	INSTITUCIÓN UNIVERSITARIA BELLAS ARTES Y CIENCIAS DE BOLÍVAR	**Código: SM-FO-003**
	SOPORTE Y MEJORAMIENTO AL SGC	**Versión: 1**
	FORMATO DE IDENTIFICACIÓN DE RIESGOS TIC	**Fecha de aprobación: 30/10/2009**

					ANALISIS DE RIESGOS					EVALUACIÓN DE RIESGOS							CALIFICACIÓN DE RIESGO RESIDUAL					TRATAMIENTO			
(1) CÓDIGO	**(2) RIESGO**	**(3) DESCRIPCIÓN**	**(4) CAUSAS**	**(5) CONSECUENCIAS**	**(6) VALOR**	**(7) PROBABILIDAD**	**(8) VALOR**	**(9) IMPACTO**	**(10) SEVERIDAD (Riego Inherente)**	**(11) CONTROL**	**(12) DESCRIPCIÓN DEL CONTROL**	**(13) TIPO DE CONTROL**	**(14) ESTA DOCUMENTADOT**	**(15) DONDE ESTA DOCUMENTADO**	**(16) APLICACIÓN**	**(17) EFICACIA DEL CONTROL**	**(18) FRECUENCIA DEL CONTROL**	**(19) VALOR**	**(20) PROBABILIDAD**	**(21) VALOR**	**(22) IMPACTO**	**(23) SEVERIDAD**	**ACCIÓN DE TRATAMIENTO**	**(25) TIEMPO DE IMPLEMENTACIÓN**	**(26) COSTO**	**(27) RESPONSABLE**
GTIC-R1	Inadecuada adquisicion de software y hardware	1. Adquirir un software que no cumpla los requerimientos y las necesidades de la universidad. 2. Adquirir activos de comunicación (sw, router, etc) que no cumpla los requerimientos y las necesidades de la universidad	1.Suministro y/o captura inadecuada de la información de requerimiento y/o necesidades del software 2. Desconocimiento de las caracteristicas de los dispositivos	1. Perdidas economicas 2. Indisponibilidad de los sistemas de información 3. Inestabilidad de los procesos - fallas en la red de datos	10	MEDIA	2	MODERADO	20	Evalución de experto	Diagnostico sobre ventajas y desventajas del software	PREVENTIVO	NO	Plan de compras	SI	ALTA	Según Ocurrencia	5	BAJA	2	MODERADO	10	Considerar la participación de la(s) persona experta, preferiblemente directamente con el fabricante.	Según Ocurrencia	Bajo	Gestión TIC
GTIC-R2	Uso indebido de la información	Posibilidad de que se acceda, manipule y/o divulgue sin autorización la información privilegiada o de reserva que se origine, suministre o custodie en los sistemas de información	1. Bajo nivel de seguridad para el acceso a la información. 2. Desconocimiento de las politicas de manejo de información. 3. Actos mal intencionados de terceros. 4. Acceso no autorizado a información. 5. Fraude interno.	1. Mala imagen 2. Toma de decisiones no adecuadas 3. Filtración de información clasificada 4. Perdida de información	10	MEDIA	2	MODERADO	20	1. Mejoramiento de la jerarquia de usuarios. 2. Divulgación de las politicas de manejo de la información. 3. Monitoreo a los sistemas de información. 4. Procedimientos para la asignación de roles y accesos a los sistemas de información.	1. Establecimiento de roles y responsabilidades en los sistemas de información. 2. Optimización de los controles en los sistemas de información. 3. Actualización mensual de acuerdo a informe de Talento Humano sobre contratación y retiro de personal. 4. Actualización mensual de acuerdo a reporte de	PREVENTIVO	NO	1. Politicas de seguridad de la información. 2. Manuales de administración de los sistemas de información. 3. Manual de contratación 4. Manual de Talento Humano	SI	ALTA	Mensual	5	BAJA	1	LEVE	5	Reasignación de Roles en el sistema, implementación de mas niveles de seguridad, socialización de las politicas de manejo de información	Mensual	Medio	Contraqtaciones Talento Humano Gestión TIC
