

INGENIERÍA EN FINANZAS Y AUDITORÍA, CONTADORA
PÚBLICA-AUDITORA

DECLARACIÓN DE RESPONSABILIDAD

GINA LOLLOBRIGIDA BURGOS BENITES

DECLARO QUE:

El proyecto de grado denominado Evaluación de Controles a los Sistemas Informáticos de la Empresa Caltec Buró de Información Crediticia, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan el pie de las páginas correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es mi autoría.

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

Sangolquí, Septiembre 10 del 2008

GINA LOLLOBRIGIDA BURGOS BENITES

ESCUELA POLITÉCNICA DEL EJÉRCITO

INGENIERÍA EN FINANZAS Y AUDITORÍA, CONTADORA
PÚBLICA-AUDITORA

CERTIFICADO

Dra. Eugenia Camacho, Ing. Carlos Sierra

CERTIFICAN

Que el trabajo titulado Evaluación de Controles a los Sistemas Informáticos de la Empresa Caltec Buró de Información Crediticia, realizado por Gina Lollobrígida Burgos Benites, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Escuela Politécnica del Ejército.

Debido a que la Evaluación de Controles a los Sistemas Informáticos es un gran apoyo para las empresas de nuestro País y una herramienta para conocer si los sistemas aplicados cumplen con eficiencia y eficacia con los objetivos de la empresa, si recomiendan su publicación.

El mencionado trabajo consta de dos documentos empastados y tres discos compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a Gina Lollobrígida Burgos Benites que lo entregue a Economista Galo Acosta, en su calidad de Director de la Carrera.

Sangolquí, Septiembre 10 del 2008

Dra. Eugenia Camacho, Msc
DIRECTOR

Ing. Carlos Sierra
CODIRECTOR

ESCUELA POLITÉCNICA DEL EJÉRCITO

INGENIERÍA EN FINANZAS Y AUDITORÍA, CONTADORA
PÚBLICA-AUDITORA

AUTORIZACIÓN

Yo, Gina Lollobrígida Burgos Benites

Autorizo a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la Institución del trabajo Evaluación de Controles a los Sistemas Informáticos de la Empresa Caltec Buró de Información Crediticia, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, Septiembre 10 del 2008

Gina Lollobrígida Burgos Benites

DEDICATORIA

A mis hijos, fuente inagotable de luz, amor, paciencia, tenacidad, y valor para superar todos los inconvenientes que se suscitaron a lo largo de mi carrera; ellos con su inocencia y callada espera supieron afrontar los momentos en los que no contaron con mi presencia y eran importantes para ellos. Hoy quiero que este trabajo les sirva de ejemplo para que en el futuro luchen para alcanzar sus metas y sueños, para que la palabra “no puedo” no esté en su diccionario y que sean triunfadores ante todo y ante todos, que con suspicacia y sabiduría sepan enfrentar los problemas y a quienes les hagan los problemas, que sean éstos valiosa herramienta para fortalecer su espíritu y su alma.

A mi padre, que desde el cielo me acompaña con su amor y ternura, que a pesar de no estar físicamente conmigo siento siempre su presencia y apoyo cuando más lo necesito.

AGRADECIMIENTO

A la Escuela Politécnica del Ejército, por haberme acogido en sus aulas y en ellas aprendí los conocimientos que necesito para ser una buena profesional.

A la Doctora Eugenia Camacho, maestra sabia que supo impartir y compartir sus conocimientos conmigo, gracias a su paciencia, constancia y tenacidad hoy este trabajo llega a un buen final, y me ha enriquecido personal y profesionalmente.

A Dios; padre, compañero y amigo; mi refugio y consuelo en los momentos más difíciles, mi celebración y alegría en mis triunfos, luz divina que ilumina mi alma y mi vida, manantial de fe, esperanza, perdón, amor, y todos los valores que han sido en mi vida la principal arma para vencer obstáculos y convertirlos en enseñanzas positivas para llenar mi vida y la de los míos de momentos inolvidables y únicos.

A mi madre, que gracias a Dios es la mejor madre del mundo, de ella aprendí a luchar por lo que quiero, ella me enseñó siempre a salir adelante, me exigió hacer las cosas bien o no hacerlas y lo más importante me ha dado su amor, tesoro incalculable para una vida feliz. Gracias porque de todas las madres tú eres la mejor.

