ANEXO E: Lista Resumida de Riesgos por Activos de Información[1]

No. Activo *(Anexos C y D)*	Impacto *(cuadro 4-06)*	Probabilidad *(cuadro 4-07)*	Riesgo *(cuadro 4-08)*
AI1.1	Alto	Medio	Alto
AI1.2	Bajo	Alto	Moderado
AI1.3	Moderado	Medio	Moderado
AI2.1	Bajo	Bajo	Bajo
AI2.2	Bajo	Bajo	Bajo
AI2.3	Bajo	Bajo	Bajo
AI3.1	Bajo	Medio	Bajo
AI3.2	Bajo	Medio	Bajo
AI4.1	Moderado	Bajo	Bajo
AI4.2	Bajo	Medio	Bajo
AI4.3	Moderado	Medio	Moderado
AI5.1	Alto	Medio	Alto
AI5.2	Moderado	Medio	Moderado
AI6.1	Bajo	Medio	Bajo
AI7.1	Bajo	Medio	Bajo
AI8.1	Bajo	Medio	Bajo
AI8.2	Bajo	Medio	Bajo
AI9.1	Moderado	Medio	Moderado
AI9.2	Moderado	Medio	Moderado
AI9.3	Moderado	Alto	Alto
AI10.1	Moderado	Medio	Moderado
AI11.1	Alto	Medio	Alto
AI12.1	Moderado	Medio	Moderado
AI12.2	Alto	Medio	Alto

No. Activo *(Anexos C y D)*	Impacto *(cuadro 4-06)*	Probabilidad *(cuadro 4-07)*	Riesgo *(cuadro 4-08)*
AI13.1	Bajo	Bajo	Bajo
AI13.2	Bajo	Bajo	Bajo
AI14.1	Moderado	Medio	Moderado
AI15.1	Bajo	Medio	Bajo
AI15.2	Moderado	Medio	Moderado
AI16.1	Alto	Medio	Alto
AI17.1	Bajo	Medio	Bajo
AI18.1	Moderado	Medio	Moderado
AI18.2	Alto	Medio	Alto
AI19.1	Moderado	Medio	Moderado
AI19.2	Moderado	Medio	Moderado
AI20.1	Moderado	Bajo	Bajo
AI20.2	Bajo	Moderado	Bajo
AI21.1	Bajo	Bajo	Bajo
AI22.1	Moderado	Alto	Alto
AI23.1	Bajo	Bajo	Bajo
AI23.2	Bajo	Bajo	Bajo
AI24.1	Alto	Medio	Alto
AI25.1	Moderado	Bajo	Bajo
AI25.2	Alto	Alto	Alto
AI26.1	Moderado	Bajo	Bajo
AI26.2	Alto	Medio	Alto
AI27.1	Bajo	Bajo	Bajo
AI27.2	Moderado	Bajo	Bajo
AI28.1	Bajo	Bajo	Bajo

No. Activo *(Anexos C y D)*	Impacto *(cuadro 4-06)*	Probabilidad *(cuadro 4-07)*	Riesgo *(cuadro 4-08)*
AI28.2	Alto	Alto	Alto
AI29.1	Moderado	Medio	Moderado
AI29.2	Alto	Medio	Alto
AI29.3	Moderado	Medio	Moderado
AI30.1	Alto	Medio	Alto
AI31.1	Moderado	Medio	Moderado
AI32.1	Bajo	Bajo	Bajo
AI32.2	Bajo	Bajo	Bajo
AI32.3	Bajo	Bajo	Bajo
AI33.1	Bajo	Alto	Moderado
AI34.1	Bajo	Bajo	Bajo
AI35.1	Bajo	Bajo	Bajo
AI35.2	Alto	Medio	Alto
AI36.1	Bajo	Medio	Bajo
AI37.1	Bajo	Bajo	Bajo
AI38.1	Bajo	Bajo	Bajo
AI39.1	Moderado	Bajo	Bajo
AI40.1	Bajo	Bajo	Bajo
AI41.1	Moderado	Medio	Moderado
AI42.1	Bajo	Bajo	Bajo
AI43.1	Alto	Alto	Alto
AI44.1	Bajo	Bajo	Bajo
AI45.1	Moderado	Alto	Alto
AI46.1	Moderado	Medio	Moderado
AI47.1	Alto	Moderado	Alto

No. Activo *(Anexos C y D)*	Impacto *(cuadro 4-06)*	Probabilidad *(cuadro 4-07)*	Riesgo *(cuadro 4-08)*
AI48.1	Alto	Moderado	Alto
AI49.1	Alto	Moderado	Alto
AI50.1	Moderado	Medio	Moderado
AI51.1	Moderado	Alto	Alto
AI52.1	Alto	Bajo	Moderado
AI53.1	Bajo	Bajo	Bajo
AI54.1	Moderado	Medio	Moderado
AI55.1	Moderado	Medio	Moderado
AI56.1	Moderado	Medio	Moderado
AI57.1	Moderado	Medio	Moderado
AI58.1	Alto	Moderado	Alto
AI59.1	Moderado	Medio	Moderado
AI60.1	Moderado	Medio	Moderado
AI61.1	Alto	Medio	Alto
AI62.1	Moderado	Medio	Moderado
AI63.1	Moderado	Medio	Moderado
AI63.2	Moderado	Alto	Alto
AI64.1	Moderado	Alto	Alto
AI65.1	Moderado	Alto	Alto
AI66.1	Alto	Medio	Alto
AI67.1	Alto	Medio	Alto
AI68.1	Moderado	Bajo	Bajo
AI69.1	Moderado	Medio	Moderado
AI70.1	Alto	Medio	Alto
AI71.1	Alto	Medio	Alto