GTIC-R3	Vulnerabilidad del sistema de información	1. Probabilidad que terceros entre de forma indebida o fraudulenta a los sistema de información de la Universidad, para alterar, hurtar o dañar la información. 2. Probabilidad de que los sistemas de información no se encuentren debidamente actualizados.	1. Inadecuado nivel de seguridad para el acceso a la información. 2. Cortafuegos sin la configuración adecuada o sin configuración. 3. Bugs en los sistemas de información. 4. Desconocimiento en estándares para laimplementación de seguridad de los sistemas de información.	1. Perdidas economicas. 2. Indisponibilidad de los sistemas de información. 3. Fuga de información. 4. Perdida de Integridad, Disponibilidad y Confidencialidad de la información.	20	ALTA	3	CATASTROFICO	60	1. Fortalecimiento de las reglas de los cortafuegos. 2. Procedimientos de control para la detección de vulnerabilidades en los sistemas de información. 3. Aplicación de buenas practicas para el desarrollo e implementación de sistemas de información seguros.	1. Verificar periódicamente que las reglas de cortafuegos estén funcionando adecuadamente. 2. Verificar periódicamente las actualizaciones de las aplicaciones y sistemas de información. 3. Verificar periódicamente que el desarrollo de las aplicaciones se lleva a cabo usando buenas prácticas de seguridad.	PREVENTIVO	NO	1. Politicas de seguridad de la información. 2. Documen tación de reglas de Cortafuegos. 3. Politica de actualizaciones de software. 4. Politicas de desarrollo de software seguro.	SI	ALTA	Mensual	10	MEDIA	1	LEVE	10	Robustecer la seguridad mejorando los cortafuegos. Aplicar buenas practicas en el desarrollo de sistemas de información seguros.	Mensual	Medio	Gestión TIC
GTIC-R4	Daños, deterioro o pérdida de los recursos tecnológicos	Posibilidad de que se presenten daños, fallas o perdidas de los recursos tecnologicos, en su uso, y/o almacenamiento .	1.Falta y/o inadecuado mantenimiento de los recursos tecnologicos 2.Baja calidad de los recursos tecnologicos 3. Inadecuado uso de los recursos tecnologicos 4. Falta de capacitación sobre el adecuado uso de los recursos tecnologicos. 5. Falta de protección de los recursos tecnologicos. 6. Terrorismo. 7. Factores ambientales	1. Equipos dañados. 2. Desprovechamientos de los recursos tecnologicos. 3. Indisponibilidad de los servicios de información o de información necesaria.	10	MEDIA	2	MODERADO	20	1. Mantenimiento preventivo de los equipos. 2. Instalación y verificación software de seguridad. 3. Verificación de los tomas electricos, con el fin de establecer que el voltaje sea el apropiado para la instalaciónn de los equipos. 4. Capacitaciones a los usuarios sobre el uso de los equipos a su cargo. 5. Instalación de los equipos en lugares apropiados.	1. Programa de mantenimiento periódico de los equipos. 2. Verificación perdiódica de las herramientas de seguridad. 3. Mantenimiento preventivo de dispositivos de protección del fluido eléctrico. 4. Verificación de los puntos electricos, con el objetivo de detectar alguna falla en el fluido que puedad afectar el funcionamiento de los recursos tecnologicos. 5. Verificación periódica de las	PREVENTIVO	NO	1. Programa de mantenimeinto preventivo de los equipos de cómputo. 2. Programa de mantenimiento de dispositivos de protección eléctrica. 3. Programa de verificación de instalaciones físicas.	SI	ALTA	Trimestral	5	BAJA	2	MODERADO	10	1. Mantenimientos preventivos de software y hardware. 2. Revisiones periódicas de las instalaciones físicas.	Trimestral	Medio	Gestión TIC Gestión de Recursos Fisicos Personal de todas la áreas
GTIC-R5	Ausencia y/o deficiencia en los software y sistemas de información	Hace referencia a la falta y/o deficiencia en los software y/o sistemas de información.	1. Demora en el tramite de compra de los recursos necesitados. 2. Falta y/o inadecuado mantenimiento de los recursos tecnologicos 3. Baja calidad de los recursos tecnologicos	1. Cambios de precios de compras. 2. Mantenimientos preventivos y correctivos insuficientes. 3. Soporte técnico insuficiente por parte del faricante/desarrollador	10	MEDIA	2	MODERADO	20	1. Negociar dentro de términos aceptables con el proveedor. 2. Determinar las caracteristicas adecuadas del software, sistema de información o hardware. 3. Cumplir con los cronogramas de mantenimientos preventivos. 4. Adquirir productos y/o servicios reconocidos.	Asegurar la apropiación oportuna de tecnología y su mantenimiento y soporte anual.	PREVENTIVO	NO	1. Politicas de compras 2. Plan anual de mantenimientos preventivos. 3. Documento de requerimientos tipo para hardware y software.	SI	ALTA	Según Ocurrencia	10	MEDIA	2	MODERADO	20	Participación activa del experto en la determinación de adquirir tecnologia	Según Ocurrencia	Medio	Gestión TIC Gestión de Recursos Fisicos