ÍNDICE DE CONTENIDOS

RESUMEN	1
SUMARY	4
CAPÍTULO 1	7
ASPECTOS GENERALES	7
1.1. ANTECEDENTES	7
1.1.1. Base Legal de la Empresa	8
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.	8
Ley de Propiedad Intelectual.	9
Ley de Burós y de Información Crediticia.	9
Ley General de Instituciones del Sistema Financiero.	10
Ley de Instituciones Financieras.	11
Ley de Régimen Tributario Interno.	11
Ley de Régimen Laboral.	11
Código de trabajo.	11
Ley de Seguridad Social.	12
Organismos de Control.	12
Superintendencia de Bancos.	12
Servicio de Rentas Internas.	13
Instituto Ecuatoriano de Seguridad Social.	13
Ministerio de Trabajo.	14
1.1.2. Objetivos de la Empresa.	14
1.2. LA EMPRESA	15
Concepto	15
Clasificación de las Empresas	15
Por su naturaleza	15
Empresas Industriales	15
Empresas Comerciales	15
Empresas de Servicios	15
Por el sector al que pertenece	16
Empresas públicas	16

Empresas Privadas	16
Empresas Mixtas	16
Por la integración del capital	16
Unipersonales	16
Sociedades o compañías	16
Sociedades de personas	16
Sociedades de capital	17
1.2.1. Reseña Histórica	17
1.2.2 Organigramas	19
1.2.2.1. Organigrama Estructural	19
1.2.2.2. Organigrama Funcional	20
1.2.2.3. Organigrama de Personal	20
1.2.2.4. Organigrama por Procesos	20
CAPITULO 2	25
ANÁLISIS SITUACIONAL	25
2.1. ANÁLISIS INTERNO	25
Departamento de Sistemas de CALTEC BURÓ	25
2.1.1. Área de Análisis	25
2.1.2. Área de Diseño	26
2.1.3. Área de Programación	26
2.1.4. Área de Digitación	27
2.2. ANÁLISIS EXTERNO	28
2.2.1. Influencias Macroeconómicas	28
2.2.1.1 Incidencia del Factor Político	28
2.2.1.2. Incidencia de Factor Económico	29
2.2.1.3. Incidencia del Factor Legal	30
2.2.2. Influencias Micro económicas	30
2.2.2.1. Clientes	30
2.2.2.2. Precios	31
2.2.2.3. Competencia	32
CAPITULO 3	35
DIRECCIONAMIENTO ESTRATÉGICO	35

3.1. Misión	35
3.2. Visión	36
3.3. Objetivos	37
3.4. Políticas	38
3.5. Estrategias	39
3.6. Principios y Valores	41
CAPITULO 4	44
CONTROLES INTERNOS INFORMÁTICOS	44
4.1. CONTROLES INTERNOS PARA LA SEGURIDAD DEL DEPARTAMENTO DE SISTEMAS	44
4.1.1. SEGURIDAD FÍSICA.	44
Inventario de Hardware, mobiliario y equipo.	45
Resguardo del equipo de cómputo.	45
Bitácoras de mantenimiento y correcciones.	45
Controles de acceso del personal al área de sistemas.	46
Control del mantenimiento a instalaciones y construcciones.	46
Seguros y fianzas para el personal, equipos y sistemas.	46
Contratos de actualización, asesoría, y mantenimiento del hardware.	46
4.1.2. SEGURIDAD LÓGICA	47
Control para el acceso al sistema, a los programas y a la información.	47
Establecimiento de niveles de acceso	48
Dígitos verificadores y cifras de control	48
Palabras claves de acceso.	48
Controles para el seguimiento de las secuencias y rutinas lógicas del sistema.	48
4.1.3. SEGURIDAD DE LAS BASES DE DATOS	48
Programas de protección para impedir el uso inadecuado	49

y la alteración de datos de uso exclusivo	
Respaldos periódicos de información	49
Planes y programas para prevenir contingencias y recuperar información	50
Control de accesos a las bases de datos.	50
Rutinas de monitoreo y evaluación de operaciones relacionadas con las bases de datos	50
4.1.4 SEGURIDAD EN LA OPERACIÓN	51
Controles para los procedimientos de Operación.	51
Controles para el procesamiento de la información	51
Controles para la emisión de resultados	52
Controles específicos para la operación de la computadora	52
Controles para el almacenamiento de información.	52
Controles para el mantenimiento del sistema.	53
4.1.5. SEGURIDAD DEL PERSONAL DE INFORMÁTICA	53
Controles administrativos de personal.	54
Seguros y fianzas para el personal de sistemas.	54
Planes y programas de capacitación	54
4.1.6 SEGURIDAD DE LAS TELECOMUNICACIONES	55
Establecimiento de contraseñas y medios controlados de transmisión.	55
Adopción de medidas de verificación de transmisión de información	55 56
4.1.7 SEGURIDAD EN LAS REDES	56
Restricción de accesos para los usuarios	57
Uso de palabras clave para ingresar a los programas y archivos	58
Monitoreo de actividades	58
4.2. CONTROLES INTERNOS PARA LA ORGANIZACIÓN DEL DEPARTAMENTO DE SISTEMAS	59
Dirección	59
División del trabajo.	60
Dirección General del Área de Informática.	60