No. Activo *(Anexos C y D)*	Impacto *(cuadro 4-06)*	Probabilidad *(cuadro 4-07)*	Riesgo *(cuadro 4-08)*
AI72.1	Alto	Medio	Alto
AI73.1	Moderado	Medio	Moderado
AI74.1	Moderado	Medio	Moderado
AI75.1	Moderado	Alto	Alto
AI76.1	Moderado	Medio	Moderado
AI77.1	Alto	Medio	Alto
AI78.1	Alto	Medio	Alto

Anexo E - Lista resumida de riesgos de activos de información [1]

ANEXO F-01: Lista de Prioridades de Riesgos Detallado por Activos de Información – Situación Actual[1]

Situación actual: sin ISO/IEC 27001:2005

No. Activo *(Anexos C y D)*	[H] Impacto al Negocio *(4-04)*	[A] Confidencialidad e integridad *(4-10)*	[B] Disponibilidad *(4-11)*	[C] Nivel de Exposición Detallado *(mayor valor entre [A] y [B])*	[D] Factor de Exposición % *(4-12)*	[E] Nivel de Impacto Detallado *(4-13)* *[H]*[D]*	[F] Nivel de probabilidad sin ISO/IEC 27001:2005 *(4-14)*	[G] Nivel de riesgo sin ISO/IEC 27001:2005 *(4-15)* *[E]*[F]*
AI1.1	10	3	4	4	0,8	8	7	56
AI5.1	10	4	4	4	0,8	8	8	64
AI9.3	5	3	3	3	0,6	3	8	24
AI11.1	10	4	4	4	0,8	8	6	48
AI12.2	10	3	3	3	0,6	6	8	48
AI16.1	10	3	3	3	0,6	6	6	36
AI18.2	10	3	3	3	0,6	6	6	36
AI22.1	5	3	3	3	0,6	3	8	24
AI24.1	10	3	2	3	0,6	6	6	36
AI25.2	10	4	4	4	0,8	8	8	64
AI26.2	10	3	3	3	0,6	6	7	42

No. Activo *(Anexos C y D)*	[H] Impacto al Negocio *(4-04)*	[A] Confidencialidad e integridad *(4-10)*	[B] Disponibilidad *(4-11)*	[C] Nivel de Exposición Detallado *(mayor valor entre [A] y [B])*	[D] Factor de Exposición % *(4-12)*	[E] Nivel de Impacto Detallado *(4-13)* *[H]*[D]*	[F] Nivel de probabilidad sin ISO/IEC 27001:2005 *(4-14)*	[G] Nivel de riesgo sin ISO/IEC 27001:2005 *(4-15)* *[E]*[F]*
AI28.2	10	3	3	3	0,6	6	6	36
AI29.2	10	3	3	3	0,6	6	7	42
AI30.1	10	3	3	3	0,6	6	7	42
AI35.2	10	3	3	3	0,6	6	7	42
AI43.1	5	3	2	3	0,6	3	8	24
AI45.1	5	3	3	3	0,6	3	7	21
AI47.1	10	4	5	5	1	10	8	80
AI48.1	10	4	4	4	0,8	8	7	56
AI49.1	5	3	3	3	0,6	3	7	21
AI51.1	5	3	3	3	0,6	3	7	21
AI58.1	10	3	3	3	0,6	6	6	36
AI61.1	10	3	3	3	0,6	6	5	30
AI63.2	5	3	3	3	0,6	3	7	21

No. Activo *(Anexos C y D)*	[H] Impacto al Negocio *(4-04)*	[A] Confidencialidad e integridad *(4-10)*	[B] Disponibilidad *(4-11)*	[C] Nivel de Exposición Detallado *(mayor valor entre [A] y [B])*	[D] Factor de Exposición % *(4-12)*	[E] Nivel de Impacto Detallado *(4-13)* *[H]*[D]*	[F] Nivel de probabilidad sin ISO/IEC 27001:2005 *(4-14)*	[G] Nivel de riesgo sin ISO/IEC 27001:2005 *(4-15)* *[E]*[F]*
AI64.1	5	3	3	3	0,6	3	8	24
AI65.1	5	3	3	3	0,6	3	8	24
AI66.1	5	4	4	4	0,8	4	7	28
AI67.1	5	3	4	4	0,8	4	7	28
AI70.1	10	3	3	3	0,6	6	7	42
AI71.1	10	3	3	3	0,6	6	6	36
AI72.1	10	3	3	3	0,6	6	8	48
AI75.1	5	4	4	4	0,8	4	9	36
AI77.1	10	4	4	4	0,8	8	7	56
AI78.1	10	4	3	4	0,8	8	7	56

Anexo F-01 - Listado de Nivel de Riesgo Detallado – Sin ISO/IEC 27001:2005 [1]

ANEXO F-02: Lista de Prioridades de Riesgos Detallado por Activos de Información – Situación Proyectada[1]

Situación proyectada: con ISO/IEC 27001:2005
Referirse a las columnas del cuadro F-01

