SISTEMA DE ALERTAS DE SEGURIDAD INFORMÁTICA PARA LOS SERVICIOS CRÍTICOS DE LA DIVISIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DE LA UNIVERSIDAD DEL CAUCA (FASE I DEL PROYECTO SGSI-UNICAUCA)

ANEXO

ANDRÉS FELIPE MERA ARCOS
OSCAR EDUARDO MONDRAGON MACA

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE SISTEMAS
LINEA DE INVESTIGACIÓN: SEGURIDAD INFORMÁTICA
POPAYÁN
ABRIL de 2012

SISTEMA DE ALERTAS DE SEGURIDAD INFORMÁTICA PARA LOS SERVICIOS CRÍTICOS DE LA DIVISIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DE LA UNIVERSIDAD DEL CAUCA (FASE I DEL PROYECTO SGSI-UNICAUCA)

ANEXO

ANDRÉS FELIPE MERA ARCOS
OSCAR EDUARDO MONDRAGON MACA

Documento Final de Trabajo de Grado para optar al título de Ingeniero en Electrónica y Telecomunicaciones

Director
Ing. SILER AMADOR DONADO

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE SISTEMAS
LINEA DE INVESTIGACIÓN: SEGURIDAD INFORMÁTICA
POPAYÁN
ABRIL de 2012

ANEXOS

ANEXO A: Listas de chequeo y tablas comparativas

Tabla A.1. Identificación de los objetivos de control presentes en la División de TIC de la Universidad del Cauca.

LISTA DE CHEQUEO PARA IDENTIFICAR LOS CRITERIOS DE GESTION CON LOS QUE CUENTA LA DIVISION DE TIC DE LA UNIVERSIDAD DEL CAUCA CON BASE EN LA NORMA ISO/IEC 27001						
ENTIDAD: División de Tecnologías de la Información y la comunicación de la Universidad del Cauca						
FECHA DE REALIZACION DE LA LISTA DE CHEQUEO: 23 – Marzo - 2011						
PARTICIPANTES EN EL LLENADO DE LOS DATOS Y SU RESPONSABILIDAD Alexis Adolfo Solarte Fabián Andrés Mera						
REALIZADO POR: Andrés Felipe Mera Oscar Eduardo Mondragón						
1	**Políticas de seguridad**				**SI**	**NO**	**Observaciones**
1.1		Política de seguridad de la información.					*No aprobadas.*
1.1.1			Documentación y revisión regular las políticas de seguridad de la información.			x	
2	**Organización de la seguridad de la información**						
2.1		Organización interna.					
2.1.1			Compromiso de los administradores en el reconocimiento de las responsabilidades de la seguridad de la información.		✓		*Ciertas áreas.*
2.1.2			Coordinación de la seguridad de la información por representantes de la división de las TIC's.			x	
2.1.3			Asignación de responsabilidades de la seguridad de la información en la división de las TIC's.			x	
2.1.4			Proceso de autorización por parte de los administradores para los nuevos medios de			x	

			procesamiento de información.			
2.1.5			Identificación y revisión en los acuerdos de confidencialidad para la protección de la información.	✓		*No estandarizados.*
2.1.6			Existencia de contactos con grupos de seguridad especializados o asociaciones profesionales.		x	
2.1.7			Revisión independiente cuando ocurran cambios significativos en la seguridad de la información.		x	
2.2		Organización externa.				
2.2.1			Identificación de los riesgos relacionados con entidades externas antes de otorgar los accesos.	✓		*No hay protocolo o lineamiento.*
2.2.2			Tratamiento de la seguridad cuando se trabaja con clientes y terceras personas.	✓		*No estandarizado.*
3	**Gestión de activos**					
3.1		Responsabilidad por los activos.				
3.1.1			Elaboración y mantenimiento de los activos importantes.	✓		
3.1.2			Selección del propietario de los activos en la división de TIC.		x	
3.1.3			Identificación, documentación e implementación para el uso aceptable de los activos asociados con los medios de procesamiento de la información.	✓		*Fase inicial.*
3.2		Clasificación de la información.				
3.2.1			Clasificación y manejo de la información según requerimientos legales, confidencialidad.	✓		*No hay estándar.*
4	**Seguridad de los recursos humanos**					
4.1		Antes del empleo.				
4.1.1			Selección del personal mediante la verificación de antecedentes, conducta ética y profesional.	✓		*Monitorias.*
4.2		Durante el empleo.				
4.2.1			Capacitación y actualizaciones regulares en las políticas de la seguridad de la información.		x	
4.2.2			Existencia de un proceso disciplinario ante empleados que violen la seguridad de la información.		x	*No reglamentado.*
4.3		Terminación o cambio de empleo				
4.3.1			Devolución de activos por parte del personal al término de su contrato.		x	

4.3.2			Eliminación de derechos de acceso al personal cuando finalice su contrato.		x	
5	**Gestión de las comunicaciones**					
5.1		Planeación y aceptación del sistema.				*No documentado.*
5.1.1			Criterios de aceptación para nuevos sistemas o actualizaciones.		x	
5.2		Protección contra software malicioso y código móvil.				
5.2.1			Detección, prevención y recuperación contra software malicioso y códigos móviles.		x	
5.3		Respaldo				
5.3.1			Realización frecuente de copias de seguridad (Back-up).	✓		
5.4		Gestión de seguridad de redes.				
5.4.1			Protección de la información mediante controles en la seguridad de los servicios de red.	✓		
5.5		Gestión de medios				
5.5.1			Procedimientos formales y seguros en la eliminación de los activos.		x	
5.5.2			Procedimientos de manejo y almacenamiento de la información para su protección.	✓		
5.6		Intercambio de información.				
5.6.1			Procedimientos y políticas en el intercambio de información y software.		x	
5.6.2			Protección en el envío de Mensajes electrónicos.		x	
5.7		Monitoreo.				
5.7.1			Producción de registros de auditorías, excepciones y eventos de seguridad de la información.	✓		*Fase inicial.*
5.7.2			Existencia de un sistema de monitoreo y revisión regular del resultado de las actividades.	✓		*Aplicación helpdesk*
5.7.3			Protección de la información del registro contra alteraciones y accesos no autorizados.		x	
5.7.4			Registro de las actividades de los administradores y operadores.		x	
5.7.5			Registro y análisis correspondiente ante fallas del sistema.		x	
6	**Control de acceso**					
6.1		Gestión del acceso del usuario				

6.1.1			Existencia de procedimientos formales para la inscripción del usuario que otorga acceso a servicios y sistemas de información.		x	
6.1.2			Existencia de gestión de privilegios.		x	
6.1.3			Existencia de proceso de gestión formal para la asignación de claves de usuario.		x	
6.1.4			Revisión de derechos de acceso de usuario en intervalos constantes.		x	
6.2		Control de acceso a redes.				
6.2.1			Aplicación de políticas sobre el acceso a servicios por parte de usuarios autorizados.	✓		
6.2.2			Autenticación del usuario para conexiones remotas.	✓		
6.2.3			Identificación automática de equipo en red como medio de autenticación.		x	
6.2.4			Protección de acceso físico y lógico al puerto de diagnostico remoto.		x	
6.2.5			Segregación de información, usuarios y sistemas de información en las redes.		x	
6.2.6			Existencia de controles de conexiones de redes que restringa la capacidad de acceso de los usuarios en las redes compartidas.	✓		
6.3		Control de acceso al sistema de operación				
6.3.1			Existencia de procedimientos de registro en el terminal para controlar el acceso a los servicios operativos.		x	
6.3.2			Identificación y autenticación del usuario para uso personal y exclusivo (ID de usuario).	✓		
6.3.3			Existencia de sistemas de gestión de claves que asegure la calidad de las claves.		x	
6.3.4			Restricción y control de uso de programas de utilidades que podrían superar el sistema.		x	
6.3.5			Sesiones inactivas se cierran después de un periodo de inactividad definido.	✓		
6.3.6			Restricción sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.		x	*Manejado por aplicativos.*
7	**Adquisición, desarrollo y mantenimiento de los sistemas de información**					
7.1		Procesamiento correcto en las aplicaciones.				
7.1.1			Validación de los datos de entrada en las aplicaciones para asegurar que la data sea correcta y segura.		x	
7.1.2			Control de procesamiento interno a través de		x	