Área de análisis	61
Área de diseño	61
Área de programación	61
Área de digitación	61
Asignación de responsabilidad y autoridad	62
Establecimiento de estándares y métodos.	62
Perfiles de puestos.	62
4.3. CONTROLES INTERNOS PARA LA ADMINISTRACIÓN DE LOS SISTEMAS	64
4.4. CONTROLES INTERNOS PARA EL ANÁLISIS, DESARROLLO E IMPLEMENTACIÓN DE LOS SISTEMAS	65
Análisis del sistema actual	65
Diseño conceptual.	65
Diseño detallado	65
Programación	66
Pruebas y correcciones	66
Documentación del sistema	66
Capacitación de usuarios	66
Implementación del sistema	66
Liberación del sistema	66
Mantenimiento.	67
4.5. CONTROLES INTERNOS PARA EL INGRESO DE DATOS, PROCESO DE INFORMACIÓN, SALIDA DE RESULTADOS	67
Verificar la existencia y funcionamiento de los procedimientos de captura de datos	68
Comprobar que todos los datos sean debidamente procesados	68
Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos	68
Comprobar la suficiencia en la emisión de información.	69
4.6. HERRAMIENTAS PARA LA EVALUACIÓN DE CONTROLES INTERNOS INFORMÁTICOS	69
Herramientas de control	69
4.7. TÉCNICAS PARA LA EVALUACIÓN DE CONTROLES INTERNOS	70

INFORMÁTICOS	
Descripción de técnicas de auditoria con ayuda de computadora (TAACs – CAATs Computer assisted audit Techniques).	71
4.8. DISEÑO DE PAPELES DE TRABAJO PARA LA EVALUACIÓN DE CONTROLES INTERNOS INFORMÁTICOS.	85
CAPITULO 5	104
PROPUESTA DE EVALUACION DE CONTROLES A LOS SISTEMAS INFORMÁTICOS DE LA EMPRESA CALTEC BURÓ DE INFORMACIÓN CREDITICIA S. A.	104
5.1. AREA DE ANÁLISIS	104
5.1.1 EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO	104
5.1.1.1 CONTROLES INTERNOS PARA LA SEGURIDAD. DEL ÁREA DE ANÁLISIS	105
1. SEGURIDAD FÍSICA	107
Inventario de hardware, mobiliario y equipo del área de análisis	107
Resguardo de los equipos del centro de cómputo	113
Bitácoras de mantenimiento y reparaciones de los equipos del área de análisis	115
Control de acceso del personal al área de análisis.	115
Control del mantenimiento a instalaciones y construcciones	115
Seguros y fianzas para el personal, equipos y sistemas	115
Contratos de actualización, asesoría y mantenimiento del hardware	116
2. SEGURIDAD LÓGICA	116
Control para el acceso al sistema, a los programas y a la información	116
Establecimiento de niveles de acceso.	118
Dígitos verificadores y cifras de control	118
Palabras claves de acceso	118

3. SEGURIDAD DE LA BASE DE DATOS	119
Programas de protección para impedir el uso inadecuado	119
Y la alteración de datos de uso exclusivo	
Respaldos periódicos de información	120
Planes y programas para prevenir contingencias y recuperar información	120
Control de acceso a las bases de datos	121
Rutinas de monitoreo y evaluación de operaciones relacionadas con las bases de datos	121
4. SEGURIDAD EN LA OPERACIÓN	121
Controles para los procedimientos de operación	122
Controles para el procesamiento de la información	122
Controles para la emisión de resultados	124
Controles específicos para la operación de la computadora	124
Controles para el almacenamiento de información	124
Controles para el mantenimiento del sistema	124
5. SEGURIDAD DEL PERSONAL DE INFORMÁTICA	125
Controles administrativos de personal	126
Seguros y fianzas para el personal de sistemas	126
Planes y programas de capacitación	126
6. SEGURIDAD DE LAS TELECOMUNICACIONES	127
Establecimiento de contraseñas y medios controlados de transmisión	127
Adopción de medidas de verificación de transmisión de información	127
7. SEGURIDADES EN LAS REDES	128
Restricción de acceso para los usuarios	129
Uso de palabras clave para ingresar a los programas y archivos	129