No. Activo *(Anexos C y D)*	[H]	Controles propuestos por la ISO/IEC 27001 en el Anexo A de la norma (ISO/IEC 27002)	[A]	[B]	[C]	[D]	[E]	[F]	[G]
AI1.1	10	A.10.5.1. Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada. A.10.1.1. Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	3	3	3	0,6	6	2	12
AI5.1	10	A.10.5.1. Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada. A.10.11.1. Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	3	4	4	0,8	8	2	16
AI9.3	5	A.13.1.1. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible. A.13.2.2. Deben existir mecanismos que permitan cuantificar monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.	3	3	3	0,6	3	3	9
AI11.1	10	A.9.2.4. Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	4	3	4	0,8	8	3	24

AI12.2	10	A.9.2.1. Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado A.10.5.1. Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada. A.10.1.1. Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten. A.14.1.3. Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.	3	2	3	0,6	6	3	18
AI16.1	10	A.10.1.2. Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información. A.10.1.4. Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo. A.10.3.2. Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo ensayos adecuados del sistema durante el desarrollo antes de la aceptación. A.12.5.1. Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios. A.12.5.2. Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización. A.12.5.3. Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente. A.12.1.1. Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.	2	2	2	0,4	4	4	16

AI18.2	10	A.7.1.1. Todos los activos deben estar claramente identificados y se deben elaborar mantener un inventario de todos los activos importantes. A.7.1.2. Toda la información y los activos asociados con los servicios de procesamiento de la información deben ser "propiedad" de una parte designada de la organización. A.7.1.3. Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.	2	2	2	0,4	4	2	8
AI22.1	5	A.6.1.4. Se debe definir e implementar un proceso de autorización de la dirección para nuevos servicios de procesamiento de información. A.6.1.5. Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no divulgación que reflejan las necesidades de la organización para la protección de la información.	2	2	2	0,4	2	3	6
AI24.1	10	A.10.9.1. Comercio electrónico Control: Se debe proteger la información involucrada en el comercio electrónico que se trasmite a través de redes públicas de cualquier actividad fraudulenta, disputa contractual y divulgación y modificación no autorizada. A.10.9.2. La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje. A.10.9.3. La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.	3	2	3	0,6	6	4	24
AI25.2	10	A.6.1.5. Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no divulgación que reflejan las necesidades de la organización para la protección de la información. A.10.1.3. Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de información A.10.7.3. Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	3	3	3	0,6	6	3	18

AI26.2	10	A.1.5.1.3. Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios reglamentarios, contractuales y del negocio. A.15.1.6. Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes. A.7.2.1. La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización. A.7.2.2. Se deben desarrollar e implementar un conjunto de procedmientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.	2	3	3	0,6	6	4	24
AI28.2	10	A.11.1.1. Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales. A.11.2.1. Debe existir un procedimiento formal para a inscripción y desinscripción para otorgar acceso a todos los sistemas servicios de información. A.11.2.2. Se debe restringir y controlar la asignación y uso de privilegios. A.11.2.3. La asignación de claves se debe controlar a través de un proceso de gestión formal A.11.2.4. La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal. A.11.3.1. Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves. A.11.4.1. Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar. A.11.4.2. Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados. A.11.6.1. Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.	2	3	3	0,6	6	2	12

AI29.2	10	A.10.5.1. Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada. A.10.1.1. Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	3	2	3	0,6	6	2	12
AI30.1	10	A.1.5.1.3. Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios reglamentarios, contractuales y del negocio. A.7.2.1. La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización. A.7.2.2. Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización. A.9.2.1. Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado A.10.7.3. Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.	2	2	2	0,4	4	3	12
AI35.2	10	A.7.2.1. La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización. A.7.2.2. Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización. A.12.2.4. Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.	3	2	3	0,6	6	3	18

AI43.1	5	A.10.10.1. Se deben producir registros de las actividades de auditoría, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso. A.10.10.2. Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado e las actividades de monitoreo se debe revisar regularmente. A.10.10.3. Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no autorizado. A.10.10.4. Se deben registrar las actividades del administrador y operador del sistema. A.10.10.5. Las fallas se deben registrar, analizar y se debe tomar la acción apropiada. A.15.3.1. Se deben planear cuidadosamente los requerimientos y actividades de las auditorias que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales. A.15.3.2. Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.	1	2	2	0,4	2	2	4
AI45.1	5	A.10.2.1. Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles e entrega incluidos en el contrato de entrega de servicio a terceros. A.10.2.3. Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la revaluación de los riesgos. A.15.2.1. Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad. A.15.2.2. Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	2	3	3	0,6	3	3	9

AI47.1	10	A.9.2.1. Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado A.10.5.1. Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada. A.10.1.1. Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten. A.14.1.3 Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.	4	4	4	0,8	8	2	16
AI48.1	10	A.9.2.1. Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado A.10.5.1. Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada. A.10.1.1. Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten. A.14.1.3. Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.	4	3	4	0,8	8	3	24
AI49.1	5	A.7.1.1. Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes. A.9.2.4. Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad. A.10.2.3. Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la revaluación de los riesgos.	3	2	3	0,6	3	4	12

