizar la configuración de las ofertas comerciales.
- Notificar la pre producción de las ofertas
- Realizar los ajustes necesarios a las nuevas ofertas comerciales (solicitadas por MKT) antes de liberarlas a producción.
- Realizar el seguimiento necesario a la nueva oferta comercial.

Controles Aplicados.

Frente a los problemas detectados en este proceso, se han aplicado los siguientes controles para disminuir los errores operativos y que sin estos controles la afectación puede ser alta y puede implicar pérdidas económicas considerables.

Tabla 17 Controles Aplicados para los casos de estudio.

AMENAZA	VULNERABILIDAD	CONTROLES
[E.1] Errores de los usuarios	<input type="checkbox"/> E.1.1 Errores por desconocimiento <input type="checkbox"/> E.1.2 Errores por falta de definición <input type="checkbox"/> E.1.3 Error por mal envío del requerimiento	A.10.1.1 Documentación de los procedimientos A.10.7.4 Seguridad de la documentación del sistema
[E.4] Errores de Configuración	<input type="checkbox"/> E.4.1 Errores por ingreso erróneo de datos <input type="checkbox"/> E.4.2 Errores por omisión del proceso	A.10.10.5 Registro de fallos

	<input type="checkbox"/> E.4.3 Errores por no tener un sistema de control de cambios	A.12.2.2 Control de procesamiento interno
[E.15] Alteración accidental de la información	<input type="checkbox"/> Alteración de información autorización <input type="checkbox"/> Alteración de información respaldo <input type="checkbox"/> Alteración de información notificarlo	E.15.1 de sin E.15.2 de sin E.15.3 de sin A.10.7.3 Procedimientos de manipulación de la información A.10.10.1 Registro de auditorías
[E.19] Fuga de información	<input type="checkbox"/> Divulgación de información indiscreción <input type="checkbox"/> Divulgación de información correo <input type="checkbox"/> E.19.1 Robo de información dispositivos electrónicos	E.19.1 de por E.19.2 de por A.10.10.1 Registro de auditorías A.10.10.3 Protección de la información de los registros

6.2 CARGA DE CRÉDITO O DÉBITO (NO REPUDIO).

- Actores
- Departamento de Operaciones
- Supervisor de la unidad de Configuración.
- Ingeniero de Billing.
- Herramientas
- Correo electrónico.
- Base de datos para la Configuración.

Para la realización de esta tarea, se cuenta con las siguientes secuencias de pasos:

- a) El departamento de Operaciones, envía un correo al departamento de GSI Billing para que realicen la carga de créditos a un listado de clientes correspondiente a un corte de facturación.
- b) El requerimiento es analizado por el supervisor del área y él se encargará de asignarlo a un ingeniero (interno o de apoyo).
- c) Debido a que el personal de apoyo trabaja con la sesión de un ingeniero de plata, el requerimiento es enviado a un sólo correo.
- d) Luego de recibido el correo, el ingeniero encargado realizará un insert directo a la base de datos.
- e) El insert realizado servirá como descuento de valores en las facturas de los clientes, de acuerdo al corte de facturación.
- f) El problema presentado es que, pese a que existen auditorias en las tablas, no se lleva una bitácora de quién realmente realizó la tarea, es decir, en la auditoría puede registrar el nombre del ingeniero de planta, cuando en realidad lo generó un ingeniero de apoyo.

6.2.1 ROLES QUE INTERVIENEN EN EL PROCESO

Analista de Créditos y Cobranzas (OPE)

- Realizar el análisis de clientes que aplican para un descuento en sus facturas, por algún cobro indebido, o por promociones o condonación de deudas.
- Generar un listado con el número de cuenta de los clientes y el valor que se debe realizar el descuento.
- Luego de que envían el requerimiento, esperan la confirmación por parte de GSI Billing para dar por cerrada la tarea.
- Supervisor de la unidad de Configuración (SIS).
- Establecer tiempos de respuesta para nuevos requerimientos por parte de OPE.
- Coordinar con los ingenieros la disponibilidad de tiempo para la realización de la tarea.
- Administrar al personal de apoyo asignados al proceso de configuración.
- Cumplir con los acuerdos de servicio entre áreas.
- Ingeniero de Billing (unidad de configuración SIS)
- Analizar el requerimiento asignado por el supervisor de la unidad de configuración.
- Validar el requerimiento y notificar si existen novedades no contempladas en el proceso de carga.

- Realizar la configuración de la carga del crédito.
- Notificar la atención del requerimiento.

Controles Aplicados.

Frente a los problemas detectados en este proceso, se han aplicado los siguientes controles para disminuir los errores operativos y que sin estos controles la afectación puede ser alta y puede implicar pérdidas económicas considerables.

Tabla 18 Controles aplicados para Carga de Crédito o Débito.

AMENAZA	VULNERABILIDAD	CONTROLES
[E.1] Errores de los usuarios	<input type="checkbox"/> E.1.1 Errores por desconocimiento <input type="checkbox"/> E.1.2 Errores por falta de definición <input type="checkbox"/> E.1.3 Error por mal envío del requerimiento	A.10.1.1 Documentación de los procedimientos A.10.7.4 Seguridad de la documentación del sistema
[E.4] Errores de Configuración	<input type="checkbox"/> E.4.1 Errores por ingreso erróneo de datos <input type="checkbox"/> E.4.2 Errores por omisión del proceso <input type="checkbox"/> E.4.3 Errores por no tener un sistema de control de cambios	A.10.10.5 Registro de fallos A.12.2.2 Control de procesamiento interno
[E.7] Deficiencias en la organización	<input type="checkbox"/> E.7.1 Problema al identificar la persona que realizó la actividad.	A10.1.3 Segregación de Funciones A10.2.2 El seguimiento y la revisión de los servicios de terceros
	<input type="checkbox"/> E.7.2 No tener una sesión de invitado para el personal de apoyo.	A11.2.1 Registro de usuarios A11.5.2 Identificación y autenticación de usuarios.
[E.15] Alteración accidental de la información	<input type="checkbox"/> E.15.1 Alteración de información sin autorización <input type="checkbox"/> E.15.2 Alteración de información sin respaldo <input type="checkbox"/> E.15.3 Alteración de información sin notificarlo	A.10.7.3 Procedimientos de manipulación de la información A.10.10.1 Registro de auditorías
[A.5] Suplantación de la	<input type="checkbox"/> A.5.1 Realizar tareas no asignadas con un usuario diferente al asignado.	A11.2.1 Registro de usuarios