Monitoreo de actividades	130
Matriz de Evaluación	130
Guía de evaluación de controles Internos Informáticos	132
Matriz de Ponderación	135
5.1.2. OBJETIVOS DEL CONTROL INTERNO INFORMÁTICO	145
5.1.3. DIAGRAMA DE FLUJO DEL PROCESO ACTUAL	146
5.1.4. DEBILIDADES DETECTADAS	147
5.1.5. DIAGRAMA DE FLUJO PROPUESTO	148
5.1.6. INFORME DE EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO	149
5.2. AREA DE DISEÑO	152
5.2.1 EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO	152
5.2.1.1. CONTROLES INTERNOS PARA LA SEGURIDAD DEL ÁREA DE DISEÑO	152
1. SEGURIDAD FÍSICA	154
Inventario de hardware, mobiliario y equipo del área de diseño	155
Resguardo de los equipos del centro de cómputo	160
Bitácoras de mantenimiento y reparaciones de los equipos del área de diseño	162
Control de acceso del personal al área de diseño	162
Control del mantenimiento a instalaciones y construcciones.	162
Seguros y fianzas para el personal, equipos y sistemas	162
Contratos de actualización, asesoría y mantenimiento del hardware	163
2. SEGURIDAD LÓGICA	163
Control para el acceso al sistema, a los programas y a la información	163

Establecimiento de niveles de acceso	164
Dígitos verificadores y cifras de control	164
Palabras claves de acceso	164
3. SEGURIDAD DE LAS BASES DE DATOS	165
Programas de protección para impedir el uso inadecuado	165
y la alteración de datos de uso exclusivo	
Respaldos periódicos de información	166
Planes y programas para prevenir contingencias y recuperar información	166
Control de acceso a las bases de datos	167
Rutinas de monitoreo y evaluación de operaciones relacionadas con las bases de datos	167
4. SEGURIDAD EN LA OPERACIÓN	167
Controles para los procedimientos de operación	168
Controles para el procesamiento de información	168
Controles para la emisión de resultados	168
Controles específicos para la operación de la computadora	169
Controles para el almacenamiento de información	169
Controles para el mantenimiento del sistema	169
5. SEGURIDAD DEL PERSONAL DE INFORMÁTICA	170
Controles administrativos del personal	170
Seguros y fianzas para el personal de sistemas	171
Planes y programas de capacitación	171
6. SEGURIDAD DE LAS TELECOMUNICACIONES	171
Establecimiento de contraseñas y medios controlados de transmisión	171
Adopción de medidas de verificación de transmisión de información	172
7. SEGURIDAD EN LAS REDES	172

Restricción de acceso para los usuarios	173
Uso de palabras clave para ingresar a los programas y archivos	173
Monitoreo de actividades	174
Matriz de Evaluación	175
Guía de evaluación de controles Internos Informáticos	177
Matriz de Ponderación	180
5.2.2. Objetivos del control interno informático	190
5.2.3. Diagrama de flujo del proceso actual	191
5.2.4. Debilidades detectadas	192
5.2.5. Diagrama de flujo propuesto	193
5.2.6. Informe de evaluación del control interno informático	194
5.3. AREA DE PROGRAMACION	197
5.3.1 EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO	197
5.3.1.1 CONTROLES INTERNOS PARA LA SEGURIDAD DEL ÁREA DE PROGRAMACIÓN	197
1. SEGURIDAD FÍSICA	199
Inventario del hardware, mobiliario y equipo del área de programación	200
Resguardo de los equipos del centro de cómputo	205
Bitácoras de mantenimiento y reparaciones de los equipos del área de programación	207
Control de acceso del personal al área de programación	207
Control del mantenimiento a instalaciones y construcciones	207
Seguros y fianzas para el personal, equipos y sistemas.	207
Contratos de actualización, asesoría y mantenimiento del hardware	208
2. SEGURIDAD LÓGICA	208