			chequeos de validación en las aplicaciones que detecten cualquier corrupción de la información.			
7.2		Controles criptográficos.				
7.2.1			Existencia de políticas sobre el uso de controles criptográficos para la protección de la información.	✓		*Hay mecanismos pero no son suficientes.*
7.2.2			Utilización de gestión de clave para dar soporte al uso al uso de las técnicas de criptografía en la organización.		x	
7.3		Seguridad de los archivos del sistema				
7.3.1			Control de instalación de software en los sistemas operacionales.		x	
7.3.2			Control de acceso al código fuente del programa.	✓		*A medias.*
7.4		Seguridad en los procesos de desarrollo y soporte				
7.4.1			Procedimientos de revisión y control de las aplicaciones después de cambios en el sistema operativo.		x	
7.4.2			Prevención contra la filtración de la información.		x	
7.5		Gestión de vulnerabilidad técnica.				
7.5.1			Control, evaluación y solución de vulnerabilidades técnicas para tratar el riesgo asociado.		x	
8	**Gestión de incidentes en la seguridad de la información**					
8.1		Reporte de eventos y debilidades en la seguridad de la información				
8.1.1			Reporte de eventos en la seguridad de la información a través de los canales gerenciales apropiados lo más rápidamente posible.		x	
8.1.2			Reporte de cualquier debilidad observada o sospechosa en la seguridad de los sistemas o servicios por parte de empleados, contratistas y terceros usuarios.		x	
8.2		Gestión de incidentes y mejoras en la seguridad de la información.				
8.2.1			Existencia de responsabilidades y procedimientos gerenciales para asegurar una respuesta eficiente ante incidentes de seguridad de la información.	✓		*No estandarizado.*
8.2.2			Existencia de mecanismos que permitan		x	

			cuantificar los tipos, volúmenes y costos de los incidentes en la seguridad de la información.				
9	**Cumplimiento**						
9.1		Cumplimiento con las políticas y estándares de seguridad y el cumplimiento técnico					
9.1.1			Asegurar el cumplimiento de las políticas y estándares de seguridad que permitan que los procedimientos de seguridad sean realizados correctamente.		x		
9.1.2			Chequeo de cumplimiento con los estándares de implementación de la seguridad en los sistemas de información.		x		
9.2		Consideraciones de auditoría de los sistemas de información.					
9.2.1			Planeación de controles de auditoría en los sistemas de información.		x		
TOTAL				21	43	**Cumple (%)**	32.81
						No Cumple (%)	67.19

- **Cumple (%)** = Cumple con un porcentaje de los criterios de gestión evaluados en la norma ISO/IEC 27001.
- **No Cumple (%)** = No cumple con un porcentaje de los criterios de gestión evaluados en la norma ISO/IEC 27001.

ANALISIS DE RESULTADOS
Se concluye que a pesar de haber ciertos lineamientos implementados en la División de TIC de la Universidad del Cauca, sigue existiendo un gran déficit de reglamentos y controles los cuales permitirán aumentar la seguridad de los activos de la información. Los controles implementados se encuentran muchos en etapa de prueba o de estandarización, por lo que se debe realizar una rápida acreditación e implantación de un sistema de gestión confiable.

Tabla A.2. Clasificación de los objetivos de control presentes en la División de TIC de la Universidad del Cauca.

Entrevistado: Ing. Fabián Mera **Fecha:** 31 – Marzo - 2011
Entidad: División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca (TIC's).

NORMA ISO/IEC 27001	CRITERIOS DE GESTION APLICADOS EN LA DIVISION DE TIC DE LA UNIVERSIDAD DEL CAUCA
1. POLÍTICAS DE SEGURIDAD	**1. POLÍTICAS DE SEGURIDAD**
• Definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información.	Existen políticas de seguridad creadas por el administrador pero no están documentadas, solo fueron creadas por uno de los encargados.
• Marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo.	
• Explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización.	
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	**2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
2.1 Organización interna. Seguridad de la información dentro de la organización. (Administradores, usuarios).	**2.1 Organización interna.**
2.1.1 Compromiso de los administradores en el reconocimiento de las responsabilidades de la seguridad	**2.1.1** Solo esta implementada en ciertas aéreas, donde algunos ingenieros tienen el control de algunos

de la información.	servicios. **a.** Se revisa la efectividad de la implementación de algunas políticas de seguridad. **b.** Se aprueban las asignaciones de roles y responsabilidades específicas para la seguridad de la información.
2.1.2 Coordinación de la seguridad de la información por representantes de la división de las TIC's.	**2.1.2 No aplicado.**
2.1.3 Asignación de responsabilidades de la seguridad de la información en la división de las TIC's.	**2.1.3 No aplicado.**
2.1.4 Proceso de autorización por parte de los administradores para los nuevos medios de procesamiento de información.	**2.1.4 No aplicado.**
2.1.5 Identificación y revisión en los acuerdos de confidencialidad para la protección de la información.	**2.1.5** Existen algunos acuerdos pero no están estandarizados. **a.** Definir la información a protegerse. **b.** Responsabilidades y acciones de los firmantes para evitar la divulgación de la información no autorizada. **c.** Propiedad de la información.
2.1.6 Existencia de contactos con grupos de seguridad especializados o asociaciones profesionales.	**2.1.6 No aplicado.**
2.1.7 Revisión independiente cuando ocurran cambios significativos en la seguridad de la información.	**2.1.7 No aplicado.**
2.2 Organización externa. Seguridad de la información de la Universidad del Cauca cuando se trata	**2.2 Organización externa.**

con grupos externos a los que se debe dar permisos a los medios de procesamiento.	
2.2.1 Identificación de los riesgos relacionados con entidades externas antes de otorgar los accesos.	**2.2.1** Accesos físico, lógicos, conectividad red entre las redes de la organización, aunque no existen protocolos o lineamientos. *(Aplicado en Unicauca)*
2.2.2 Tratamiento de la seguridad cuando se trabaja con clientes y terceras personas.	***2.2.2*** Existen los procedimientos para proteger los activos, proceso de autorización para el acceso y privilegios de usuario, se prohíbe el acceso a todo lo que no esté explícitamente autorizado. Pero no está estandarizado. *(Aplicado en Unicauca)*
3. GESTIÓN DE ACTIVOS	**3. GESTIÓN DE ACTIVOS**
3.1 Responsabilidad por los activos.	**3.1 Responsabilidad por los activos.**
3.1.1 Elaboración y mantenimiento de los activos importantes.	**3.1.1** Cuenta con: *(Aplicado en Unicauca)* **a.** Información (bases de datos contratos y acuerdos.) **b.** Activos de software: aplicación, software sistema herramientas de desarrollo y utilidades. **c.** Activos físicos. Equipos de computo, de comunicaciones, medios removibles. **d.** Servicios: servicios de computación y comunicación, servicios generales. **e.** Personas, sus capacidades y experiencia. **f.** Prestigios de la organización.
3.1.2 Selección del propietario de los activos en la división de las TIC's.	**3.1.2** Existen propietarios para ciertos activos: Hardware - Inmuebles. En el caso de la información se determina un encargado por

	servicio, ya sea en el caso de SIMCA, correo, web etc.
3.1.3 Identificación, documentación e implementación para el uso aceptable de los activos asociados con los medios de procesamiento de la información.	**3.1.3** Existen reglas BASICAS para el uso de correo electrónico e internet, clasificación de la información, se encuentra en la FASE INICIAL. *(Aplicado en Unicauca).*
3.2 Clasificación de la información.	**3.2** Clasificación de la información.
3.2.1 Clasificación y manejo de la información según requerimientos legales, confidencialidad.	**3.2.1** Aunque no esté documentado en su totalidad los requerimientos de seguridad. *(Aplicado en Unicauca).*
4 SEGURIDAD DE LOS RECURSOS HUMANOS	**4. SEGURIDAD DE LOS RECURSOS HUMANOS**
4.1 Antes del empleo.	**4.1** Antes del empleo.
4.1.1 Selección del personal mediante la verificación de antecedentes, conducta ética y profesional.	**4.1.1** Referencias personales e institucionales, hoja de vida, calificaciones académicas, chequeo de identidad.
4.2 Durante el empleo.	**4.2** Durante el empleo.
4.2.1 Capacitación y actualizaciones regulares en las políticas de la seguridad de la información.	**4.2.1 No aplicado.**
4.2.2 Existencia de un proceso disciplinario ante empleados que violen la seguridad de la información.	**4.2.2 No aplicado.**
4.3 Terminación o cambio de empleo	**4.3** Terminación o cambio de empleo
4.3.1 Devolución de activos por parte del personal al término de su contrato.	**4.3.1 No aplicado.**
4.3.2 Eliminación de derechos de acceso al personal cuando finalice su	**4.3.2 No aplicado.**