AI51.1	5	A.9.2.1. Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado A.9.2.2. Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro. A.9.2.4. Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	3	2	3	0,6	3	3	9
AI58.1	10	A.10.6.1. Las redes deben estar adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utiilizando la red, incluyendo la información en tránsito. A.10.6.2. Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en casa o abastecidos nuevamente. A.10.2.1. Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles e entrega incluidos en el contrato de entrega de servicio a terceros. A.10.2.3. Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la revaluación de los riesgos.	3	2	3	0,6	6	3	18
AI61.1	10	A.10.5.1. Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada. A.10.1.1. Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	2	2	2	0,4	4	3	12
AI63.2	5	A.10.5.1. Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada. A.10.1.1. Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	3	2	3	0,6	3	3	9

AI64.1	5	A.9.1.3. Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios. A.9.1.5. Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras. A.9.2.2. El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos. A.9.2.3. El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.	3	3	3	0,6	3	2	6
AI65.1	5	A.9.1.3. Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios. A.9.1.5. Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras. A.9.2.2. El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos. A.9.2.3. El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.	3	2	3	0,6	3	2	6
AI66.1	5	A.9.1.4. Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre. A.9.1.5. Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras. A.9.2.1. El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.	3	3	3	0,6	3	2	6
AI67.1	5	A.9.1.4. Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre. A.9.1.5. Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras. A.9.2.1. El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.	2	3	3	0,6	3	2	6

AI70.1	10	A.10.1.1. Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten. A.8.2.1. La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización. A.8.2.2. Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral. A.8.2.3. Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.	2	2	2	0,4	4	3	12
AI71.1	10	A.10.1.1. Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten. A.8.2.1. La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización. A.8.2.2. Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral. A.8.2.3. Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.	2	2	2	0,4	4	3	12

AI72.1	10	A.8.1.1. Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización A.8.1.2. Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. A.8.2.1. La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización. A.8.2.2. Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral. A.8.2.3. Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.	3	2	3	0,6	6	3	18
AI75.1	5	A.5.1.1. La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes. A.5.1.2. La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad. A.6.1.1. La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información. A.6.1.3. Se deben definir claramente las responsabilidades de la seguridad de la información. A.14.1.1. Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.	3	3	3	0,6	3	5	15

AI77.1	10	A.10.5.1. Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada. A.10.1.1. Los procedimientos de operación se deben documentar, mantenery estar disponibles para todos los usuarios que los necesiten.	3	3	3	0,6	6	3	18
AI78.1	10	A.10.5.1. Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada. A.10.1.1. Los procedimientos de operación se deben documentar, mantenery estar disponibles para todos los usuarios que los necesiten.	3	2	3	0,6	6	3	18

Anexo F-02 Listado de Nivel de Riesgo Detallado – Con ISO/IEC 27001:2005[1]

ANEXO G: Cuantificación de Activos[1]

No. Activo (*Anexos C y D*)	Compra	Instalación	Implementación	Customización	Otros Costos	Valor Físico	Valor para la Empresa	Valor para los Usuarios	Propiedad Intelectual	Otros Valores	Mejora de la Productividad	Valor para la Competencia	Valoración del Mercado	Marca	Otros Valores	Otros Valores	Valor Total del Activo
	Costos (Valores Negativos)					Valores Directos					Valores Indirectos					Otros	Total
AI1.1	3,80	0,00	2,83	0,00	3,25	577,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	123,75	0,00	**691.372**
AI5.1	29,40	1,50	0,00	0,00	0,19	1155,00	0,00	0,00	0,00	1443,75	0,00	0,00	0,00	0,00	0,00	0,00	**2.567.658**
AI9.3	13,20	0,00	0,00	0,00	30,00	577,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	247,50	0,00	**781.800**
AI11.1	7,26	0,00	0,00	0,00	0,28	577,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	247,50	0,00	**817.464**
AI12.2	30,26	0,00	2,83	0,00	5,75	577,50	2310,00	3465,00	1732,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	**8.046.167**
AI16.1	305,39	0,00	0,00	0,00	360,00	577,50	0,00	5197,50	1732,50	0,00	1485,00	0,00	0,00	0,00	0,00	0,00	**8.327.112**
AI18.2	68,60	0,00	0,00	0,00	0,00	577,50	0,00	1732,50	0,00	0,00	990,00	0,00	0,00	0,00	0,00	0,00	**3.231.400**
AI22.1	0,00	0,00	0,00	0,00	0,00	0,00	4620,00	1732,50	3465,00	0,00	495,00	371,25	0,00	990,00	0,00	0,00	**11.673.750**
AI24.1	0,00	0,00	0,00	0,00	10,00	0,00	2310,00	1732,50	0,00	0,00	0,00	1485,00	0,00	0,00	0,00	0,00	**5.517.500**
AI25.2	0,00	0,00	0,00	0,00	1166,00	0,00	4620,00	3465,00	1732,50	0,00	0,00	1113,75	2970,00	0,00	0,00	0,00	**12.735.250**
AI26.2	0,00	0,00	0,00	0,00	1555,45	0,00	4620,00	3465,00	0,00	0,00	0,00	1856,25	3960,00	1980,00	0,00	0,00	**14.325.796**