GTIC-R6	Inadecuada utilizacion del portal institucional	Hace referencia a la subutilización del portal por parte de la comunidad universitaria	1. Falta de cultura tecnologica 2. Falta de información sobre el uso y la utilizada 3. Falta de capacitación 4. Falta de socialización sobre el contenido del sitio web	Desinformación de la comunidad universitaria	5	BAJA	1	LEVE	5	Capacitación y divulgación del portal web	A traves de cursos y/o manuales de usuario	PREVENTIVO	NO	Manual del sitio web	SI	ALTA	Según Ocurrencia	5	BAJA	1	LEVE	5	Involucrar en el plan de capacitación institucional el uso adecuado del portal	Según Ocurrencia	Bajo	Talento Humano Bienestar Universitario Gestión TIC
GTIC-R7	Fallas en las telecomunicaciones	Posibilidad de que se presenten fallas en las telecomunicaciones (internet, redes, intranet, servicio telefonico)	1. Falta de disponibilidad del servicio por parte del proveedor 2. Falta de mantenimiento de los equipos y redes 3. Deterioro de las redes 4. Operación inadecuada de los recursos por parte de usuarios y/o tecnicos. 6. Falla en las comunicaciones. 7. Fluctuación en el fluido eléctrico	1. Perdida de información, demora en los procesos,perdidad de la imagen de la entidad ante el publico 2. Información inoportuna 3. Incumplimiento del proceso 4. Alteración de la operación.	20	ALTA	2	MODERADO	40	Mantenimiento preventivo y periódico de los dispositivos de red y comunicaciones	1. Se debe establecer un plan anual para revisar conexiones y estado de la infraestructura física de los dispositivos. 2. Se debe contar con contratos de soporte y mantenimiento con los proveedores de los equipos de red y comunicaciones.	PREVENTIVO	NO	Plan anual de mantenimiento	SI	ALTA	Según Ocurrencia	10	MEDIA	2	MODERADO	20	1. Mantenimiento preventivo de dispositivos de red 2. Adquisición periódica de dispositivos de acuerdo a necesidades	Según Ocurrencia	Alto	Gestión TIC
GTIC-R8	Fallas en el fluido eléctrico	Posibilidad de que se presenten fallas en el fluido eléctrico de la entidad para el desarrollo de sus operaciones	1. Fluctuaciones en el fluido electrico. 2. Falta de protección ante pico de voltajes y/o interrupción del fluido electrico no planificado (Redundancia de Energia).	1. Perdida de información 2. Demora en los procesos 3. Perdidad de la imagen de la entidad ante el publico 4. Información inoportuna 5. Incumplimiento del proceso 6. Alteración de la operación.	20	ALTA	2	MODERADO	40	1. Verificación de las condiciones operativas de las instalaciones eléctricas. 2. Verificación de las condiciones operativas de los dispositivos que intervienen en la distribución eléctrica interna. 3. Compra de dispositivos de	1. Se debe establecer un plan anual para revisar conexiones y estado de la infraestructura física de los dispositivos. 2. Se debe contar con contratos de soporte y mantenimiento con los proveedores de los equipos de red y comunicaciones.	Preventivo	NO	Plan de compras Plan anual de mantenimiento	SI	Alta	Según Ocurrencia	5	BAJA	2	MODERADO	10	Lograr la redundancia electrica en la institución	Según Ocurrencia	Alto	Gestión TIC Gestión de Recursos Fisicos