contrato.	
5 GESTIÓN DE LAS COMUNICACIONES	**5 GESTIÓN DE LAS COMUNICACIONES**
5.1 Planeación y aceptación del sistema. Planeación y preparación anticipadas para asegurar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño del sistema requerido.	**5.1 Planeación y aceptación del sistema.**
5.1.1 Criterios de aceptación para nuevos sistemas o actualizaciones.	**5.1.1 No se tiene documentación para**: **a.** Desempeño y requerimientos de capacidad. **b.** Procedimientos para la recuperación tras fallos. **c.** Capacitación para la operación o uso de los sistemas nuevos.
5.2 Protección contra software malicioso y código móvil.	**5.2 Protección contra software malicioso y código móvil.**
5.2.1 Detección, prevención y recuperación contra software malicioso y códigos móviles.	**5.2.1** *(Aplicado en Unicauca)* **a.** Poseen políticas de prohibir el uso de software no-autorizado. Hechas por el encargado pero aun no están aprobadas. **b.** Revisiones regulares del software y contenidos de información. **c.** Instalación y actualización regular de software para la detección o reparación de códigos maliciosos para revisar Las computadoras.
5.3 Respaldo	**5.3 Respaldo**
5.3.1 Realización frecuente de copias de seguridad (Back-up).	**5.3.1** *(Aplicado en Unicauca)* **a.** Se define el nivel necesario de respaldo de la información.

	b. Se prueban regularmente los medios de respaldo. **c.** Las copias de respaldo NO están codificadas.
5.4 Gestión de seguridad de redes.	**5.4 Gestión de seguridad de redes.**
5.4.1 Protección de la información mediante controles en la seguridad de los servicios de red.	**5.4.1** Existen controles especiales para salvaguardar la confidencialidad e integridad de la información en tránsito por la red. *(Aplicado en Unicauca)*
5.5 Gestión de medios	**5.5 Gestión de medios**
5.5.1 Procedimientos formales y seguros en la eliminación de los activos.	**5.5.1 No aplicado.**
5.5.2 Procedimientos de manejo y almacenamiento de la información para su protección.	**5.5.2** *(Aplicado en Unicauca)* **a.** Existen restricciones de acceso de personal no-autorizado. **b.** Se marcan claramente todas las copias de los medios con atención al destinatario autorizado.
5.6 Intercambio de información.	**5.6 Intercambio de información.**
5.6.1 Procedimientos y políticas en el intercambio de información y software.	**5.6.1 No aplicado.** **a.** No hay manejo de las responsabilidades para el control y notificación de la transmisión, despacho y recepción.
5.6.2 Protección en el envío de Mensajes electrónicos.	**5.6.2 No aplicado.** **a.** No hay protección de los mensajes de accesos no autorizados, modificación o negación del servicio.
5.7 Monitoreo.	**5.7 Monitoreo**.
5.7.1 Existencia de un sistema de	**5.7.1** SI. Se encuentra en la fase inicial

monitoreo y revisión regular del resultado de las actividades.	donde incluye algunos detalles como: *(Aplicado en Unicauca)* Acceso autorizado: **a.** ID del usuario. **b.** Tipos de eventos. **c.** Archivos a los cuales se tuvo acceso. **d.** Programas/utilidades usadas. Operaciones privilegiadas: **a.** Uso de cuentas privilegiadas. **b.** Inicio y pagado del sistema. Intentos de acceso no autorizados: **a.** Accesiones del usuario fallidas o rechazadas. **b.** Acciones fallidas o rechazadas donde se incluyen datos. **c.** Violaciones a la política de acceso y notificaciones para los Gateways y firewalls. Alertas del sistema: **a.** Alertas o mensajes en consola. **b.** Alarmas activadas por el sistema de control de acceso. **c.** Alertas de los sistemas de detección de intrusiones.
5.7.2 Protección de la información del registro contra alteraciones y accesos no autorizados.	**5.7.2 No aplicado.** se almacena sin protección.
5.7.3 Registro de las actividades de los administradores y operadores.	**5.7.3 No aplicado.**
5.7.4 Registro y análisis correspondiente ante fallas del sistema.	**5.7.4 No aplicado.**
6. CONTROL DE ACCESO	**6. CONTROL DE ACCESO**
6.1 Gestión del acceso al usuario	**6.1 Gestión del acceso al usuario**

6.1.1 Existencia de procedimientos formales para la inscripción del usuario que otorga acceso a servicios y sistemas de información.	**6.1.1 No aplicado.**
6.1.2 Existencia de gestión de privilegios.	**6.1.2 No aplicado.**
6.1.3 Existencia de proceso de gestión formal para la asignación de claves de usuario.	**6.1.3 No aplicado.**
6.1.4 Revisión de derechos de acceso de usuario en intervalos constantes.	**6.1.4 No aplicado.**
6.2 Control de acceso a redes.	**6.2 Control de acceso a redes.**
6.2.1 Aplicación de políticas sobre el acceso a servicios por parte de usuarios autorizados.	**6.2.1** Aplicación de políticas sobre el acceso a servicios por parte de usuarios autorizados. *(Aplicado en Unicauca)* **a.** Manejo de ID's. **b.** Utilización de equipos específicos para asignar funciones. **c.** Procedimientos de autorización para acceso a redes y servicios. **d.** Utilización de VPN (Red Privada Virtual).
6.2.2 Autenticación del usuario para conexiones remotas.	**6.2.2** Autenticación del usuario para conexiones remotas. *(Aplicado en Unicauca)* **a.** Permitir al acceso a la red a través de log in. **b.** El control no es 100% seguro. **c.** Nivel de criptografía o enmascaramiento bajo.
6.2.3 Identificación automática de equipo en red como medio de autenticación.	**6.2.3 No aplicado.**
6.2.4 Protección de acceso físico y lógico al puerto de diagnostico remoto.	**6.2.4 No aplicado.**
6.2.5 Separación de la información,	**6.2.5 No aplicado.** Se comete el error de

usuarios y sistemas de información en las redes.	que todos los usuarios pueden compartir el mismo equipo. Todos los usuarios pueden ingresar sin importar su roll. No existe seguridad suficiente.
6.2.6 Existencia de controles de conexiones de redes que restringa la capacidad de acceso de los usuarios en las redes compartidas.	**6.2.6** Existencia de controles de conexiones de redes que restringa la capacidad de acceso de los usuarios en las redes compartidas. *(Aplicado en Unicauca)* **a.** Básicamente a través de Firewalls **b.** Satisfacción de la seguridad aceptable
6.3 Control de acceso al sistema de operación	**6.3 Control de acceso al sistema de operación**
6.3.1 Existencia de procedimientos de registro en el terminal para controlar el acceso a los servicios operativos.	**6.3.1 No aplicado.**
6.3.2 Identificación y autenticación del usuario para uso personal y exclusivo (ID de usuario).	**6.3.2** Identificación y autenticación del usuario para uso personal y exclusivo (ID de usuario). *(Aplicado en Unicauca)* **a.** Tipo de identificación: Iniciando sesión mediante datos de correo electrónico Unicauca. **b.** Se autentica cuando se confirma que los datos como el correo y contraseña son correctos. **c.** Es de uso personal y exclusivo.
6.3.3 Existencia de sistemas de gestión de claves que asegure la calidad de las claves.	**6.3.3 No aplicado.**
6.3.4 Restricción y control de uso de programas de utilidades que podrían superar el sistema.	**6.3.4 No aplicado.**
6.3.5 Sesiones inactivas se cierran después de un periodo de inactividad definido.	**6.3.5** Sesiones inactivas se cierran después de un periodo de inactividad definido. *(Aplicado en Unicauca)* **a.** Basado en sistema de solicitudes.

	b. Se maneja y modifica a través de apache. **c.** Se logra evitar saturación de la red con conexiones inactivas. **d.** Se satisface la seguridad informática. **e.** Se maneja en SIMCA.
6.3.6 Restricción sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.	**6.3.6 No aplicado.** Es manejado por diferentes aplicativos, pero es variable la seguridad.
7. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	**7. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**
7.1.1 Validación de los datos de entrada en las aplicaciones para asegurar que los datos sean correctos y seguros.	**7.1.1 No aplicado.** Se necesita implementación con urgencia. Los datos no se evalúan, así que se corre el riesgo de corrupción de datos de entrada.
7.1.2 Control de procesamiento interno a través de chequeos de validación en las aplicaciones que detecten cualquier corrupción de la información.	**7.1.2 No aplicado.**
7.2 Controles criptográficos.	**7.2 Controles criptográficos.**
7.2.1 Existencia de políticas sobre el uso de controles criptográficos para la protección de la información.	**7.2.1** Existencia de políticas sobre el uso de controles criptográficos para la protección de la información. *(Aplicado en Unicauca) (Hay mecanismos pero no son suficientes)* **a.** No está aplicado pero es necesaria la aplicación inmediata. **b.** Se hace un backup pero no hay nada estandarizado. **c.** No proporciona seguridad.
7.2.2 Utilización de gestión de clave para dar soporte al uso al uso de las técnicas de criptografía en la organización.	**7.2.2 No aplicado.**
7.3 Seguridad de los archivos del sistema	**7.3 Seguridad de los archivos del sistema**