No. Activo *(Anexos C y D)*	Compra	Instalación	Implementación	Customización	Otros Costos	Valor Físico	Valor para la Empresa	Valor para los Usuarios	Propiedad Intelectual	Otros Valores	Mejora de la Productividad	Valor para la Competencia	Valoración del Mercado	Marca	Otros Valores	Otros Valores	Valor Total del Activo
	Costos (Valores Negativos)					Valores Directos					Valores Indirectos					Otros	Total
AI28.2	0,00	0,00	0,00	0,00	50,00	0,00	2310,00	1732,50	0,00	0,00	0,00	1113,75	0,00	0,00	0,00	0,00	**5.106.250**
AI29.2	0,00	0,00	0,00	0,00	0,00	0,00	2310,00	1732,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	**4.042.500**
AI30.1	0,00	0,00	0,00	0,00	20,00	0,00	4620,00	1732,50	1732,50	0,00	0,00	742,50	5940,00	2970,00	0,00	0,00	**17.717.500**
AI35.2	19,80	16,24	0,00	0,00	13,17	0,00	4620,00	1732,50	3465,00	0,00	495,00	0,00	0,00	0,00	0,00	0,00	**10.263.290**
AI43.1	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1732,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	**1.732.500**
AI45.1	0,00	0,00	0,00	0,00	0,00	0,00	2310,00	1732,50	0,00	0,00	0,00	371,25	0,00	0,00	0,00	0,00	**4.413.750**
AI47.1	76,00	0,07	0,00	0,00	1,42	1155,00	0,00	0,00	0,00	2021,25	1485,00	0,00	0,00	0,00	0,00	0,00	**4.583.763**
AI48.1	38,08	0,07	0,00	0,00	0,46	577,50	0,00	0,00	0,00	1155,00	990,00	0,00	0,00	0,00	0,00	0,00	**2.683.890**
AI49.1	216,16	2,20	0,00	0,00	7,78	577,50	0,00	0,00	0,00	0,00	990,00	0,00	0,00	0,00	0,00	0,00	**1.341.359**
AI51.1	49,50	0,07	0,00	0,00	5,53	577,50	0,00	0,00	0,00	577,50	495,00	0,00	0,00	0,00	0,00	0,00	**1.594.899**
AI58.1	39,73	0,00	0,00	0,00	0,50	577,50	0,00	3465,00	0,00	0,00	990,00	0,00	0,00	0,00	0,00	0,00	**4.992.270**
AI61.1	15,00	0,50	0,00	0,00	0,54	577,50	0,00	0,00	0,00	577,50	0,00	0,00	0,00	0,00	0,00	0,00	**1.138.958**
AI63.2	14,62	0,55	0,00	0,00	0,97	577,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	123,75	0,00	**685.110**

No. Activo *(Anexos C y D)*	Compra	Instalación	Implementación	Customización	Otros Costos	Valor Físico	Valor para la Empresa	Valor para los Usuarios	Propiedad Intelectual	Otros Valores	Mejora de la Productividad	Valor para la Competencia	Valoración del Mercado	Marca	Otros Valores	Otros Valores	Valor Total del Activo
	Costos (Valores Negativos)					Valores Directos					Valores Indirectos					Otros	Total
AI64.1	12,30	0,70	0,00	0,00	0,38	577,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	247,50	0,00	**811.617**
AI65.1	7,59	1,39	0,00	0,00	0,46	577,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	247,50	0,00	**815.556**
AI66.1	5,00	0,20	0,00	0,00	0,05	577,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	247,50	0,00	**819.746**
AI67.1	3,57	0,23	0,00	0,00	0,35	577,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	371,25	0,00	**944.598**
AI70.1	0,00	0,00	0,00	0,00	0,00	0,00	4620,00	0,00	0,00	0,00	1485,00	0,00	0,00	990,00	0,00	0,00	**7.095.000**
AI71.1	0,00	0,00	0,00	0,00	0,00	0,00	2310,00	0,00	1732,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	**4.042.500**
AI72.1	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	1732,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	**1.732.500**
AI75.1	0,00	0,00	0,00	0,00	0,00	0,00	4620,00	0,00	0,00	0,00	0,00	371,25	6930,00	2970,00	0,00	0,00	**14.891.250**
AI77.1	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	371,25	0,00	**371.250**
AI78.1	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	247,50	0,00	**247.500**
TOTAL	**955,26**	**23,72**	**5,66**	**0,00**	**3232,54**	**11550,00**	**46200,00**	**34650,00**	**17325,00**	**5775,00**	**9900,00**	**7425,00**	**19800,00**	**9900,00**	**2475,00**	**0,00**	**160.782.825**

Anexo G - Cuantificación de Activos con riesgo ALTO y MODERADO[1]

ANEXO H-01: Expectativa de Pérdida Anual – Situación Actual[1]

Situación actual: sin ISO/IEC 27001:2005

No. Activo *(Anexos C y D)*	Impacto al Negocio *(4-04)*	Factor de Exposición: FE *(4-12)*	Valor de la Clase de Activo de Impacto al Negocio: VA *(6-16)*	Expectativa de Pérdida Simple: SLE *(FE * VA)*	Tasa Anual de Ocurrencia: ARO *(4-17)*	Valor de Expectativa de Pérdida Anual: ALE *(SLE * ARO))*
AI1.1	10	0,8	247.500,00	198.000,00	0,33	**66.000,00**
AI5.1	10	0,8	247.500,00	198.000,00	0,33	**66.000,00**
AI9.3	5	0,6	685.100,00	411.060,00	1,00	**411.060,00**
AI11.1	10	0,8	247.500,00	198.000,00	1,00	**198.000,00**
AI12.2	10	0,6	247.500,00	148.500,00	0,33	**49.500,00**
AI16.1	10	0,6	247.500,00	148.500,00	0,50	**74.250,00**
AI18.2	10	0,6	247.500,00	148.500,00	1,00	**148.500,00**
AI22.1	5	0,6	685.100,00	411.060,00	1,00	**411.060,00**
AI24.1	10	0,6	247.500,00	148.500,00	0,33	**49.500,00**
AI25.2	10	0,8	247.500,00	198.000,00	1,00	**198.000,00**
AI26.2	10	0,6	247.500,00	148.500,00	1,00	**148.500,00**
AI28.2	10	0,6	247.500,00	148.500,00	1,00	**148.500,00**

