

| | | |
|-------------------------------|---------------------|-----------------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 1 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|--|-----------------|----------------------------|
| 5.1 | POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN | | |
| 5.1.1 | Se tiene documento de la política de seguridad de la Información | | |
| 5.1.2 | Se hace revisión y evaluación de este documento y se promulga su lectura y aplicación. | | |
| 6.1 | ORGANIZACIÓN SEGURIDAD | | |
| 6.1.1 | Compromiso de las Directivas con la seguridad de la información | | |
| 6.1.2 | Coordinación de la Seguridad | | |
| 6.1.3 | Asignación de responsabilidades | | |
| 6.1.4 | Proceso de Autorización a áreas de procesamiento de información | | |
| 6.1.5 | Se realizan acuerdos de confidencialidad | | |
| 6.1.6 | Contacto con las autoridades | | |

| | | |
|-------------------------------|---------------------|-----------------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 2 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|---|-----------------|----------------------------|
| 6.1.7 | Contacto con grupos de especial interés | | |
| 6.1.8 | Se realiza Auditoría interna | | |
| 6.2 | Terceros | | |
| 6.2.1 | Identificación de riesgos | | |
| 6.2.2 | Aproximación a la seguridad al tratar con clientes | | |
| 6.2.3 | Aproximación a la seguridad en acuerdos con terceros | | |
| 7.1 | GESTION DE ACTIVOS | | |
| 7.1.1 | Inventario de activos tecnológicos y de la información. | | |
| 7.1.2 | Responsables de los activos tecnológicos | | |
| 7.1.3 | Uso aceptable de las activos tecnológicos | | |
| 7.2 | Clasificación de la Información | | |

| | | |
|-------------------------------|---------------------|----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 3 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|--|-----------------|----------------------------|
| 7.2.1 | Normas para clasificación de la información | | |
| 7.2.2 | Identificación y Manejo de la información | | |
| 8.1 | SEGURIDAD RECURSO HUMANO Previo a la contratación | | |
| 8.1.1 | Roles y responsabilidades | | |
| 8.1.2 | Investigación del personal que va a ser contratado | | |
| 8.1.3 | Términos y condiciones laborales | | |
| 8.2 | Durante el empleo | | |
| 8.2.1 | Responsabilidades de las directivas | | |
| 8.2.2 | Conciencia de la seguridad, educación y entrenamiento | | |
| 8.2.3 | Procesos disciplinarios | | |
| 8.3 | Terminación del contrato o cambio de empleo | | |

| | | |
|-------------------------------|--------------|----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 4 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|--|-----------------|----------------------------|
| 8.3.1 | Responsabilidades en la terminación del contrato | | |
| 8.3.2 | Devolución de activos tecnológicos | | |
| 8.3.3 | Eliminación de permisos sobre los activos | | |
| 9.1 | SEGURIDAD FISICA Áreas Restringidas | | |
| 9.1.1 | Perímetro de Seguridad Física | | |
| 9.1.2 | Controles físicos de entrada | | |
| 9.1.3 | Aseguramiento de oficinas, cuartos e instalaciones | | |
| 9.1.4 | Protección contra amenazas externas y ambientales | | |
| 9.1.5 | Trabajo en áreas restringidas | | |
| 9.1.6 | Acceso público, envíos y áreas de carga | | |
| 9.2 | Seguridad de los Componentes Tecnológicos | | |

| | | |
|-------------------------------|---------------------|-----------------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 5 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|--|-----------------|----------------------------|
| 9.2.1 | Ubicación y protección de equipos tecnológicos | | |
| 9.2.2 | Seguridad en el suministro de electricidad y servicios (utilities) | | |
| 9.2.3 | Seguridad en el cableado | | |
| 9.2.4 | Mantenimiento | | |
| 9.2.5 | Seguridad de equipos fuera de las áreas seguras | | |
| 9.2.6 | Dstrucción y reutilización de equipos | | |
| 9.2.7 | Extracción de activos informáticos | | |
| 10.1 | COMUNICACIONES Y MANEJOS OPERATIVOS Procedimientos Operativos y Responsabilidades | | |
| 10.1.1 | Documentación de procesos operativos | | |
| 10.1.2 | Control de Cambios | | |