identidad del usuario		A11.5.2 Identificación y autenticación de usuarios.
[A.13] Repudio	<input type="checkbox"/> A.13.1 Negación de haber realizado una tarea.	A13.2.1 Responsabilidades y procedimientos

CONCLUSIONES Y RECOMENDACIONES

1. El análisis de los problemas de seguridad ayudó a encontrar vulnerabilidades en los procesos de configuración y de facturación, y a su vez determinar las medidas para mitigarlas.
2. Se determinó que la implementación del Sistema GSI Billing, ayudó a automatizar ciertos procesos que eran consultados a nivel de base de datos, esto mejoró el tiempo en de respuesta para la auditoría en los cambios realizados a nivel de bases de datos.
3. Los controles sugeridos ayudaran a reducir los riesgos encontrados en los procesos que lleva el área de GSI Billing, de esta manera se puede garantizar un buen manejo en el tratamiento de la información.

4. Adicional al software de SIS GSI Billing sugerido, se desarrolló una propuesta para la gestión de Activos, accesos e incidentes que mejorará la custodia de la información.
5. El utilizar la metodología Magerit permitió conocer al detalle sobre las amenazas que pueden estar expuestas las organizaciones a nivel mundial.
6. La gerencia está comprometida a revisar constantemente los controles y las nuevas amenazas que pueden presentarse con el avance de la tecnología y coordinar la inmediata implementación.
7. Es importante que se dé a conocer las políticas implementadas a todo el personal, para concienciar sobre los riesgos que se corren al trabajar con información.
8. Con el paso del tiempo, el área de GSI Billing debe ir actualizando su bitácora de activos de información que poseen para saber el plan de contingencia que debe implementar al momento de ocurrir un incidente de seguridad informática.

RECOMENDACIONES

1. Realizar actualizaciones constantes al sistema GSI Billing, ya que, al crear nuevas estructuras a nivel de base de datos, el sistema quedaría obsoleto y no cumpliría su objetivo.
2. Realizar reuniones semanales para tratar incidentes de seguridad presentados, para conocer cuál fueron las decisiones tomadas y los controles para mitigarlos.
3. Fomentar una cultura de seguridad a nivel interno, para que todo el personal conozca sobre las actividades que se están llevando a cabo para garantizar la seguridad de la información que manejan.
4. Especificar responsabilidades de acuerdo a las tareas realizadas tanto para el personal interno como para el de apoyo, deben conocer en su totalidad la importancia del trabajo que están realizando y lo que implicaría el no hacerlo a cabalidad.
5. Asegurar que el personal del área, sea capacitando constantemente para garantizar que los procesos sean realizados por personal idóneo.

6. Mantener actualizados los manuales de configuración y seguir el esquema propuesto para que esta documentación esté disponible en todo momento.

BIBLIOGRAFÍA

- [1] Hugo del Pozo, Ley Orgánica de Telecomunicaciones del Ecuador,
<https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf>, febrero 2015
- [2] Chano Ibarra, Investigación Descriptiva,
<http://metodologadelainvestigacinsiis.blogspot.com/2011/10/tipos-de-investigacion-exploratoria.html>, octubre 2011
- [3] Fernando Sandoval, Delitos informáticos en Ecuador,
<http://www.eltelegrafo.com.ec/noticias/judicial/13/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario>, agosto 2016
- [4] Camilo Gutierrez, ISO/IEC 27002:2013,
<http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/>, diciembre 2013
- [5] Grupo redex, Clasificación de la información,
<https://www.gruporedex.com.mx/soluciones/administracion-de-la-informacion/>, mayo 2016
- [6] Sara Bursztein, Evolución de incidentes,
<http://www.magazcitum.com.mx/?p=3446#.WKN5Hm997cc>, diciembre 2016

[7] Milenio Digital, Hackeo a Sony Pictures,

http://www.milenio.com/hey/cine/Sony_pictures_ciberataque-

[ex_empleado_Sony_Hackeo_de_estudios_0_436756438.html](http://www.milenio.com/hey/cine/Sony_pictures_ciberataque-ex_empleado_Sony_Hackeo_de_estudios_0_436756438.html), diciembre 2014

[8] Sale Systems, Top 10 principales amenazas,

<http://salesystems.es/10-amenazas-la-seguridad-informatica-debes-evitar/>,

septiembre 2016

[9] Man Red, Gráfico de amenazas,

<http://manred.es/seguridad/>, fecha de consulta Mayo 2016

[10] Camilo Gutiérrez, Diferencia norma ISO 27002:2013,

<http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios->

[dominios-control/](http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/), diciembre 2013

[11] 27001 Academy, ISO 27001,

<https://advisera.com/27001academy/es/que-es-iso-27001/>, fecha de consulta:

Febrero 2017

[12] Laurent Charlet, ISO Survey,

<https://www.iso.org/the-iso->

[survey.html?certificate=ISO%209001&countrycode=AF](https://www.iso.org/the-iso-survey.html?certificate=ISO%209001&countrycode=AF), fecha de consulta marzo