7.3.1 Control de instalación de software en los sistemas operacionales.	**7.3.1 No aplicado.**
7.3.2 Control de acceso al código fuente del programa.	**7.3.2** Control de acceso al código fuente del programa. *(Aplicado en Unicauca)* **a.** Se puede aplicar mientras este bajo su control. **b.** No hay totalidad de los manejos, depende más del control externo. **c.** Si el código es de la Unicauca si tienen control.
7.4 Seguridad en los procesos de desarrollo y soporte	**7.4 Seguridad en los procesos de desarrollo y soporte**
7.4.1 Procedimientos de revisión y control de las aplicaciones después de cambios en el sistema operativo.	**7.4.1 No aplicado.**
7.4.2 Prevención contra la filtración de la información.	**7.4.2 No aplicado.**
7.5 Gestión de vulnerabilidad técnica.	**7.5 Gestión de vulnerabilidad técnica.**
7.5.1 Control, evaluación y solución de vulnerabilidades técnicas para tratar el riesgo asociado.	**7.5.1 No aplicado.**
8. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	**8. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**
8.1 Reporte de eventos y debilidades en la seguridad de la información	**8.1 Reporte de eventos y debilidades en la seguridad de la información**
8.1.1 Reporte de eventos en la seguridad de la información a través de los canales gerenciales apropiados lo más rápidamente posible.	**8.1.1 No aplicado.**
8.1.2 Reporte de las debilidades en la seguridad de los sistemas o servicios por parte de empleados, contratistas y terceros usuarios.	**8.1.2 No aplicado.** No se tiene relación con terceros ya que es una división institucional.

8.2 Gestión de incidentes y mejoras en la seguridad de la información.	**8.2 Gestión de incidentes y mejoras en la seguridad de la información.**
8.2.1 Existencia de responsabilidades y procedimientos gerenciales para asegurar una respuesta eficiente ante incidentes de seguridad de la información.	**8.2.1** Existencia de responsabilidades y procedimientos gerenciales para asegurar una respuesta eficiente ante incidentes de seguridad de la información. *(Aplicado en Unicauca) (No estandarizado)* **a.** Se encuentra en fase inicial de desarrollo. **b.** Se implementa a través de manuales de usuario escritos por ellos. **c.** Se utiliza técnica de "*Rollback*"[1] para realizar cambios. **d.** Se están realizando políticas para planes de contingencia.
8.2.2 Existencia de mecanismos que permitan cuantificar los tipos, volúmenes y costos de los incidentes en la seguridad de la información.	**8.2.2 No aplicado.**
9. CUMPLIMIENTO	**9. CUMPLIMIENTO**
9.1 Cumplimiento con las políticas y estándares de seguridad y el cumplimiento técnico	**9.1 Cumplimiento con las políticas y estándares de seguridad y el cumplimiento técnico**
9.1.1 Asegurar el cumplimiento de las políticas y estándares de seguridad que permitan que los procedimientos de seguridad sean realizados correctamente.	**9.1.1 No aplicado.** No existen entes encargados.
9.1.2 Chequeo de cumplimiento con los estándares de implementación de la seguridad en los sistemas de información.	**9.1.2 No aplicado.**
9.2 Consideraciones de auditoría de los sistemas de información.	**9.2 Consideraciones de auditoría de los sistemas de información.**
9.2.1 Planeación de controles de auditoría en los sistemas de información.	**9.2.1 No aplicado.**

[1] Operación que devuelve de un estado a un estado previo.

Tabla A.3. Investigación sobre las plataformas de gestión presentes en la división de TIC de la Universidad del Cauca.

LISTA DE CHEQUEO PARA IDENTIFICAR LAS PLATAFORMAS DE GESTION QUE EXISTEN EN LA DIVISION DE TIC DEL A UNIVERSIDAD DEL CAUCA					
ENTIDAD: División de Tecnologías de la Información y la comunicación de la Universidad del Cauca					
FECHA DE REALIZACION DE LA LISTA DE CHEQUEO: 28 - Abril – 2011					
PARTICIPANTES EN EL LLENADO DE LOS DATOS Y SU RESPONSABILIDAD Fabián Andrés Mera					
REALIZADO POR: Andrés Felipe Mera Oscar Eduardo Mondragón					
1	**NAGIOS**			**SI**	**NO**	**Observaciones**
1.1		Monitorización de servicios de redes:			
1.1.1			SMTP		X	
1.1.2			POP3	✓		*Nagios*
1.1.3			HTTP	✓		
1.1.4			NNTP		X	
1.1.5			PING	✓		*Algunos servidores como por ejemplo maquinas virtuales*
1.1.6			SSH	✓		*Nagios*
1.1.7			DNS	✓		
1.2		Monitorización de recursos de los servidores.			
1.2.1			Carga de procesador.	✓		
1.2.2			Uso de Disco.	✓		
1.2.3			Uso de memoria.	✓		
1.2.4			Procesos ejecutándose.	✓		
1.2.5			Ficheros de log.	✓		
1.2.6			Espacio libre en filesystem.	✓		
1.2.7			Otro:			
1.3		Monitorización de sistemas ambientales:			
1.3.1			Temperatura		X	

1.3.2			Humedad		X	
1.3.3			Luminosidad.		X	
1.3.3			Otro:			
1.4		Capacidad de desarrollar plugins de forma sencilla que permita a los usuarios programar sus propios chequeos.		✓		
1.5		Envío de notificaciones mediante múltiples mé todos cuando los problemas aparecen y cuando se resuelven.		✓		
1.5.1			Pantalla.	✓		
1.5.2			Vía e-mail.	✓		
1.5.3			Vía SMS.	✓		*Gammu*
1.5.4			Alertas sonoras.	✓		
1.5.5			WAP		X	
1.5.5			Otra:			
1.6		Controles que permitan solventar un problema de forma inmediata.			X	
1.7		Visión rápida y sencilla de los elementos.		✓		
2	**AWstats**					
2.1		Análisis de servicios de internet:				*SIMCA*
2.1.1			Web	✓		
2.1.2			Streaming		X	*NO se tiene implementado el servicio*
2.1.3			Mail	✓		
2.1.4			FTP	✓		*Ftp Unicauca*
2.1.5			HTML	✓		*Servidores web*
2.2		Generación de informes HTML de los logs gestionados.		✓		*Awstats Sarge*
2.3		Generación de informes dinámicos.			X	
2.4		Generación de informes estáticos mediante una interfaz de línea de comando.			X	
2.5		Generación de informes on-demand a través de un navegador web gracias a un programa CGI.			X	
2.6		Restricción de acceso a la información de usuarios internos.		✓		
2.7		Seguridad informática para programas CGI.			X	
2.8		Soporte de formatos de archivo log de servidor web como Apache.		✓		
2.9		Sistemas operativos utilizados para gestionar				

		a través de AWstats:				
2.9.1			Distribuciones Linux.	✓		
2.9.2			Distribuciones Windows.	✓		
2.9.3			Otro:			
2.10		Análisis de logs descargados desde servidores remotos.		✓		
3		**SARG (Squid Analysis Report Generator)**				
3.1		¿Permite ver los sitios visitados por los usuarios en internet?		✓		
3.2		Generación de informes HTML.		✓		
3.3		Campos usados en los informes HTML:				
3.3.1			Usuarios	✓		
3.3.2			Direcciones IP	✓		
3.3.3			Bytes transmitidos	✓		
3.3.4			Sitios web	✓		
3.3.5			Servidores	✓		
3.3.6			Tiempos de uso	✓		
3.3.7			Otros:			
3.4		Sistemas operativos utilizados para gestionar a través de SARG:				
3.4.1			Distribuciones Linux.	✓		
3.4.2			Distribuciones Windows.	✓		
3.4.3			Otro:			
3.5		¿Generación de alertas a través de SARG?			X	
4		**Sistema de Solicitudes[2]**				
4.1		¿Sistema de solicitudes a través de llamada?		✓		
4.2		¿Maneja atención y requerimientos de usuario?		✓		
4.3		¿Generación de informes HTML para observar reportes?		✓		
4.4		¿Acción inmediata de este sistema?			X	*Depende del momento en que se lea la solicitud*
4.5		¿Sistema de alertas?		✓		
4.6		Servicios soportados:				
4.6.1			Internet.	✓		
4.6.2			Servidores.	✓		

[2] Sistema propietario de la Universidad del Cauca el cual permite reportar fallas o anomalías en los servicios realizando una llamada telefónica al centro de atención.