No. Activo *(Anexos C y D)*	Impacto al Negocio *(4-04)*	Factor de Exposición: FE *(4-12)*	Valor de la Clase de Activo de Impacto al Negocio: VA *(6-16)*	Expectativa de Pérdida Simple: SLE *(FE * VA)*	Tasa Anual de Ocurrencia: ARO *(4-17)*	Valor de Expectativa de Pérdida Anual: ALE *(SLE * ARO))*
AI29.2	10	0,6	247.500,00	148.500,00	0,33	**49.500,00**
AI30.1	10	0,6	247.500,00	148.500,00	0,33	**49.500,00**
AI35.2	10	0,6	247.500,00	148.500,00	2,00	**297.000,00**
AI43.1	5	0,4	685.100,00	411.060,00	2,00	**822.120,00**
AI45.1	5	0,6	685.100,00	411.060,00	1,00	**411.060,00**
AI47.1	10	1	247.500,00	247.500,00	0,33	**82.500,00**
AI48.1	10	0,8	247.500,00	198.000,00	0,33	**66.000,00**
AI49.1	5	0,6	685.100,00	411.060,00	0,33	**137.020,00**
AI51.1	5	0,6	685.100,00	411.060,00	0,67	**274.040,00**
AI58.1	10	0,6	247.500,00	148.500,00	0,67	**99.000,00**
AI61.1	10	0,6	247.500,00	148.500,00	0,33	**49.500,00**
AI63.2	5	0,6	685.100,00	411.060,00	1,00	**411.060,00**
AI64.1	5	0,6	685.100,00	411.060,00	1,00	**411.060,00**
AI65.1	5	0,6	685.100,00	411.060,00	1,00	**411.060,00**
AI66.1	5	0,8	685.100,00	548.080,00	0,17	**91.346,67**

No. Activo *(Anexos C y D)*	Impacto al Negocio *(4-04)*	Factor de Exposición: FE *(4-12)*	Valor de la Clase de Activo de Impacto al Negocio: VA *(6-16)*	Expectativa de Pérdida Simple: SLE *(FE * VA)*	Tasa Anual de Ocurrencia: ARO *(4-17)*	Valor de Expectativa de Pérdida Anual: ALE *(SLE * ARO))*
AI67.1	5	0,8	685.100,00	548.080,00	0,17	**91.346,67**
AI70.1	10	0,6	247.500,00	148.500,00	0,33	**49.500,00**
AI71.1	10	0,6	247.500,00	148.500,00	0,33	**49.500,00**
AI72.1	10	0,6	247.500,00	148.500,00	0,67	**99.000,00**
AI75.1	5	0,8	685.100,00	548.080,00	1,00	**548.080,00**
AI77.1	10	0,8	247.500,00	198.000,00	0,17	**33.000,00**
AI78.1	10	0,8	247.500,00	198.000,00	0,17	**33.000,00**
				9.056.280,00		**6.534.063,33**

Anexo H-01 - Expectativa de Pérdida Anual de Activos con riesgo ALTO y MODERADO sin la ISO/IEC 27001:2005[1]

ANEXO H-02: Expectativa de Pérdida Anual – Situación Proyectada[1]

Situación proyectada: con ISO/IEC 27001:2005

No. Activo *(Anexos C y D)*	Impacto al Negocio *(4-04)*	Factor de Exposición: FE *(4-12)*	Valor de la Clase de Activo de Impacto al Negocio: VA *(6-16)*	Expectativa de Pérdida Simple: SLE *(FE * VA)*	Tasa Anual de Ocurrencia: ARO *(4-17)*	Valor de Expectativa de Pérdida Anual: ALE *(SLE * ARO))*
AI1.1	10	0,6	247.500,00	148.500,00	0,17	**24.750,00**
AI5.1	10	0,8	247.500,00	198.000,00	0,33	**66.000,00**
AI9.3	5	0,6	685.110,00	411.066,00	1,00	**411.066,00**
AI11.1	10	0,8	247.500,00	198.000,00	1,00	**198.000,00**
AI12.2	10	0,6	247.500,00	148.500,00	0,17	**24.750,00**
AI16.1	10	0,4	247.500,00	99.000,00	0,33	**33.000,00**
AI18.2	10	0,4	247.500,00	99.000,00	1,00	**99.000,00**
AI22.1	5	0,4	685.110,00	274.044,00	0,67	**182.696,00**
AI24.1	10	0,6	247.500,00	148.500,00	0,33	**49.500,00**
AI25.2	10	0,6	247.500,00	148.500,00	0,33	**49.500,00**
AI26.2	10	0,6	247.500,00	148.500,00	0,67	**99.000,00**