2016

[13] 27001 Academy, Filosofía de la norma ISO 27001,

<https://advisera.com/27001academy/es/que-es-iso-27001/>, fecha de consulta:

Febrero 2017

[14] Isotools, Fases ISO 27001,

<https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf>, fecha de consulta: mayo 2017

[15] Ministerio de hacienda/España, Metodología Magerit,

<https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>, octubre 2012

[16] Carlos Serra, Herramienta para la gestión de Riesgos 31000:2009,

<https://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf>, fecha de consulta octubre 2016

[17] Instituto nacional de estadísticas y Geografía/México, Criterios para valorar la información,

http://sc.inegi.org.mx/repositorioNormateca/Oda2_20Ene16.pdf, diciembre 2015

[18] Duvan Ernesto Castro, Amenazas y su clasificación,

<http://repository.ucatolica.edu.co/bitstream/10983/1305/1/RIESGOS%20AMENAZAS%20Y%20VULNERABILIDADES%20DE%20LOS%20SISTEMAS%20DE%20INFORMACION%20GEOGRAFICA%20GPS.pdf>, 2013

[19] Carolina Álvarez, Clasificación de la información,

https://prezi.com/vhff2y_dllxb/clasificacion-de-activos-de-informacion/, Enero

2014

[20] ISO.ORG, Países con certificación ISO 27001,

[https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&](https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1)

[viewType=1](https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1), fecha de consulta: diciembre 2017

[21] Andalucía, Guía de seguridad informática,

<http://www.blog.andaluciaesdigital.es/guia-de-seguridad-informatica/>, noviembre

2016

ANEXOS

ANEXO 1 SoA 27001

Anexo A de referencia	Título de control	Descripción del control	Se aplica	Observación
A.5	Política de Seguridad			
A5.1	Información Política de Seguridad	Para proporcionar a la dirección de gestión y apoyo a la seguridad de la información de acuerdo con los requerimientos del negocio y las leyes y reglamentos pertinentes.		
A.5.1.1	Documento de Política de seguridad de la información	Un documento de política de seguridad de la información deberá ser aprobado por la administración, y publicado y comunicado a todos los empleados y colaboradores externos.	SI	
A.5.1.2	Revisión de las políticas de seguridad informática	La política de seguridad de la información será revisada a intervalos planificados o si se producen cambios significativos para asegurar su conveniencia, adecuación y eficacia.	SI	
A.6	Organización de la seguridad de la información			
A.6.1	Organización Interna	Para gestionar la seguridad de la información dentro de la organización		
A.6.1.1	Compromiso de la dirección de seguridad de la información	Gestión apoyará activamente a la seguridad dentro de la organización a través de una dirección clara, demuestra el compromiso, la asignación explícita, y el reconocimiento de las responsabilidades de seguridad de la información.	SI	

A.6.1.2	Coordinación de la seguridad de información	Actividades de seguridad de información estarán coordinadas por representantes de diferentes sectores de la organización con un papel relevante y función de trabajo.	SI	
A.6.1.3	La asignación de las responsabilidades de seguridad de la información	Todas las responsabilidades de seguridad de la información deben estar claramente definidas.	SI	
A.6.1.4	Proceso de autorización para instalaciones de procesamiento de información	Un proceso de autorización de la administración para las nuevas instalaciones de procesamiento de información se define y se aplica.	SI	
A.6.1.5	Los acuerdos de confidencialidad	Requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados y revisados con regularidad.	SI	
A.6.1.6	Contacto con las autoridades	Se mantendrán los contactos apropiados con las autoridades pertinentes.	SI	
A.6.1.7	Contacto con grupos de interés especial	Se mantendrán los contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.	NO	Sólo se tendrá acceso a portales de interés, no con personas, manteniendo en reserva la información de la empresa.

A.6.1.8	Revisiones independientes de la política de seguridad de la información	El enfoque de la organización para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se revisará de forma independiente a intervalos planificados, o cuando se producen cambios significativos en la implementación de seguridad se producen.	SI	
A6.2	Partes Externas	Para mantener la seguridad de la información y de las instalaciones de procesamiento de información de la organización que se tiene acceso, procesan, comunican a, o administrados por entidades externas.		
A.6.2.1	Identificación de los riesgos relacionados con los agentes externos	Los riesgos para la información y las instalaciones de procesamiento de información de la organización de los procesos de negocio relacionados con las partes externas deben ser identificados y los controles apropiados implementados antes de conceder el acceso.	SI	
A.6.2.2	Abordar la seguridad cuando se trata de clientes	Todos los requisitos de seguridad identificados deberán dirigirse antes de dar a los clientes el acceso a la información o de los activos de la organización.	SI	
A.6.2.3	Abordar la seguridad en los contratos de terceros	Acuerdos con terceros relacionados con el acceso, tratamiento, la comunicación o la gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de información se referirán a todos los requisitos de seguridad pertinentes.	SI	
A.7	Gestión de Activos			
A.7.1	La responsabilidad de los activos	Para lograr y mantener la protección adecuada de los activos de la organización.		
A.7.1.1	Inventarios de Activos	Todos los activos deben estar claramente identificados y un inventario de todos los activos	SI	

		importantes establecimiento y el mantenimiento.		
A.7.1.2	Propiedad de Activos	Toda la información y los activos asociados a las instalaciones de tratamiento de la información serán propiedad de una parte designada de la organización.	SI	
A.7.1.3	Uso aceptables de los activos	Normas para el uso aceptable de la información y de los activos asociados a las instalaciones de procesamiento de información deberán ser identificados, documentados e implementados.	SI	
A.7.2	clasificación de la información	Para asegurar que la información reciba un nivel adecuado de protección.		
A.7.2.1	directrices de clasificación	La información se clasificará en función de su valor, los requisitos legales, la sensibilidad y criticidad para la organización.	SI	
A.7.2.2	Etiquetado de la información y la manipulación	Un conjunto apropiado de procedimientos para el etiquetado de información y de tramitación se desarrollará y ejecutará de conformidad con el sistema de clasificación adoptado por la organización.	NO	la información no es presentada en forma impresa.
A.8	La seguridad de los recursos humanos			
A.8.1	Antes del Empleo	Para asegurarse de que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades, y son adecuados para las funciones que se consideran para, y para reducir el riesgo de robo, fraude o mal uso de las instalaciones.		
A.8.1.1	Roles y Responsabilidades	Funciones y responsabilidades de los empleados, contratistas y usuarios de terceras partes de protección se definen y documentan de conformidad con la política de seguridad de la información de la organización.	SI	