4.6.3			DNS.	✓		
4.7		¿Estados de la solicitud recibida?		✓		
5		**FortiGate**				
5.1		¿Funcionalidad principal Firewall o Modo Proxy?		✓		
5.2		Servicios:				
5.2.1			Proxy.	✓		
5.2.2			DNS.	✓		
5.3		Funcionalidades UTM:				
5.3.1			VPN.	✓		
5.3.2			Antispam.	✓		
5.3.3			Antiphishing.		X	
5.3.4			Antispyware.		X	
5.3.5			Filtro de contenidos.		X	
5.3.6			Antivirus.		X	
5.3.7			Detección/Prevención de Intrusos (IDS/IPS).		X	
5.4		¿Se puede observar todos los equipos de la red gestionada?		✓		
5.5		¿Gestión de Logs?		✓		
5.6		¿Generación de informes HTML del tráfico de la red?		✓		*Allot, MRTG*
5.7		¿Provee un sistema de alertas inmediatas?			X	
6		**MRTG[3]**				
6.1		¿Uso de Scripts creados en la Universidad del Cauca para monitorear el tráfico de la red?			X	
6.2		Identificación de Usuario.		✓		
6.3		¿Generación de informes HTML del tráfico de la red?		✓		
6.4		Usos:				
6.5.1			Trafico de la red.	✓		
6.5.2			Memoria utilizada por los equipos.		X	
6.5.3			Sesiones abiertas por los usuarios.	✓		
6.5.4			Disponibilidad de módems.		X	
6.5.5			Tráfico en los routers.	✓		
6.6		¿El tráfico es analizado por días?		✓		
6.7		¿Generación de alertas?			X	

[3] http://oss.oetiker.ch/mrtg/

6.8		¿Método de aviso de la alerta?				
6.8.1			SMS.		X	
6.8.2			Correo Electrónico.		X	
6.8.3			Alerta Sonora.		X	
6.8.4			Pantalla del equipo de gestión.		X	
7		**SSI Wiki[4]**				
7.1		¿Acceso restringido solo habilitado para administradores de los servicios?		✓		
7.2		¿Base de datos de documentación?		✓		
7.3		¿Base de datos de repositorios?		✓		
8		**NetXplorer - Estadísticas**				
8.1		Análisis de tráfico de la red.		✓		
8.2		Análisis de servicios utilizados dentro de la red.		✓		
8.3		¿Generación de informes HTML del tráfico y servicios de red?		✓		
8.4		¿Reportes generados se envían al correo de los administradores?		✓		
8.5		¿Permite realizar control de tráfico de red?		✓		
8.6		Además de los reportes, ¿Envía algún tipo de alarma?			X	

ANALISIS DE RESULTADOS
Se concluye que a pesar de que existen diversas herramientas de gestión capacitadas para la resolución de inconvenientes en los diferentes servicios, ninguna permite actuar de manera segura y realizar un control efectivo, además del despliegue de la alarma visual y de manera escrita a los administradores.

[4] Es una herramienta que permite el alojamiento de información importante como guías de usuario para los diferentes servicios las cuales solo pueden ser accedidas por los administradores de la división de las TIC's de la Universidad del Cauca.

Tabla A.4. Evaluación de los recursos críticos encontrados en las plataformas de gestión y las tesis encontradas.

Entrevistado: Ing. Fabián Mera **Fecha:** 15 – Mayo - 2011
Entidad: División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca (TIC).

ANALISIS DE HERRAMIENTAS DE GESTION ENCONTRADAS EN LAS TIC's DE LA UNIVERSIDAD DEL CAUCA - APORTES

NAGIOS

CRITERIOS DE GESTION ENCONTRADOS EN LA DIVISION DE TIC APLICABLES AL PROYECTO	ANALISIS DE APLICABILIDAD EN EL PRESENTE PROYECTO
1. Capacidad de monitorización de los servicios de redes y servidores de las TIC's.	**1.** Permite a nuestro proyecto utilizar los métodos implementados para monitorizar los comportamientos de los dos servicios críticos que se identificaran posteriormente. Nos permitirá conocer el análisis de estado de servicios y como se muestra en pantalla.
2. Análisis de fallas e informe de alarmas a los administradores a través de mensajes de texto (gammu), correo electrónico, pantalla y alarmas sonoras.	**2.** Se analiza el método de envió de mensajes de texto a los administradores utilizado por esta herramienta. Nuestro aporte radicaría en la implementación de alertas de seguridad informática para dos servicios críticos de la División de TIC enviando SMS y correos electrónicos a los administradores. Se conoce que la implementación actual de este método en la División de TIC es reciente por lo que está sujeto a mejoras, además que tiene un enfoque más básico a diferencia del que piensa brindar nuestro proyecto.

3. Brinda una interfaz sencilla al administrador para su uso.	**3.** Se analiza el tipo de interfaz utilizada que es sencilla para su gestión. Se planea implementar una interfaz para nuestro sistema de gestión basada en estos criterios de facilidad.
4. El sistema está abierto a la posibilidad de inserción de script que permitan la mejora en la gestión de los recursos.	**4.** Se planea que nuestro sistema este abierto a posibilidades de actualizaciones futuras, todo esto basado en el ciclo Deming implementado por la norma ISO/IEC 27001.

AWstats

CRITERIOS DE GESTION ENCONTRADOS EN LA DIVISION DE TIC APLICABLES AL PROYECTO	ANALISIS DE APLICABILIDAD EN EL PRESENTE PROYECTO
1. Brinda la posibilidad de análisis de servicios de red como el Web, FTP, HTML y Mail.	**1.** Se analiza el método de análisis para los servicios críticos que se encontraran.
2. Genera informes HTML sobre análisis de logs gestionados.	**2.** El sistema de informes de alertas de seguridad informática se generaran también en forma visual a través de pantallazos que se mostrara a los administradores, un buen método de generación de estos es el HTML.
3. Acceso restringido para diferentes usuarios.	**3.** La confidencialidad es un factor importante de la seguridad de la información, por lo que se brindara acceso limitado a nuestro sistema para evitar manipulación por personal no autorizado.
4. Soporta formatos de archivos log de servidor web como apache.	**4.** El soporte de logs tipo web como el apache servirá para su análisis y

	posterior implementación si uno de los servicios críticos encontrados es el Web.
5. Es un sistema soportado por diferentes sistemas operativos.	**5.** La interoperabilidad entre sistemas operativos brinda mayor soporte por lo que se planea que nuestro sistema este abierto a esto. En de no ser posible se realizara un análisis de sistemas y cuál de ellos brinda confiabilidad para su implementación.

SARG (Squid Analysis Report Generator)

CRITERIOS DE GESTION ENCONTRADOS EN LA DIVISION DE TIC APLICABLES AL PROYECTO	ANALISIS DE APLICABILIDAD EN EL PRESENTE PROYECTO
1. Visualización de tráfico de internet.	**1.** Servirá para el análisis de tráfico futuro dependiendo el tipo de servicio.
2. Generación de informes HTML con campos como direcciones IP, Bytes transmitidos, usuarios, sitios web, servidores, entre otros.	**2.** Se podrá utilizar información de campos como los implementados por SARG para brindar total información al administrador a través de nuestro sistema.

FortiGate

CRITERIOS DE GESTION ENCONTRADOS EN LA DIVISION DE TIC APLICABLES AL PROYECTO	ANALISIS DE APLICABILIDAD EN EL PRESENTE PROYECTO
1. Servicios analizados como el DNS y el Proxy donde este último es el principal.	**1.** En caso posible que los servicios críticos encontrados sean el DNS y/o el Proxy se analizara en profundidad el sistema de gestión implementado por esta herramienta para estos.
2. Brinda funcionalidades como VPN y anti-spam.	**2.** Se podrá analizar el método de evitar el spam que es causante de muchas amenazas en los sistemas.