Control para el acceso al sistema, a los programas y a la información	208
Establecimiento de niveles de acceso	210
Dígitos verificadores y cifras de control	210
Palabras claves de acceso	210
3. SEGURIDAD DE LAS BASES DE DATOS	211
Programas de protección para impedir el uso inadecuado y la alteración de datos de uso exclusivo	211
Respaldos periódicos de información	212
Planes y programas para prevenir contingencias y recuperar información	212
Control de acceso a las bases de datos	213
Rutinas de monitoreo y evaluación de operaciones relacionadas con las bases de datos	213
4. SEGURIDAD EN LA OPERACIÓN	213
Controles para los procedimientos de operación	214
Controles para el procesamiento de la información	214
Controles para la emisión de resultados	216
Controles específicos para la operación de la computadora	216
Controles para el almacenamiento de información	216
Controles para el mantenimiento del sistema	216
5. SEGURIDAD DEL PERSONAL DE INFORMÁTICA	217
Controles administrativos de personal	217
Seguros y fianzas para el personal de sistemas	218
Planes y programas de capacitación	218
6. SEGURIDAD DE LAS TELECOMUNICACIONES	218
Establecimiento de contraseñas y medios controlados de transmisión	219
Adopción de medidas de verificación de transmisión	219

de información	
7. SEGURIDAD EN LAS REDES	220
Restricción de acceso para los usuarios	220
Uso de palabras clave para ingresar a los programas y archivos	221
Monitoreo de actividades	221
Matriz de Evaluación	222
Guía de evaluación de controles Internos Informáticos.	224
Matriz de Ponderación	227
5.3.2. Objetivos del control interno informático	237
5.3.3. Diagrama de flujo del proceso actual	238
5.3.4. Debilidades detectadas	239
5.3.5. Diagrama de flujo propuesto	240
5.3.6. Informe de evaluación del control interno informático	241
5.4 AREA DE DIGITACION	244
5.4.1 EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO	244
5.4.1.1. CONTROLES INTERNOS PARA LA SEGURIDAD DEL ÁREA DE DIGITACIÓN	244
1. SEGURIDAD FÍSICA	246
Inventario del hardware, mobiliario y equipo del área de digitación	247
Resguardo de los equipos del centro de cómputo	252
Bitácoras de mantenimiento y reparaciones de los equipos del área de digitación	254
Control de acceso del personal al área de digitación	254
Control del mantenimiento a instalaciones y construcciones	254
Seguros y fianzas para el personal, equipos y sistemas	254
Contratos de actualización, asesoría y mantenimiento	255

del hardware	
2. SEGURIDAD LÓGICA	255
Control para el acceso al sistema, a los programas y a la información	255
Establecimiento de niveles de acceso	257
Dígitos verificadores y cifras de control	257
Palabras claves de acceso	257
3. SEGURIDAD DE LAS BASES DE DATOS	258
Programas de protección para impedir el uso inadecuado y la alteración de datos de uso exclusivo	258
Respaldos periódicos de información	259
Planes y programas para prevenir contingencias y recuperar información	259
Control de acceso a las bases de datos	260
Rutinas de monitoreo y evaluación de operaciones relacionadas con las bases de datos	260
4. SEGURIDAD EN LA OPERACIÓN	260
Controles para los procedimientos de operación	261
Controles para el procesamiento de información	261
Controles para la emisión de resultados	261
Controles específicos para la operación de la computadora	262
Controles para el almacenamiento de información	262
Controles para el mantenimiento del sistema	262
5. SEGURIDAD DEL PERSONAL DE INFORMÁTICA	263
Controles administrativos de personal	263
Seguros y fianzas para el personal de sistemas	264
Planes y programas de capacitación	264
6. SEGURIDAD DE LAS TELECOMUNICACIONES	264

Establecimiento de contraseñas y medios controlados de transmisión	264
Adopción de medidas de verificación de transmisión de información	265
7. SEGURIDAD EN LAS REDES	265
Restricción de acceso para los usuarios	266
Uso de palabras clave para ingresar a los programas y archivos	266
Monitoreo de actividades	267
Cuestionario de Evaluación de Control Interno	268
Entrevistas	274
5.4.2. Objetivos del control interno informático.	278
5.4.3. Diagrama de flujo del proceso actual.	279
5.4.4. Debilidades detectadas.	280
5.4.5. Diagrama de flujo propuesto.	281
5.4.6. Informe de evaluación del control interno informático.	282
CAPITULO 6	285
6.1. CONCLUSIONES	285
6.2. RECOMENDACIONES	287
GLOSARIO DE TÉRMINOS	290
BIBLIOGRAFÍA	295

INDICE DE CUADROS Y ANEXOS

- Cuadro No. 1: Listado de Planes del Servicio
- ANEXO A: Boletines instructivos de la Superintendencia de Bancos y Seguros del Ecuador para los Burós de Crédito.
- ANEXO B: Modelos de Reporte de Información Crediticia.