A.8.1. 2	Proyección	Controles de verificación de antecedentes de todos los candidatos a empleo, contratistas y usuarios de terceras partes se llevarán a cabo de conformidad con las leyes, regulaciones y ética, y proporcional a los requerimientos del negocio, la clasificación de la información que se acceda, y los riesgos percibidos.	SI	
A.8.1. 3	Terminos y condiciones del empleo	Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes se pondrán de acuerdo y firmar los términos y condiciones de su contrato de trabajo, en el que expondrá y responsabilidades de sus de la organización para la seguridad de la información.	SI	
A.8.2	Durante el empleo	Para asegurar que todos los empleados, contratistas y usuarios de terceras partes son conscientes de la información amenazas y preocupaciones, sus responsabilidades y obligaciones de seguridad, y están equipados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, y para reducir el riesgo de error humano.		
A.8.2. 1	Gestion de responsabilidades	Administración exigir a los empleados, contratistas y usuarios de terceras partes para aplicar la seguridad de conformidad con las políticas y procedimientos de la organización establecidas	SI	
A.8.2. 2	Concienciación sobre la seguridad de la información, la educación y la formación	Todos los empleados de la organización y, en su caso, los contratistas y usuarios de terceras partes, deberán recibir una capacitación adecuada sensibilización y actualizaciones regulares en las políticas y procedimientos de la organización, que sea relevante para su función de trabajo.	SI	
A.8.2. 3	Proceso Dicipinario	Habrà un proceso disciplinario formal para los empleados que han cometido una infracción de seguridad.	SI	

A.8.3	El termino o cambio de empleo	Para asegurarse de que los empleados, contratistas y usuarios de terceras partes salen de una organización o el cambio de empleo de una manera ordenada.		
A.8.3.1	Termino de responsabilidades	Las responsabilidades para la realización de la terminación del empleo o cambio de empleo, deberán estar claramente definidas y asignadas.	SI	
A.8.3.2	Retorno de los activos	Todos los empleados, contratistas y usuarios de terceras partes deberán devolver todos los activos de la organización en su poder a la terminación de su empleo, contrato o acuerdo.	SI	
A.8.3.3	Eliminacion de los derechos de acceso	Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes a las instalaciones de procesamiento de la información y de la información del reglamento será eliminado después de la terminación de su empleo, contrato o acuerdo, o se ajustan al cambio.	SI	
A.9	La seguridad física y ambiental			
A9.1	Areas Seguras	Para prevenir el acceso no autorizado físico, daños e interferencia a las instalaciones y la información de la organización.		
A9.1.1	Perímetro de seguridad física	Perímetros de protección se utilizarán (barreras tales como paredes, puertas de entrada de la tarjeta controlada o mostradores de recepción tripulados) para proteger áreas que contienen las instalaciones de procesamiento de la información y de la información.	SI	
A9.1.2	Controles de entradas físicas	Las áreas seguras quedará protegido por entrada apropiada controles para asegurarse de que se les permite el acceso sólo el personal autorizado ..	SI	

A9.1.3	Asegurar oficinas, salas e instalaciones	La seguridad física de las oficinas, habitaciones e instalaciones, se diseñó y aplicó	SI	
A9.1.4	La protección contra amenazas externas y ambientales	La protección física contra daños por incendio, inundación, terremoto, explosión, disturbios civiles, y otros tipos de catástrofes naturales o de origen humano debe ser diseñado y aplicado.	SI	
A9.1.5	Trabajar en zonas seguras	Protección física y pautas para el trabajo en las áreas de seguridad deben ser diseñadas y aplicadas.	SI	
A9.1.6	Zonas de acceso público, de entrega y de carga	Los puntos de acceso, tales como las zonas de entrega y de carga y otros puntos en los que las personas no autorizadas puedan entrar los locales se deberán controlar y, si es posible, aislada de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	SI	
A9.2	Seguridad de los equipos	Para evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las actividades de la organización.		
A9.2.1	Emplazamiento y Protección del equipo	El equipo deberá estar situado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.	SI	
A9.2.2	Apoyo a los servicios públicos	El equipo deberá estar protegida contra fallas de energía y otras interrupciones causadas por fallas en el apoyo a los servicios públicos.	SI	
A9.2.3	seguridad del cableado	Energía y telecomunicaciones cableado que transporta datos o el apoyo a los servicios de información deben estar protegidos contra la interceptación o daño.	SI	
A9.2.4	El mantenimiento del equipo	El equipo debe mantenerse correctamente para permitir su continua disponibilidad e integridad.	SI	
A9.2.5	Seguridad de los equipos fuera de las instalaciones	Seguridad se aplicará a los equipos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de los locales de la organización.	SI	