NetXplorer - Estadísticas

CRITERIOS DE GESTION ENCONTRADOS EN LA DIVISION DE TIC APLICABLES AL PROYECTO	ANALISIS DE APLICABILIDAD EN EL PRESENTE PROYECTO
1. Permite el análisis de varios de los servicios de la red.	**1.** Se podrá observar el método de análisis de los servicios para posible aplicación en nuestro sistema de gestión.
2. Los reportes generados se envían al correo electrónico de los administradores encargados.	**2.** Se analizara el método utilizado por esta herramienta para el envió de estos reportes a los administradores.

ANALISIS DE TESIS ENCONTRADAS - APORTES

Tesis - SGSI Ecuacolor[1]

CRITERIOS IMPORTANTES ENCONTRADOS EN LA TESIS DE ESTUDIO	ANALISIS DE APLICABILIDAD EN EL PRESENTE PROYECTO
• Uso de herramienta de gestión COBIT.	• Se analiza la posibilidad de uso del método de análisis de riesgos COBIT ya que se amolda a los requerimientos de la norma ISO/IEC 27001.
• Definición de arquitectura de seguridad para aplicación.	• Es importante el establecimiento de una arquitectura de seguridad para la aplicación por que esto brinda confiabilidad en la ejecución de los proceso.
• Tratamiento de riesgos: Establecer marco general -> Identificar riesgos -> Análisis de riesgos -> Evaluar y priorizar riesgos -> Tratamiento del riesgo.	• Es importante la implementación de un orden de tratamiento de riesgos para lograr un resultado adecuado en el desarrollo y gestión de nuestro proyecto.
• ***Riesgo*** = *Probabilidad de Ocurrencia * Impacto*.	• Calculo de riesgo donde se toma como valores la probabilidad de ocurrencia y el impacto que este genera en un determinado activo.

Tesis - Desarrollo de Políticas de Seguridad Informática e Implementación de cuatro dominios en base a la norma 270002 para el área de hardware en la empresa Uniplex Systems S.A en Guayaquil.[2]

CRITERIOS IMPORTANTES ENCONTRADOS EN LA TESIS DE ESTUDIO	ANALISIS DE APLICABILIDAD EN EL PRESENTE PROYECTO
• El sistema deber brindar características como disponibilidad, integrabilidad y confidencialidad.	• Es importante contar con estos tres factores y mejorarlos porque de ellos depende el nivel de seguridad de un activo o servicio en seguridad de la información.
• Método de gestión utilizado GMITS aplicable a la norma ISO/IEC 27000.	• Se analizara el método de gestión de riesgo GMITS para posible aplicabilidad a nuestro proyecto.
• ***Valor del riesgo*** = *Valor del activo x Amenazas x Vulnerabilidades.*	• Calculo del valor de riesgo presente en un activo donde se toman parámetros como el valor que tiene el activo, las amenazas que lo rodean y sus vulnerabilidades.

Tesis - Implementación del Primer Sistema de Gestión de Seguridad de la Información, en el Ecuador, Certificado Bajo la Norma ISO 27001: 2005.[3]

CRITERIOS IMPORTANTES ENCONTRADOS EN LA TESIS DE ESTUDIO	ANALISIS DE APLICABILIDAD EN EL PRESENTE PROYECTO
• Ciclo Deming basado en la norma ISO/IEC 27001. **PLAN:** Establecer SGSI (Clausula 4.2.1) – **DO:** Implementar y operar el SGSI (clausula 4.2.2) – **CHECK:** Monitorear y revisar el SGSI (clausula 4.2.3) – **ACT:** Mejorar el SGSI (clausula 4.2.4).	• Se toma como referencia el ciclo Deming sugerido e implementado por la norma ISO/IEC 27001 junto con las clausulas en cada fase del proceso.
• Ciclo Metodológico de implantación de un SGSI basado en ISO 27001: ➢ Entendimiento de los	• Es importante para un buen desarrollo el entendimiento y aplicación de un ciclo de métodos sugeridos por la norma ISO/IEC

requerimientos del modelo. ➢ Determinación de la brecha. ➢ Análisis y evaluación del riesgo. ➢ Elaboración del plan de gestión de continuidad comercial. ➢ Desarrollo de competencias organizacionales. ➢ Redacción del manual de seguridad de la información. ➢ Ejecución de auditorías internas. ➢ Obtención de la certificación internacional.	27001.
• Parámetros para tabla de medición de riesgo: ➢ Activos de información. ➢ Amenazas. ➢ Posibilidad de ocurrencia de la amenaza. ➢ Vulnerabilidades. ➢ Posibilidad que la amenaza penetre la vulnerabilidad. ➢ Valor de activos en riesgo. ➢ Posibilidad de ocurrencia de la amenaza. ➢ Total Riesgo.	• Esta tesis brinda una serie de parámetros los cuales son necesarios para realizar la medición de riesgo en la empresa. Estos parámetros incluyen el activo que se estudia junto con sus amenazas y vulnerabilidades.
• Opciones de tratamiento del riesgo: ➢ Reducir el riesgo. ➢ Evitar el riesgo. ➢ Transferir el riesgo. ➢ Aceptar el riesgo.	• Es importante saber el procesamiento que se le debe dar al riesgo. Lo primordial debe radicar en evitar el riesgo pero si no se puede del todo se deben realizar planes de reducción de este. También se puede realizar la transferencia de riesgo a sectores que no sean de vital importancia o no se vean tan afectados.

	En última instancia se procede por aceptar el riesgo dándole un manejo más adecuado y que no afecte en alto grado los activos y la empresa como tal.

Tesis - Implementación Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, para la intranet de la Corporación Metropolitana de Salud.[4]

CRITERIOS IMPORTANTES ENCONTRADOS EN LA TESIS DE ESTUDIO	ANALISIS DE APLICABILIDAD EN EL PRESENTE PROYECTO
• Documentación del SGSI: Manual de seguridad – Procedimientos - instrucciones, listas de chequeo, formularios - registros.	• La documentación es primordial en la implantación de un SGSI, por lo que se deberá realizar una serie de documentos que brinden la suficiente información para que el sistema sea sostenible y actualizable.
• Se define el documento de políticas: definición de seguridad de la información y sus objetivos globales y alcance. **-** Soportes de los objetivos y principios de la seguridad de la información. **–** Estructura para el establecimiento de los objetivos de control y controles, incluida la estructura de valoración y manejo de riesgos. **–** Breve explicación de políticas, principios, normas y requisitos de conformidad más importantes para la organización. **–** Definición de las responsabilidades generales y específicas en materia de la seguridad de la información, incluida el reporte de incidentes en seguridad. **–** Referencias a documentación de las políticas.	• Pasos necesarios para la implementación de un documento de políticas el cual brinda objetividad en el desarrollo e implementación del sistema de gestión.

• Registros de auditoría (actividades de los usuarios): - ID usuario **–** fecha, hora, conexión, desconexión **–** identificación del monitor o localización **–** ingreso al sistema exitoso o no **–** cambio en configuración de los sistemas **–** uso de privilegios **–** acceso de archivos y tipos **–** direcciones de red y protocolos **–** activación y desactivación de antivirus.	• Es muy importante contar con diferentes registros de auditoría debido a que estos sirven para futuras mejoras y correcciones.
• Nivel de monitorización (se determina por el nivel de riesgo): **-** Acceso autorizado **–** Operaciones privilegiadas **–** intentos de acceso desautorizados **–** alertas del sistema o fallas **–** cambios o intentos de cambios en el sistema de seguridad y controles.	• El nivel de monitorización debe estar fundamentado por el nivel de riesgo presente en la empresa. Esto ayuda a la prevención y manejo por parte del sistema de los riesgos circundantes.
• Para esta tesis se usa el GMITS que se ajusta a la norma ISO/IEC 27001. Métodos para la valoración de riesgos: ➢ <u>Acercamiento Básico</u>: Se hace un análisis rápido de los riesgos de la empresa. Se implementan controles generales. ➢ <u>Análisis de Riesgo Detallado</u>: Se analizan efectos, amenazas y vulnerabilidades que causan la pérdida de confidencialidad, integridad o disponibilidad de los activos de información. Se seleccionan controles reales y efectivos basados en el riesgo presente. ➢ <u>Acercamiento Combinado</u>:	• Se analiza el método de gestión de riesgo GMITS que se ajusta a la norma ISO/IEC 27001. Brinda un análisis profundo y efectivo del riesgo.

se combinan los dos métodos anteriores. Se clarifican las ventajas y desventajas de los dos métodos. ➢ Acercamiento Informal: Se realiza un análisis de riesgo basado en el conocimiento o la experiencia de las personas responsables.	