| | | |
|-------------------------------|---------------------|----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 6 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|--|-----------------|----------------------------|
| 10.1.3 | Segregación de funciones | | |
| 10.1.4 | Separación de los ambientes de Desarrollo, prueba y producción | | |
| 10.2 | Administración de Servicios de terceros | | |
| 10.2.1 | Entrega de servicios | | |
| 10.2.2 | Monitoreo y revisión de servicios de terceros | | |
| 10.2.3 | Administración de cambios a servicios de terceros | | |
| 10.3 | Planeamiento y aceptación de sistemas | | |
| 10.3.1 | Administración de la capacidad | | |
| 10.3.2 | Aceptación de sistemas | | |
| 10.4 | Protección contra código malicioso y móvil | | |
| 10.4.1 | Controles contra código malicioso | | |

| | | |
|-------------------------------|---------------------|----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 7 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|---|-----------------|----------------------------|
| 10.4.2 | Controles contra código móvil | | |
| 10.5 | Copias de seguridad | | |
| 10.5.1 | Respaldo de la información. | | |
| 10.6 | Administración de la seguridad de la red | | |
| 10.6.1 | Controles de la Red | | |
| 10.6.2 | Seguridad de los Servicios de Red | | |
| 10.7 | Manipulación de medios | | |
| 10.7.1 | Administración de medios removibles | | |
| 10.7.2 | Destrucción de medios | | |
| 10.7.3 | Procedimientos de manejo de la información | | |
| 10.7.4 | Seguridad de la documentación de los sistemas | | |

| | | |
|-------------------------------|---------------------|----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 8 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|---|-----------------|----------------------------|
| 10.8 | Intercambio de información | | |
| 10.8.1 | Políticas y procedimientos del intercambio de información | | |
| 10.8.2 | Acuerdos para el intercambio de información. | | |
| 10.8.3 | Medios físicos en movimiento | | |
| 10.8.4 | Mensajería Electrónica | | |
| 10.8.5 | Sistemas de información de negocios | | |
| 10.9 | Servicios de Comercio Electrónico | | |
| 10.9.1 | Comercio Electrónico | | |
| 10.9.2 | Transacciones en Línea | | |
| 10.9.3 | Información pública | | |
| 10.10 | Monitoreo | | |

| | | |
|-------------------------------|---------------------|----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 9 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|--|-----------------|----------------------------|
| 10.10.1 | Auditoría de registros | | |
| 10.10.2 | Uso de sistemas de monitoreo | | |
| 10.10.3 | Protección de registros de monitoreo | | |
| 10.10.4 | Registros de monitoreo de administradores y operadores | | |
| 10.10.5 | Registro de fallas | | |
| 10.10.6 | Sincronía | | |
| 11.1 | CONTROL DE ACCESO A LA INFORMACIÓN; de acuerdo a las necesidades del negocio. | | |
| 11.1.1 | Política de Control de Acceso | | |
| 11.2 | Administración de acceso de los usuarios | | |
| 11.2.1 | Registro de Usuarios | | |
| 11.2.2 | Administración de privilegios | | |
| 11.2.3 | Administración de Contraseñas (passwords) | | |

| | | |
|-------------------------------|---------------------|-----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 10 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|--|-----------------|----------------------------|
| 11.2.4 | Revisión de los permisos asignados a los usuarios | | |
| 11.3 | Responsabilidades de los usuarios | | |
| 11.3.1 | Uso de las contraseñas | | |
| 11.3.2 | Equipos desatendidos | | |
| 11.3.3 | Política de escritorios y pantallas limpias | | |
| 11.4 | Control de acceso a la red de datos | | |
| 11.4.1 | Políticas para el uso de los servicios de la red de datos | | |
| 11.4.2 | Autenticación de usuarios para conexiones externas | | |
| 11.4.3 | Identificación de equipos en la red | | |
| 11.4.4 | Diagnóstico remoto y protección de la configuración de puertos | | |
| 11.4.5 | Segregación en la red | | |
| 11.4.6 | Control de conexión a la red | | |

| | | |
|-------------------------------|--------------|-----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 11 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|---|-----------------|----------------------------|
| 11.4.7 | Control de enrutamiento de la red | | |
| 11.5 | Control de acceso a los sistemas operativos | | |
| 11.5.1 | Procedimientos para inicio de sesión de las estaciones de trabajo | | |
| 11.5.2 | Identificación y autenticación de los usuarios. | | |
| 11.5.3 | Sistema de administración de contraseñas. | | |
| 11.5.4 | Uso de las utilidades del sistema | | |
| 11.5.5 | Time-out para las estaciones de trabajo. | | |
| 11.5.6 | Limitación en los periodos de tiempo de conexión a servicios y aplicaciones | | |
| 11.6 | Control de acceso a las aplicaciones | | |
| 11.6.1 | Restricción de acceso a los sistemas de información | | |
| 11.6.2 | Aislamiento de sistemas sensibles | | |