A9.2. 6	La eliminación segura o de re-uso de equipos	Todos los elementos del equipo que contiene los medios de almacenamiento deberán ser evaluados para verificar que los datos sensibles y el software con licencia se ha eliminado o sobrescrito de forma segura antes de su eliminación.	SI	
A9.2. 7	Eliminación de los equipos	Equipo, la información o el software no se tomarán fuera del sitio sin la previa autorización.	SI	
A10	Gestión de Comunicación y Operaciones			
A10.1	Procedimientos y responsabilidades operacionales	To ensure the correct and secure operation of information processing facilities.		
A10.1 .1	Procedimientos operacionales, adecuadamente documentados	Los procedimientos de operación deberán ser documentados, mantenidos y puestos a disposición de todos los usuarios que los necesitan.	SI	
A10.1 .2	Gestión del Cambio	Los cambios en las instalaciones y los sistemas de procesamiento de información deben controlarse.	SI	
A10.1 .3	La segregación de funciones	Deberes y áreas de responsabilidad deben estar separados para reducir las oportunidades de modificación o mal uso de los activos de la organización no autorizado o involuntario.	SI	
A10.1 .4	Separación de desarrollo, prueba e instalaciones operacionales	Estarán separadas de desarrollo, prueba e instalaciones operacionales para reducir el riesgo de acceso no autorizado o alteraciones en el sistema operativo.	NO	los desarrolladores, podrán realizar pruebas en el área de producción
A10.2	Gestión de entrega de servicios de terceros	Para implementar y mantener el nivel adecuado de seguridad de la información y la prestación de servicios en línea con los acuerdos de prestación de servicios de terceros.		

A10.2 .1	Servicio de entrega	Se velará por que los controles de seguridad, las definiciones de servicio, y los niveles de envío incluidos en el tercer acuerdo de prestación de servicios del partido se implementan, operado y mantenido por el tercero.	SI	
A10.2 .2	El seguimiento y la revisión de los servicios de terceros	Los servicios, los informes y los registros proporcionados por el tercero deberán ser controlados regularmente y revisados, y las auditorías se llevarán a cabo con regularidad.	SI	
A10.2 .3	Gestión de cambios en los servicios de terceros	los cambios en la prestación de servicios, incluido el mantenimiento y la mejora de las actuales políticas de seguridad de información, procedimientos y controles, se gestionarán, teniendo en cuenta la criticidad de los sistemas y procesos que intervienen empresas y re-evaluación de los riesgos.	SI	
A10.3	Planificación y aceptación del sistema	Para minimizar el riesgo de fallo de los sistemas.		
A10.3 .1	gestión de la capacidad	El uso de los recursos deberá ser monitoreada, afinado, y proyecciones de las futuras necesidades de capacidad para asegurar el rendimiento del sistema requerido.	SI	
A10.3 .2	la aceptación del sistema	Los criterios de aceptación para los nuevos sistemas de información, actualizaciones y nuevas versiones serán establecidos y las pruebas adecuadas del sistema) llevaron a cabo durante el desarrollo y antes de la aceptación.	SI	
A10.4	Protección contra código malicioso y móvil	Para proteger la integridad del software y la información.		
A10.4 .1	Controles contra código malicioso	Se llevarán a cabo la detección, prevención y recuperación controles de protección contra código malicioso y los procedimientos apropiados de sensibilización usuario.	SI	

A10.4 .2	Controles contra códigos móviles	Cuando se autorice el uso de código móvil, la configuración deberá garantizar que el código móvil autorizado opera de acuerdo con una política de seguridad claramente definido, y el código móvil no autorizado puede ser impedido de ejecutar.	NO	Al momento no se han implementado códigos móviles.
A10.5	Back-up	Para mantener la integridad y la disponibilidad de instalaciones de procesamiento de la información y de la información.		
A10.5 .1	Información back-up	Copias de respaldo de la información y software serán tomadas y analizadas con regularidad de acuerdo con la política de copia de seguridad acordado.	SI	
A10.6	Gestión de la seguridad de la red	Para garantizar la protección de la información en las redes y la protección de la infraestructura de apoyo.		
A10.6 .1	controles de red	Redes se gestionarán adecuadamente y controlados, con el fin de protegerse de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	SI	
A10.6 .2	Seguridad de los servicios de red	Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red deben ser identificados e incluidos en cualquier acuerdo de servicios de red, si estos servicios se ofrecen en la empresa o subcontratado.	SI	
A10.7	manejo del soporte	Para evitar la divulgación no autorizada, modificación, eliminación o destrucción de bienes, y la interrupción de las actividades comerciales.		
A10.7 .1	Gestión de soportes extraíbles	Deberá haber procedimientos establecidos para el manejo de los medios extraíbles.	SI	
A10.7 .2	La eliminación de los medios de comunicación	Medios deberán ser desechados de forma segura y sin peligro cuando ya no sea necesario, utilizando procedimientos formales.	SI	

A10.7 .3	Información del manejo de los procedimientos	Los procedimientos para el manejo y almacenamiento de la información se establecerán para proteger esta información contra su divulgación o uso no autorizado.	SI	
A10.7 .4	Seguridad de la documentación del sistema	Documentación del sistema deben estar protegidos contra el acceso no autorizado.	SI	
A10.8	Intercambio de información	Para mantener la seguridad de la información y software intercambiado dentro de una organización y con cualquier entidad externa.		
A10.8 .1	Las políticas y los procedimientos de intercambio de información	Políticas formales de cambio, los procedimientos y los controles deberán estar en su lugar para proteger el intercambio de información mediante el uso de todo tipo de instalaciones de comunicación.	SI	
A10.8 .2	Los acuerdos de intercambio	Los acuerdos se establecieron para el intercambio de información y software entre la organización y las partes externas.	SI	
A10.8 .3	Medios físicos en tránsito	Los medios que contienen información deben estar protegidos contra el acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.	SI	
A10.8 .4	Mensajería Electrónica	Información involucrado en la mensajería electrónica será debidamente preservado.	SI	
A10.8 .5	Sistemas de información de negocios	Las políticas y procedimientos deberán ser desarrollados e implementados para proteger la información asociada a la interconexión de los sistemas de información de negocios.	SI	
A10.9	Servicios de comercio electrónico	Para garantizar la seguridad de los servicios de comercio electrónico, y su uso seguro.		
A10.9 .1	Comercio Electrónico	Información involucrado en el comercio electrónico que pasa a través de redes públicas, serán protegidos de la actividad fraudulenta, disputa de contrato, y la divulgación y modificación no autorizada.	SI	