GTIC-R9	Desconocimiento de los avances del Plan Estrátegico	Falta de presentación del informe de gestión	Elaboración inadecuada o nula del informe. Falta de solcialización del PETI en el area de tecnologia.	1. Incumplimiento normativo 2. Desinformación de los planes TIC institucionales	5	BAJA	1	LEVE	5	Mantener cronograma de acopio de información	Involucrar a todas las instancias que suministran información	PREVENTIVO	NO	Plan Estratégico Institucional PETI	SI	ALTA	Según Ocurrencia	5	BAJA	1	LEVE	5	Divulgación del plan	Según Ocurrencia	Bajo	Procesos involucrados
GTIC-R10	Incumplimiento en las capacitaciones de seguridad al personal	No realización en la capacitaciones de seguridad al personal	1. Falta de disponibilidad del personal institucional 2. Fallos en los dispositivos de visualización 3. Fallos en los equipos de la capacitación	Incumplimiento del programa de capacitaciones	5	BAJA	2	MODERADO	10	1. Diseñar programa de capacitaciones 2. Coordinación adecuada de la logistica 3. Manejar un plan de medios	Se debe contar con un plan anual de capacitaciones acorde con las necesidades de la institución y coordinar con el área encargada de la lógistica y divulgación interna para su cumplimiento.	PREVENTIVO	NO	Plan anual de capacitaciones	SI	Media	Trimestral	5	BAJA	2	MODERADO	10	Designar tareas y controlar las responsabilidades de acuerdo con el plan de capacitaciones y de cada una de los eventos	Según Ocurrencia	Medio	Seguridad de la información Gestión de recursos fisicos Oficina asesora de prensa

GTIC-R11	Humedad producida por sistemas de refrigeración inadecuados y/o filtraciones de agua	Daños en la infraestructura física y tecnológica producida por condensación, hongos, bacterias, acaros.	1. Gas instantáneo en la Linea de Liquido 2. Restricciones en la Linea de Liquido 3. Diseño Inadecuado de Tubería 4. Subenfriamiento Inadecuado 5. Baja Presión de Condensación 6. Carga Excesiva en el Evaporador 7. Problemas y Soluciones 8. Baja Presión de Condensación 9. Control del humidificador 10. Contaminación en el Sistema. 11. Falta de un sistema de refrigeración que cuenta con características apropiadas para evitar otros problemas	1. Hospitalizaciones 2. incapacidades 3. Muerte 4. Perdida de información 5. Interrupción de procesos y/o servicios de información 6. Daños físicos de planta 7. Daños en infraestructura tecnologica	20	ALTA	3	CATASTROFICO	60	Evalución de experto, Mantenimientos preventivos y programados	Diagnostico del sistema de refrigeración y mantenimiento	Correctivo	NO	Politica de mantenimiento de infraestructura física	SI	Media	Cuando se presenta	10	MEDIA	2	MODERADO	20	1. Reporte al contratista encargado del area de salud ocupacional y la ARP para realizar las diferentes actividades que se requieran. 2. Solicitud de actualización al procedimiento DE MANTENIMIENTO CORRECTIVO Y SERVICIOS (Servicios Generales) a nivel preventivo. 3. Programación de mantenimiento por parte de servicios generales. 4. Solicitud de estudio microbiologico de ambiente a Ciencias Básicas.	Según Ocurrencia	medio	Talento Humano Servicios Generales Gestión TIC Contratistas mantenimiento
GTIC-R12	Accesos no autorizados a las instalaciones del area tecnologica	Ingreso de personas no autorizadas para la manipulación de equipos tecnologicos	1. Inadecuado control de acceso a las instalaciones 2.Puertas no aptas para la seguridad	1. Perdida, daños 2. Manipulación 3. Robos en la infraestructura tecnologica	20	ALTA	3	CATASTROFICO	60	1. Reforzar el acceso fisico a las instalaciones de tecnologia 2. Observación permanente del area	1. Instalacion de nuevas cerraduras 2. Cambio de puerta 3. Monitorización de ingresos a las instalaciones de informatica	PREVENTIVO	NO	1. Politica de seguridad de la información 2. Politica de acceso de la institución	SI	Alta	Cuando se presenta	10	MEDIA	2	MODERADO	20	Robustecer el control de acceso físico en el area	Según Ocurrencia	Medio	Gestión de recursos físicos y tecnológicos Gestión TIC Empresa de vigilancia Servicios generales