| | | |
|-------------------------------|--------------|-----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 12 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|--|-----------------|----------------------------|
| 11.7 | Computación Móvil y Teletrabajo | | |
| 11.7.1 | Computación Móvil y comunicacioines | | |
| 11.7.2 | Teletrabajo | | |
| 12.1 | DESARROLLO DE SOFTWARE Requerimientos de seguridad para los sistemas de información | | |
| 12.1.1 | Análisis y especificaciones de los requerimientos de seguridad | | |
| 12.2 | Procesamiento correcto en aplicaciones | | |
| 12.2.1 | Validación de los datos de entrada | | |
| 12.2.2 | Control del procesamiento interno | | |
| 12.2.3 | Integridad de los mensajes | | |
| 12.2.4 | Validación de los datos de salida | | |
| 12.3 | Controles Criptográficos | | |
| 12.3.1 | Política para el uso de controles criptográficos | | |

| | | |
|-------------------------------|--------------|-----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 13 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|--|-----------------|----------------------------|
| 12.3.2 | Administración de llaves | | |
| 12.4 | Seguridad en los archivos del sistema (System Files) | | |
| 12.4.1 | Control del software operacional(operativo) | | |
| 12.4.2 | Protección de los datos en sistemas de prueba | | |
| 12.4.3 | Control de acceso a las librerías de código fuente | | |
| 12.5 | Seguridad en el desarrollo y en los procesos de soporte técnico | | |
| 12.5.1 | Procedimientos para el control de cambios | | |
| 12.5.2 | Revisión técnica de aplicaciones después de cambios al sistema operativo | | |
| 12.5.3 | Restricciones a cambios en paquetes de software | | |
| 12.5.4 | Fuga de información | | |
| 12.5.5 | Desarrollo de software por parte de Outsourcing | | |
| 12.6 | Administración Técnica de Vulnerabilidades | | |
| 12.6.1 | Control técnico de vulnerabilidades | | |
| 13.1 | REPORTE DE EVENTOS DE SEGURIDAD INFORMÁTICA Y DE SUS DEBILIDADES | | |

| | | |
|-------------------------------|---------------------|-----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 14 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|--|-----------------|----------------------------|
| 13.1.1 | Reporte de eventos de Seguridad de la información. | | |
| 13.1.2 | Reporte de debilidades de seguridad | | |
| 13.2 | Administración de incidentes de seguridad informática y de su mejoramiento | | |
| 13.2.1 | Responsabilidades y procedimientos | | |
| 13.2.2 | Aprendizaje a partir de los incidentes de seguridad | | |
| 13.2.3 | Recolección de evidencia | | |
| 14.1 | ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO | | |
| 14.1.1 | Inclusión de seguridad de la información en el proceso de administración de la continuidad del negocio | | |
| 14.1.2 | Continuidad del negocio y análisis de impacto (BIA) | | |
| 14.1.3 | Desarrollo e implementación de planes de continuidad | | |
| 14.1.4 | Marco de planeación para la continuidad del negocio | | |

| | | |
|-------------------------------|--------------|-----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 15 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|---|-----------------|----------------------------|
| 14.1.5 | Pruebas, mantenimiento y revisión de los planes de continuidad del negocio | | |
| 15.1 | CUMPLIMIENTO CON REQUERIMIENTOS LEGALES | | |
| 15.1.1 | Identificación de leyes aplicables | | |
| 15.1.2 | Derechos de autor y propiedad intelectual | | |
| 15.1.3 | Salvaguardar los registros de la organización | | |
| 15.1.4 | Protección de los datos y privacidad de la información personal | | |
| 15.1.5 | Prevención mal uso de los componentes tecnológicos | | |
| 15.1.6 | Regulación de controles criptográficos | | |
| 15.2 | Revisión de la política de seguridad y cumplimiento técnico | | |
| 15.2.1 | Cumplimiento de los diferentes requerimientos y controles establecidos por la política de seguridad | | |
| 15.2.2 | Chequeo del cumplimiento técnico | | |

| | | |
|-------------------------------|---------------------|-----------------|
| SISTESEG | | |
| ISO 27001 GAP ANALYSIS | | |
| Fecha: 10/7/2007 | CONFIDENCIAL | Página 16 de 16 |

| Control ISO | Requerimiento | Control (SI/NO) | Porcentaje de cumplimiento |
|-------------|--|-----------------|----------------------------|
| 15.3 | Consideraciones relacionadas con la auditoría interna | | |
| 15.3.1 | Controles para auditoría del sistema | | |
| 15.3.2 | Protección de las herramientas para auditoría del sistema | | |

FIN