A10.9 .2	Transacciones On-line	Información involucrada en las transacciones en línea deberán estar protegidos para prevenir la transmisión incompleta, mal enrutamiento, alteración mensaje no autorizado, la divulgación no autorizada, la duplicación de mensajes no autorizada o la reproducción.	SI	
A10.9 .3	Información pública	La integridad de la información puesta a disposición de un sistema de acceso público debe ser protegido para evitar la modificación no autorizada.	SI	
A10.1 0	Monitoreo	Para detectar las actividades de procesamiento de información no autorizados.		
A10.1 0.1	Registro de Auditoria	Los registros de auditoría de grabación de las actividades del usuario, excepciones y eventos de seguridad de información se producen y se conservarán durante un período acordado para ayudar en futuras investigaciones y la vigilancia del control de acceso.	SI	
A10.1 0.2	Uso del sistema de monitoreo	Procedimientos para el uso de vigilancia de las instalaciones de procesamiento de información se establecerán y los resultados de las actividades de seguimiento de revisiones regulares.	SI	
A10.1 0.3	Protección de los registros de información	Instalaciones de registro y la información de registro se protegerán contra la manipulación y acceso no autorizado.	SI	
A10.1 0.4	Administración y operación de los registros de información	Actividades del administrador del sistema y gestor de la red se registrarán.	SI	
A10.1 0.5	Fallo de Registros	Fallos se registrarán, analizarán y tomarán las medidas correspondientes.	SI	
A10.1 0.6	Sincronización de Relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o dominio de seguridad se pueden sincronizar con una fuente horaria exacta acordado.	SI	
A11	Control de Acceso			

A11.1	Requerimiento de negocio de control de acceso	Para controlar el acceso a la información.		
A11.1 .1	Política de control de acceso	Se establecerá una política de control de acceso, documentado y revisado basado en los requisitos empresariales y de seguridad para el acceso.	SI	
A11.2	Gestión de acceso de los usuarios	Para garantizar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.		
A11.2 .1	Registro de Usuarios	Habrà un registro de usuario formal y procedimiento de la matrícula en el lugar para otorgar y revocar el acceso a todos los sistemas y servicios de información.	SI	
A11.2 .2	Administración de Privilegios	La asignación y el uso de los privilegios se limitarán y controlados.	SI	
A11.2 .3	Administración de Password de Usuarios	La asignación de contraseñas se controla a través de un proceso de gestión formal.	SI	
A11.2 .4	Revisión de los derechos de acceso de usuario	La dirección revisará los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.	SI	
A11.3	Responsabilidades de los usuarios	Para prevenir el acceso no autorizado de usuarios, y el compromiso o el robo de las instalaciones de procesamiento de la información y de la información.		
A11.3 .1	Utilización de Contraseña	Los usuarios estarán obligados a seguir las buenas prácticas de seguridad en la selección y uso de contraseñas.	SI	
A11.3 .2	Equipo de usuarios desatendido	Los usuarios deberán asegurarse de que el equipo desatendido tiene la protección adecuada.	SI	
A11.3 .3	Política de escritorio y pantalla en blanco o despejado	Se adoptarán una política de escritorio limpio de papeles y soportes de almacenamiento extraíbles y una política de la pantalla clara para las instalaciones de procesamiento de información.	SI	
A11.4	Control de acceso de red	Para prevenir el acceso no autorizado a los servicios en red.		

A11.4 .1	Política sobre el uso de los servicios de red	Los usuarios sólo deberán disponer de acceso a los servicios que han sido específicamente autorizados para su uso.	SI	
A11.4 .2	Autenticación de usuario para las conexiones externas	Métodos de autenticación adecuados se utilizan para controlar el acceso de usuarios remotos.	SI	
A11.4 .3	Identificación de los equipos en las redes	Identificación automática de los equipos se considerará como un medio para autenticar las conexiones de los lugares y equipos específicos.	SI	
A11.4 .4	Diagnóstico remoto y protección puerto de configuración	Se controlará el acceso físico y lógico a los puertos de diagnóstico y configuración.	SI	
A11.4 .5	Segregación en redes	Grupos de servicios de información, los usuarios y los sistemas de información deberán estar separados de las redes	SI	
A11.4 .6	Control de la conexión de red	Para las redes compartidas, especialmente aquellas que se extienden a través de fronteras de la organización, la capacidad de los usuarios para conectarse a la red se limitará, en línea con la política y los requisitos de las aplicaciones de negocio de control de acceso (véase 11.1).	SI	
A11.4 .7	Control de Ruta de red	Controles de enrutamiento se aplicarán a las redes para garantizar que las conexiones de la computadora y los flujos de información no infringen la política de control de acceso de las aplicaciones de negocio.	SI	
A11.5	Control de acceso del sistema operativo	Para prevenir el acceso no autorizado a los sistemas operativos.		
A11.5 .1	Procedimientos de Inicio Seguro	El acceso a los sistemas operativos se controla mediante un procedimiento de inicio de sesión seguro.	SI	
A11.5 .2	Identificación y autenticación de usuarios	Todos los usuarios deben tener un identificador único (ID de usuario) sólo para su uso personal, y una técnica de autenticación adecuados serán elegidos para corroborar la identidad declarada de un usuario.	SI	