No. Activo *(Anexos C y D)*	Impacto al Negocio *(4-04)*	Factor de Exposición: FE *(4-12)*	Valor de la Clase de Activo de Impacto al Negocio: VA *(6-16)*	Expectativa de Pérdida Simple: SLE *(FE * VA)*	Tasa Anual de Ocurrencia: ARO *(4-17)*	Valor de Expectativa de Pérdida Anual: ALE *(SLE * ARO))*
AI28.2	10	0,6	247.500,00	148.500,00	0,67	**99.000,00**
AI29.2	10	0,6	247.500,00	148.500,00	0,17	**24.750,00**
AI30.1	10	0,4	247.500,00	99.000,00	0,33	**33.000,00**
AI35.2	10	0,6	247.500,00	148.500,00	1,33	**198.000,00**
AI43.1	5	0,4	685.110,00	274.044,00	1,33	**365.392,00**
AI45.1	5	0,6	685.110,00	411.066,00	0,67	**274.044,00**
AI47.1	10	0,8	247.500,00	198.000,00	0,33	**66.000,00**
AI48.1	10	0,8	247.500,00	198.000,00	0,33	**66.000,00**
AI49.1	5	0,6	685.110,00	411.066,00	0,33	**137.022,00**
AI51.1	5	0,6	685.110,00	411.066,00	0,50	**205.533,00**
AI58.1	10	0,6	247.500,00	148.500,00	0,50	**74.250,00**
AI61.1	10	0,4	247.500,00	99.000,00	0,33	**33.000,00**
AI63.2	5	0,6	685.110,00	411.066,00	0,67	**274.044,00**

No. Activo *(Anexos C y D)*	Impacto al Negocio *(4-04)*	Factor de Exposición: FE *(4-12)*	Valor de la Clase de Activo de Impacto al Negocio: VA *(6-16)*	Expectativa de Pérdida Simple: SLE *(FE * VA)*	Tasa Anual de Ocurrencia: ARO *(4-17)*	Valor de Expectativa de Pérdida Anual: ALE *(SLE * ARO))*
AI64.1	5	0,6	685.110,00	411.066,00	1,00	**411.066,00**
AI65.1	5	0,6	685.110,00	411.066,00	1,00	**411.066,00**
AI66.1	5	0,6	685.110,00	411.066,00	0,17	**68.511,00**
AI67.1	5	0,6	685.110,00	411.066,00	0,17	**68.511,00**
AI70.1	10	0,4	247.500,00	99.000,00	0,33	**33.000,00**
AI71.1	10	0,4	247.500,00	99.000,00	0,33	**33.000,00**
AI72.1	10	0,6	247.500,00	148.500,00	0,50	**74.250,00**
AI75.1	5	0,6	685.110,00	411.066,00	0,67	**274.044,00**
AI77.1	10	0,6	247.500,00	148.500,00	0,17	**24.750,00**
AI78.1	10	0,6	247.500,00	148.500,00	0,17	**24.750,00**
				7.826.748,00		**4.510.245,00**

Anexo H-02 - Expectativa de Pérdida Anual de Activos con riesgo ALTO y MODERADO con la ISO/IEC 27001:2005[1]

ANEXO I: Costos de los Controles a implementar en la empresa

No. Activo *(Anexos C y D)*	Control *(Anexo D-02)*	Proyecto	Costo Proyecto	Soporte Técnico	Gerencia	Dirección	TOTAL
AI1.1	Disponer de un equipo para contingencia en la empresa o site alterno	Proyecto de site alterno	114.000	4.000	4.000	2.500	**124.500**
AI5.1	Documentar las configuraciones y procedimientos de restauración de discos, sistemas operativos y demás elementos del ambiente de producción	Tiempo del personal de TI		1.000	800	100	**1.900**
AI9.3	Establecer estándares de servicio, e incorporar herramientas para el registro y seguimiento de solución a requerimientos.	Proyecto con software libre. GLPI - OCS - JASPER	3.000	2.000	2.000	500	**7.500**
AI11.1	Asignar un responsable del servicio, redefinir planes de mantenimiento y establecer parámetros de cumplimiento.	Presupuesto anual asignado para contratación de 1 persona	20.000				**20.000**
AI12.2	Disponer de un equipo para contingencia en la empresa o site alterno	Proyecto de site alterno					
AI16.1	Establecer el proceso de control de cambios que garantice que las modificaciones minimicen el impacto al ambiente de producción	Implementación del proceso	0	2.000	2.000	100	**4.100**
AI18.2	Implementar un control integral del inventario de Hardware, Software y licencias.						

No. Activo *(Anexos C y D)*	Control *(Anexo D-02)*	Proyecto	Costo Proyecto	Soporte Técnico	Gerencia	Dirección	TOTAL
AI22.1	Fomentar la planeación estratégica en la organización y de TI, creando una cultura de compromiso orientada a la atención de objetivos fundamentales	Contratar consultoría para planeación estratégica empresarial y PETI	15000				**15.000**
AI24.1	Presentar al cliente información en línea del estado de sus requerimientos para su adecuado control y seguimiento	Proyecto formulario pedidos por internet e información para proveedores y clientes	2.320	1.000	1.000	100	**4.420**
AI25.2	Definir responsabilidades y establecer niveles de autorización para aprobaciones de créditos	Parte proporcional proyecto WF. Con Sharepoint	3.783	4.000	1.000	500	**9.283**
AI26.2	Establecer responsables en cada sitio del manejo de los archivos documentales.	Mejoramiento de archivos en sucursales, 2000 usd. Por sucursal	18.000				**18.000**
AI28.2	Mejorar las restricciones de acceso y permitir el ingreso a Usuarios solo a datos autorizados para su gestión	Revisión de seguridades en sistema ERP	0	1.000	2.000		**3.000**
AI29.2	Disponer de un equipo para contingencia en la empresa o site alterno	Proyecto de site alterno					**0**
AI30.1	Disponer de ambientes para almacenamiento de información crítica de la empresa, con sus respectivos procedimientos de respaldo	Incremento de discos (1326 USD) y proyecto de file server (2720 USD)	4.046	667	40		**4.753**