Tesis - Diseño SGSI para empresa MEGADATOS.[5]

CRITERIOS IMPORTANTES ENCONTRADOS EN LA TESIS DE ESTUDIO	ANALISIS DE APLICABILIDAD EN EL PRESENTE PROYECTO
• Clasificación de las amenazas: ➢ Estructuradas. ➢ No estructuradas. ➢ Externas. ➢ Internas.	• Es importante la clasificación de amenazas, porque de ello depende la eficacia de nuestro sistema.
• Clasificación de los ataques: ➢ Reconocimiento. ➢ Acceso. ➢ Negación del servicio. ➢ Gusanos, virus y troyanos.	• Al igual que las amenazas, es importante conocer el origen y como se clasifican los ataques, saber su proveniencia, su nivel de impacto, las secuelas del ataque.

Tesis – Metodología de Implantación de un SGSI en un grupo empresarial jerárquico.[6]

CRITERIOS IMPORTANTES ENCONTRADOS EN LA TESIS DE ESTUDIO	ANALISIS DE APLICABILIDAD EN EL PRESENTE PROYECTO
• Identificación de Activos según el método MAGERIT: ➢ Servicios (externos al cliente e internos) ➢ Datos / Información ➢ Aplicaciones	• Se analiza y estudia el método de identificación de activos brindado por el método de evaluación del riesgo MAGERIT.

➢ Equipos informáticos / Hardware ➢ Redes de comunicaciones: propias y contratadas ➢ Soportes de Información: dispositivos físicos de almacenamiento permanente. ➢ Personal ➢ Equipamiento Auxiliar: acondicionamiento eléctrico, térmico, mobiliario, *UPS*, cableado, etc.	
• Gestión de Riesgos (ISO/IEC 27005): ➢ Definición de criterios básicos: - Criterios para evaluación de riesgos. – Criterio para análisis de impacto. – Criterio para aceptación de riesgos. ➢ Introducción y base normativa. ➢ Enfoque. ➢ Análisis y evaluación de riesgo. ➢ Identificación de Riesgos: **-** identificación de los procesos más relevantes de la empresa **–** identificación de activos **–** identificación de amenazas **–** identificación de controles (existentes) **–** identificación de vulnerabilidades: Herramientas para detección de vulnerabilidades como scanning, test de	• Este ítem brinda soporte en la parte del desarrollo del instrumento de medición que toma como referencia la norma ISO/IEC 27005. • Se definen puntos importantes en cuanto al desarrollo software, en este caso nuestro aplicativo en el sistema SGSI. Puntos importantes como que sea actualizable, de fácil manejo al administrador, que herede funcionalidades, que sea escalable, entre otras.

penetración o hacking ético, auditorias de evaluación de seguridad, inspecciones físicas, reportes de incidentes. • Se establece las características que debe tener un software que apoye el SGSI. Este software debería contar con: ➢ Permitir heredar todos los lineamientos, políticas y recomendaciones aplicables ya sean de la ISO/IEC así como aquellas más específicas que provengan de la empresa. ➢ Brindar funcionalidad de gestión de documentación preservando los requerimientos de confidencialidad, integridad y disponibilidad. ➢ Permitir heredar clasificaciones de activos y riesgos de la empresa principal a la secundaria. ➢ Detectar entrada de activos importantes o de alto nivel para su análisis. ➢ Permitir analizar riesgos enfocándose en cualquiera de los interesantes para el análisis de seguridad: confidencialidad, integridad y disponibilidad. ➢ Ayudar a detectar e identificar procesos y activos críticos así como ayudar a	

lograr eficiencia operativa y eficacia en el establecimiento de controles. ➢ Permitir realizar revaloración de activos periódicamente.	

Tesis - Análisis y Evaluación del Riesgo de la Información: Caso de estudio Universidad Simón Bolívar.[7]

CRITERIOS IMPORTANTES ENCONTRADOS EN LA TESIS DE ESTUDIO	ANALISIS DE APLICABILIDAD EN EL PRESENTE PROYECTO
• Valoración del riesgo a partir de tres elementos: ➢ Estimado del valor de los activos de riesgo: Se analiza el daño económico que el riesgo genera a la empresa. ➢ Probabilidad de ocurrencia del riesgo**:** se analiza con los administradores las amenazas y vulnerabilidades y ocurrencia del riesgo. ➢ Valoración del riesgo de los activos.	• Se tienen en cuenta estos tres elementos para la valoración del riesgo.

Tabla A.5. Identificación de los servicios críticos y dependientes con los que cuenta la División de TIC de la Universidad del Cauca.

LISTA DE CHEQUEO PARA IDENTIFICAR LOS SERVICIOS CRITICOS Y DEPENDIENTES CON LOS QUE CUENTA LA DIVISION DE TIC DE LA UNIVERSIDAD DEL CAUCA					
ENTIDAD: División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca					
FECHA DE REALIZACION DE LA LISTA DE CHEQUEO: 30 - Mayo – 2011					
PARTICIPANTES EN EL LLENADO DE LOS DATOS Y SU RESPONSABILIDAD Fabián Andrés Mera					
REALIZADO POR: Andrés Felipe Mera Oscar Eduardo Mondragón					
1	**Servicios con los que cuenta la División de las TIC's**			**SI**	**NO**	**Observaciones**
1.1		Servidor WEB.		✓		
1.2		Servidor de Correo.		✓		
1.2.1			Correo	✓		
1.2.2			Webmail	✓		
1.2.3			Servidor de Autenticación y Enrutamiento.	✓		
1.3		Servidor DNS.		✓		
1.3.1			IPv4	✓		
1.3.2			IPv6		X	
1.4		Servidor FTP.		✓		
1.5		Servidor Proxy.		✓		
1.6		Servicio de aplicaciones WEB.		✓		
1.6.1			SIMCA	✓		
1.6.2			Aplicaciones de sistemas	✓		
1.7		Servicio Firewall.		✓		
1.8		Servidor de Bases de Datos.		✓		
1.9		Servidor Telnet.			X	
1.10		Servidor de Noticias.			X	*Se cuelga la información en el portal institucional.*
1.11		Servidor IRC			X	
1.12		Servidor de Chat.			X	
1.13		Servidor de Aplicaciones de Escritorio.			X	

1.14		Servidor Backups.	✓		
2	**Servicios Críticos**				
2.1		Servidor WEB	✓		
2.1.1		Servidor Portal Institucional	✓		
2.2		Servidor FTP			
2.3		Servidor Proxy	✓		
2.4		Servidor de Correo	✓		
2.5		Servidor DNS	✓		
2.6		Servidor de Bases de Datos	✓		
2.7		Servidor de Backups	✓		
3	**Servicios Secundarios**				
3.1		Servidor de aplicación SIMCA	✓		*Puede catalogarse como primario.*
3.2		Servidor de aplicaciones de escritorio.		X	
4	**Dependencia de los Servicios.**				
4.1		¿Si el servidor WEB institucional falla, dejan de funcionar otros servicios?	✓		
4.2		¿Existen servicios que dependan del Proxy? ¿Cuáles?		X	
4.4		¿Se afectan otros servicios si el servidor FTP falla? ¿Cuáles?		X	
4.5		¿Si el servidor DNS falla, afecta a otros servicios? ¿Cuáles?	✓		*Todos los servicios WEB, navegación.*
4.6		¿Depende SIMCA que otros servicios estén funcionando? ¿Cuáles?	✓		*WEB, autenticación, base de datos.*
4.7		¿Se podría decir que el servicio más importante es el de WEB de la página Institucional?	✓		*Dado que es la cara visible a internet, es la puerta de entrada a otros servicios (WEB, correo), pero sin DNS no hay servicio WEB.*
4.8		¿Es aceptable la afirmación de que el servidor FTP, Correo, Proxy y WEB trabajan de modo independiente?	✓		*Trabajan independiente pero dependen del DNS para funcionar.*
4.9		¿Si el servicio SIMCA no se encuentra activado, afecta directamente el funcionamiento de otro servicio? ¿Cuáles?		X	

ANALISIS DE RESULTADOS
Se pudo analizar que existen varias dependencias entre servicios, mostrando que el servicio DNS y el WEB cumplen un papel fundamental dando participación a otros servicios como SIMCA, Correo, entre otros.

Tabla A.6. Identificación de amenazas y vulnerabilidades presentes en la División de TIC de la Universidad del Cauca.