A11.5 .3	Sistema de gestión de contraseñas	Sistemas de gestión de contraseñas serán interactivos y se asegurarán de contraseñas de calidad.	SI	
A11.5 .4	Uso de las utilidades del sistema	El uso de programas utilitarios que podrían ser capaces de sistema y de aplicación controles primordiales será restringido y estrechamente controlado.	SI	
A11.5 .5	Sesión de tiempo de espera	Sesiones inactivas se cerrarán después de un período definido de inactividad.	SI	
A11.5 .6	Limitación de tiempo de conexión	Las restricciones a los tiempos de conexión se utilizan para proporcionar seguridad adicional para aplicaciones de alto riesgo.	NO	las sesiones a nivel de servidor no debería caducar.
A11.6	El control de aplicaciones y acceder a información	Para prevenir el acceso no autorizado a la información contenida en los sistemas de aplicación.		
A11.6 .1	Restricción de acceso Información	El acceso a las funciones de información y sistemas de aplicaciones por los usuarios y el personal de apoyo se limitará de acuerdo con la política de control de acceso definido.	SI	
A11.6 .2	Aislamiento del sistema Sensible	Sistemas sensibles deben tener un (aislado) entorno informático dedicado.	SI	
A11.7	Computadores Móviles y Teletrabajo	Para garantizar la seguridad de la información cuando se utilizan las instalaciones de computación y teletrabajo móvil.		
A11.7 .1	Computadores Móviles y comunicaciones	Una política formal deberá estar en su lugar, y se adoptará medidas de seguridad para proteger contra los riesgos del uso de las instalaciones de computación móvil y la comunicación.	SI	
A11.7 .2	Teletrabajo	Una política, planes y procedimientos operativos deberá ser desarrollado e implementado para las actividades de teletrabajo.	SI	

A12 Adquisición de sistemas de información, desarrollo y mantenimiento				
A12.1	Los requisitos de seguridad de los sistemas de información	Para asegurar que la seguridad es una parte integral de los sistemas de información.		
A12.1.1	Análisis de los requisitos de seguridad y las especificaciones	Declaraciones de los requerimientos del negocio para los nuevos sistemas de información, o mejoras de los sistemas de información existentes especificarán los requisitos para los controles de seguridad.	SI	
A12.2	Procesamiento correcto en aplicaciones	Para evitar errores, la pérdida, modificación o mal uso de la información en la aplicación no autorizada.		
A12.2.1	Validación de Datos de Entrada	La entrada de datos a las aplicaciones deberá ser validado para asegurarse de que esta información es correcta y apropiada.	SI	
12.2.2	Control del procesamiento interno	Comprobaciones de validación deberán ser incorporados en las aplicaciones para detectar cualquier corrupción de la información a través de los errores de procesamiento o actos deliberados.	SI	
12.2.3	Integridad de los mensajes	Requisitos para garantizar la autenticidad y la protección de la integridad del mensaje en las aplicaciones deben ser identificados, y los controles apropiados identificados e implementados.	SI	
12.2.4	Validación de datos de salida	La salida de datos desde una aplicación deberá ser validado para asegurarse de que el procesamiento de la información almacenada es correcta y adecuada a las circunstancias.	SI	se debe realizar el respectivo control de calidad
A12.3	Controles criptográficos	Para proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos.		
A12.3.1	Política sobre el uso de controles criptográficos	Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollado e implementado	SI	

12.3.2	Gestión de claves	Gestión de claves estará en el lugar para apoyar el uso de la organización de las técnicas criptográficas.	SI	
A12.4	Seguridad de los archivos del sistema	Para garantizar la seguridad de los archivos del sistema		
A12.4 .1	Control del Software Operacional	Habrán procedimientos para controlar la instalación de software en los sistemas operativos	SI	
A12.4 .2	Protección de los datos de prueba del sistema	Los datos de prueba deben seleccionarse cuidadosamente y protegidos y controlados.	SI	
A12.4 .3	Control de acceso al código fuente del programa	El acceso al código fuente del programa se limitará.	SI	no debe estar al alcance de todos.
A12.5	Seguridad en desarrollo y soporte de procesos	Para mantener la seguridad de software de sistema de aplicación y la información.		
A12.5 .1	Procedimientos de control de cambio	La implementación de los cambios se controla mediante el uso de procedimientos formales de control de cambios.	SI	se debe bitacorar
A12.5 .2	Revisión técnica de aplicaciones después de cambios en el sistema operativo	Cuando se cambian los sistemas operativos, aplicaciones críticas de negocio deben ser revisados y probados para asegurar que no hay impacto negativo en las operaciones de la organización o de la seguridad.	SI	
A12.5 .3	Restricciones en los cambios a los paquetes de software	Las modificaciones a los paquetes de software se pondrán trabas, otros, las modificaciones necesarias, y todos los cambios deben ser estrictamente controlados.	SI	
A12.5 .4	filtración de información	Se impedirá Oportunidades para la fuga de información.	SI	se deberá bloquear los puertos usb para evitar la fuga de información.