No. Activo *(Anexos C y D)*	Control *(Anexo D-02)*	Proyecto	Costo Proyecto	Soporte Técnico	Gerencia	Dirección	TOTAL
AI35.2	Generar información Gerencial, mediante una herramienta gráfica basada en los indicadores de gestión de cada proceso	Proyecto de BI con Business Objects, como parte del nuevo sistema ERP.	200.000	12.000	2.000	2.500	**216.500**
AI43.1	Redefinición de pistas de auditoría y generación de procesos de traslado de información de auditoría hacia históricos			6.000	2.000	2.000	**10.000**
AI45.1	Estandarizar en la organización las políticas y procedimientos para adquisiciones		0	600	400	100	**1.100**
AI47.1	Establecer un site alterno y realizar la actualización de procedimientos de administración tecnológica, enfatizando la continuidad de los servicios.	Proyecto de site alterno					**0**
AI48.1	Establecer un site alterno y realizar la actualización de procedimientos de administración tecnológica, enfatizando la continuidad de los servicios.	Proyecto de site alterno					**0**
AI49.1	Establecer una política y procedimientos para el dimensionamiento, remplazo y reasignación de equipos.	Plan de renovación 2012 (59 desktops y 5 laptops) - incluye migración	67.290				**67.290**
AI51.1	Establecer una política y procedimientos para el dimensionamiento, ubicación, estandarización y remplazo de equipos.	Proyecto de outsourcing de impresión	89.880				**89.880**

No. Activo *(Anexos C y D)*	Control *(Anexo D-02)*	Proyecto	Costo Proyecto	Soporte Técnico	Gerencia Dirección	TOTAL
AI58.1	Actualizar acuerdos de servicio con el proveedor y definir esquemas de contingencia para solventar problemas en enlaces críticos	Enlace alterno Aloag - Telconet, estimado en base a enlace aloag-quito de 2mb	2.400			**2.400**
AI61.1	Actualizar procedimientos de respaldo y restauración de información, enfatizando confirmaciones periódicas automáticas de su realización	Revisión de procedimientos		2.000	1.000	**3.000**
AI63.2	Establecer totales de control y respaldos de la información trasladada desde los dispositivos hacia las bases de datos de nómina, para disponer de elementos para cuadre y verificación de información	Estimado para desarrollar reportes de cuadre de información enviada desde dispositivos	1500			**1.500**
AI64.1	Definir estándares para instalaciones de energía regulada y no regulada, que deben aplicarse en todas las oficinas de la empresa.	Estandarización de procedimientos de instalación		1.000	400	**1.400**
AI65.1	Realizar un inventario de equipos UPS y establecer un contrato de mantenimiento con proveedores de este tipo de equipos	La empresa a invertido 12300 usd. En equipos, se calcula 15% anual para mantenimiento.	1.845			**1.845**
AI66.1	Establecer las necesidades para control de incendios y ejecutar su implementación, con equipo que permita el monitereo automático	Se cotiza equipos para Centro de cómputo principal (Cot. CELCO)	11.500			**11.500**
AI67.1	Establecer las necesidades de aire acondicionado y ejecutar su implementación, con equipo que permita el monitereo automático	Se cotiza equipos para Centro de cómputo principal (Cot. CELCO)	17.405			**17.405**

No. Activo *(Anexos C y D)*	Control *(Anexo D-02)*	Proyecto	Costo Proyecto	Soporte Técnico	Gerencia	Dirección	TOTAL
AI70.1	Disponer de cursos de entrenamiento para personal nuevo de la empresa, como parte de su proceso de inducción.	Se evaluará proyecto con MOODLE, software de tipo libre, se definen 2000 usd. Para equipamiento	2.000	4.000	800	200	**7.000**
AI71.1	Establecer las necesidades de capacitación en tecnología en la organización y establecer planes de entrenamiento	Se definen 2 cursos anuales para cada persona del área. (total estimado al año 10 cursos de 750 dólares cada uno)	7.500				**7.500**
AI72.1	Incorporar personal de la empresa para que coordine este servicio e incorporar herramientas para ingreso, asignación, seguimiento y solución de requerimientos	Presupuesto anual asignado para contratación de 1 persona					
AI75.1	Crear compromiso en el nivel directivo de la organización y definir un plan de incorporación de estándares y metodologías de seguridad de la información	Proyecto ISO 27001	45.650				**45650**
AI77.1	Definir procedimientos y esquemas de respaldo de configuración de ambientes críticos	Procedimientos		4.000	1.000		**5.000**
AI78.1	Definir procedimientos y esquemas de respaldo de configuración de ambientes críticos	Procedimientos					**0**
TOTAL CONTROLES							**701.426**

Anexo I – Costo de Controles del Anexo A de la ISO/IEC 27001:2005