A12.5 .5	Desarrollo de software externalizado	Desarrollo de software externalizado será supervisado y controlado por la organización	SI	existirá un lider para cada proyecto, será el encargado de garantizar el correcto desarrollo del mismo.
A12.6	Gestión de Vulnerabilidades Técnica	Para reducir los riesgos derivados de la explotación de las vulnerabilidades técnicas publicadas.		
A12.6 .1	Control de las vulnerabilidades técnicas	La información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan se obtienen, la exposición de la organización a tales vulnerabilidades evaluado y tomado las medidas adecuadas para hacer frente a los riesgos asociados.	SI	
A13	Gestión de incidentes de seguridad de información			
A13.1	Informar sobre los eventos de seguridad de información y debilidades	Para garantizar la seguridad de la información de eventos y debilidades asociadas a los sistemas de información se comunican de una manera que permite acciones correctivas oportunas que deban tomarse.		
A13.1 .1	Informar sobre los eventos de seguridad de información	Los eventos de seguridad de información se comunicarán a través de canales de gestión adecuadas tan pronto como sea posible.	SI	Se debe bitacorar cada incidente presentado.
A13.1 .2	Informes debilidades de seguridad	Todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información estarán obligados a observar y reportar cualquier debilidad de seguridad que observen o sospechen en los sistemas o servicios.	SI	

A13.2	Gestión de incidentes de seguridad de la información y mejoras	Para garantizar un enfoque coherente y eficaz se aplica a la gestión de incidentes de seguridad de la información.		
A13.2.1	Responsabilidades y procedimientos	Responsabilidades y procedimientos de manejo deberán ser establecidos para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	SI	
A13.2.2	Aprendiendo de los incidentes de seguridad de la información	Habrán mecanismos que permitan a los tipos, volúmenes y costos de los incidentes de seguridad de la información para ser cuantificados y controlados.	SI	Se manejará una bitácora que almacene los incidentes de forma histórica
A13.2.3	Acopio de Evidencias	Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de información implica una acción jurídica (civil o penal), se percibirá la evidencia, conservado, y se presentó a cumplir con las reglas para la prueba prevista en la jurisdicción correspondiente (s).	SI	
A14	Gestión de continuidad del negocio			
A14.1	Los aspectos de seguridad de información de la gestión de la continuidad del negocio	Para contrarrestar las interrupciones a las actividades comerciales y proteger los procesos críticos de negocio de los efectos de los fallos principales de los sistemas de información o los desastres y asegurar su oportuna reanudación.		
A14.1.1	Incluyendo seguridad de la información en el proceso de gestión de la continuidad del negocio	Un proceso gestionado se desarrolla y se mantiene la continuidad del negocio en toda la organización que se ocupa de los requisitos de seguridad de la información necesaria para la continuidad del negocio de la organización.	SI	

A14.1 .2	Continuidad del negocio y análisis de riesgos	Los eventos que pueden causar interrupciones en los procesos de negocio deben ser identificados, junto con la probabilidad y el impacto de estas interrupciones y de sus consecuencias para la seguridad de la información.	SI	
A14.1 .3	Desarrollo e implementación de planes de continuidad que incluyen seguridad de la información	Los planes deberán desarrollarse y aplicarse para mantener o restaurar las operaciones y asegurar la disponibilidad de información al nivel requerido y en las escalas de tiempo requeridas siguientes a la interrupción o el fracaso de los procesos críticos de negocio.	SI	
A14.1 .4	Marco de planificación de la continuidad del negocio	Deberá mantenerse un único marco de los planes de continuidad del negocio para asegurar que todos los planes son consistentes, para abordar de manera coherente los requisitos de seguridad de la información, y para identificar las prioridades de prueba y mantenimiento.	SI	
A14.1 .5	Pruebas, mantenimiento y re-evaluación de los planes de continuidad del negocio	Los planes de continuidad deberán ser probados y actualizados regularmente para asegurarse de que están al día y efectivo.	SI	
A15	Conformidad			
A15.1	El cumplimiento de los requisitos legales	Para evitar el rebasamiento de cualquier ley, obligaciones legales, reglamentarias o contractuales, y de los requisitos de seguridad.		
A15.1 .1	Identificación de la legislación aplicable	Todos los requisitos legales, reglamentarios y contractuales pertinentes y por el enfoque de la organización para cumplir con estos requisitos se definirán explícitamente, documentados, y se mantienen al día para cada sistema de información y la organización.	SI	
A15.1 .2	Derechos de propiedad intelectual (DPI)	Procedimientos apropiados se aplicarán para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales sobre el uso de material con respecto al cual puede haber derechos de propiedad intelectual y sobre el uso de productos de software propietario.	SI	

A15.1 .3	Protección de los registros de la organización	Registros importantes estarán protegidos contra pérdida, destrucción y falsificación, de acuerdo con los requisitos legales, reglamentarios, contractuales y de negocios.	SI	
A15.1 .4	Protección de datos y privacidad de la información personal	Protección de datos y privacidad se garantizará como se requiere en la legislación pertinente, los reglamentos, y, si procede, las cláusulas contractuales.	SI	
A15.1 .5	Prevención del uso indebido de las instalaciones de procesamiento de información	Los usuarios se decidan a utilizar las instalaciones de procesamiento de información para fines no autorizados.	SI	
A15.1 .6	Regulación de los controles de cifrado	Controles de cifrado serán utilizados en cumplimiento de todos los acuerdos, leyes y reglamentos.	SI	
A15.2	El cumplimiento de las políticas de seguridad y las normas y el cumplimiento técnico	Para garantizar el cumplimiento de los sistemas con las políticas y estándares de seguridad de la organización		
A15.2 .1	El cumplimiento de las políticas y normas de seguridad	Administradores se asegurarán de que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y estándares de seguridad.	SI	
A15.2 .2	Comprobación del cumplimiento técnico	Los sistemas de información deben ser revisados regularmente por el cumplimiento de las normas de aplicación de la seguridad.	SI	
A15.3	Consideraciones de auditoría del sistema de información	Para maximizar la eficacia y minimizar la interferencia a / desde el proceso de auditoría de sistemas de información.		
A15.3 .1	Controles de auditoría de sistemas de información	Requisitos de auditoría y las actividades relacionadas con los controles de los sistemas operativos deberán ser planeadas cuidadosamente y acordaron reducir al mínimo el riesgo de interrupciones en los procesos de negocio.	SI	
A15.3 .2	Protección de las herramientas de auditoría de sistemas de información	El acceso a las herramientas de auditoría de sistemas de información debe ser protegido para evitar cualquier posible mal uso.	SI	