LISTA DE CHEQUEO PARA IDENTIFICAR LAS VULNERABILIDAD Y AMENAZAS PRESENTES EN LA DIVISION DE TIC DEL A UNIVERSIDAD DEL CAUCA						
ENTIDAD: División de Tecnologías de la Información y la comunicación de la Universidad del Cauca						
FECHA DE REALIZACION DE LA LISTA DE CHEQUEO: 31 - Agosto – 2011						
PARTICIPANTES EN EL LLENADO DE LOS DATOS Y SU RESPONSABILIDAD Fabián Andrés Mera						
REALIZADO POR: Andrés Felipe Mera Oscar Eduardo Mondragón						
1	**VULNERABILIDADES**			**SI**	**NO**	**EXPLICACION**
1.1		Contraseñas:				
1.1.1			¿Usted considera que el sistema de contraseñas es seguro?	✓	X	*Si para los administradores de servicios. Las contraseñas de los usuarios NO.*
1.1.2			¿Implementan contraseñas de mínimo 8 caracteres alfanuméricos y especiales?	✓	X	*SI para admin. NO, los usuarios implementan cualquier tipo de contraseña.*
1.1.3			¿El uso de contraseñas es exclusivo para administradores?	✓		
1.1.4			¿Existen varios usuarios con privilegios de administrador? ¿Cuántos?		X	
1.1.5			¿Se están cambiando periódicamente las contraseñas? ¿Con que periodo?	✓		*Seis meses*

1.1.6			¿En caso de sufrir un accidente usted como administrador de los servicios, alguien más tiene acceso a los servicios informáticos que gestiona?	✓		*Una persona*
1.1.7			¿La infraestructura del lugar de alojamiento de los servidores podría permitir la usurpación de las contraseñas?		X	*Actualmente se están implementando mecanismos de control de acceso.*
1.1.8			¿Usted como administrador, realiza las conexiones a los servicios informáticos desde el ordenador principal o también se conecta a través de su ordenador personal?	✓		
1.1.9			¿Existen protocolos de comunicación seguros para el acceso a la gestión de los servicios a través de su ordenador personal?	✓		
1.1.10			¿Su equipo cuenta con protección de códigos malware?	✓		
1.1.11			¿Existe trazabilidad en los cambios significativos de los servicios informáticos?		X	*No está claramente definido.*
1.1.12			¿Existen procedimiento para la creación, modificación y/o eliminación de los usuarios con privilegios de administrador?		X	
1.1.12			¿Se realiza copias de respaldo de la información de las bases de datos?	✓		*Apenas se está estandarizando el proceso.*
1.1.13			¿Se cifran las copias de respaldo?		X	
1.1.14			¿Cuenta con buena ubicación física los equipos de intermedios y finales de comunicación?	✓		*Vlans separadas.*
1.2		Sistemas Operativos:				
1.2.1			¿Se utilizan diferentes S.O. en los servicios implementados?	✓		
1.2.2			¿Los S.O. están actualizados a la fecha y cuentan con todos los parches de seguridad?		X	*El 60 % cumplen con las últimas versiones.*
1.2.3			¿Entre los Sistemas Operativos se manejan diferentes contraseñas administrativas? ¿Y se cambian las que vienen por defecto?	✓		
1.2.4			¿Se maneja de forma segura la información cuando se migra de S.O.?		X	*No hay un proceso*

			(backups, copias de respaldo, destrucción de copias)			*estandarizado.*
2	**AMENAZAS**					
2.1		Malwares y ataques:				
2.1.1			¿Se cuenta con sistemas actualizados de protección de la información como antivirus, firewalls, anti-malwares?	✓		*Firewall, antivirus*
2.1.3			¿Se cuenta con IDS/IPS?	✓		*Pero está en fase de pruebas.*
2.1.4			¿El sistema es capaz de una detección y prevención de ataques como “Man-in-the-midle”, DoS, DDoS, sniffers?	✓		*No está implementado.*
2.1.4			¿El personal, a parte de los administradores, pueden realizar instalación de programas (autorizados o no) en los servidores de los servicios pudiendo comprometer la seguridad de la información?	✓		*No se hace pero es posible ya que no hay una política al respecto.*
2.2		Dispositivos de almacenamiento masivo:				
2.2.1			¿La información se transporta de forma segura en dispositivos móviles como USB y discos duros?		X	*No se transporta la información por medio de estos elementos.*
2.2.2			¿En caso de robo de un dispositivo, que medidas implementan para evitar accesos prohibidos?			
2.2.3			¿Quiénes tienen acceso al transporte de dispositivos móviles de información?			
2.2.4			¿La información va cifrada y el dispositivo móvil va protegido por contraseña?			

Tabla A.7. Encuesta para identificación de amenazas y vulnerabilidades presentes en la División de TIC de la Universidad del Cauca.

Fecha	26/09/2011						
Encuestado	Fabián Andrés Mera	**Cargo**	Administrador				
Proyecto	Sistema de alarmas de seguridad informática para los servicios críticos de la División de TIC de la Universidad del Cauca	**Piso**	1	**Tipo de Equipo**	Portátil	**Encuestador**	Andrés Felipe Mera – Oscar Mondragón

		SEGURIDAD LÓGICA	**CALIFICACIÓN TOTAL**		**NIVEL**		**Educación**		**NIVEL**	
		1. Control de acceso								
		1.1. Evaluación de contraseñas						**SI**	**NO**	**NS/NR**
1	1	a. Comparto mi contraseña de acceso al servidor con mis compañeros de trabajo							x	
2	2	b. Mi contraseña tiene estrictamente menos de 8 caracteres							x	
3	3	c. Mi contraseña tiene por lo menos un carácter especial, por ejemplo (!"#$%&/()=?¡) entre otros						x		
4	4	d. Mi contraseña tiene que ver algo con mi lugar de trabajo, familia o amigo							x	
5	5	e. Mi contraseña tiene que ver con una secuencia de solo números, placa de mi transporte o la identificación de algún documento							x	
6	6	f. Repito periódicamente mis contraseñas para no olvidarlas							x	
7	7	g. Para no olvidar mi contraseña la anoto en un sitio seguro o cercano a mi lugar de trabajo							x	
8	8	h. Acostumbro utilizar programas que generen la contraseña por mi							x	
9	9	i. Mi contraseña ha sido descifrada alguna vez								No sé, de pronto
1	1	j. Mi equipo tiene contraseña de arranque							x	

00	en la BIOS				
11	k. Conozco alguna política sobre el manejo de contraseñas	x			
12	l. He recibido alguna capacitación sobre el manejo correcto de contraseñas	x		Buscando en internet	
13	m. Conoce usted algún control de intentos de accesos no autorizados al sistema	x			
14	n. No puedo acceder a ningún sistema si no me identifico correctamente		x		
15	o. Quedo inhabilitado después de un número determinado de intentos infructuosos al dar la contraseña en el servidor de acceso local		x		
16	p. Utilizo la misma contraseña para acceder a diferentes programas		x		
17	q. Comparto mi contraseña de acceso a programas con mis compañeros de trabajo		x		
18	r. Utilizo la misma contraseña para acceder a diferentes equipos	x			
19	s. Mi equipo tiene protector de pantalla con contraseña		x		

Calificación		Nivel:		Educación		Nivel:	

2. Manejo de la información			
2.1 Controles de actualización	**SI**	**NO**	**NS/NR**
201 a. Mantengo una copia actualizada en el servidor		x	
212 b. Conozco las actualizaciones del software licenciado que tengo instalado en mi equipo		x	
223 c. Existen políticas de actualización del software		x	
234 d. Informo sobre actualizaciones del software instalado en mi equipo a la División de Sistemas		x	
245 e. Verifico que la actualización del software sea del mismo proveedor		x	
256 f. Recibo capacitación para la utilización del software actualizado		x	

Calificación		Nivel:		Educación		Nivel:	

2.2 Control de virus	**SI**	**NO**	**NS/NR**
261 a. Sé manejar completamente el antivirus que se me instaló en el equipo		x	
272 b. Actualizo por lo menos una vez al mes mi antivirus		x	
23 c. Vacuno por lo menos una vez al día mi		x	

8		equipo			
29	4	d. Cualquier archivo que llega a mi equipo, sea desde una página web, correo electrónico, servidor de archivos o diskette es vacunado		x	
30	5	e. He perdido información por causa de algún virus		x	
31	6	f. Existen políticas para la utilización de los antivirus		x	
32	7	g. Tengo correctamente configurado mi antivirus			No se
33	8	h. Tengo en cuenta las sugerencias del administrador de la red sobre solución de problemas de virus			x
34	9	i. Instalo programas desde internet, sin autorización del administrador de la red, que me facilitan un poco el trabajo	x		
35	10	i. Conozco medidas de contingencia ante el ataque de un virus			x

Calificación		**Nivel:**		**Educación**		**Nivel:**	

		2.3 Controles para el manejo seguro de la información	**SI**	**NO**	**NS/NR**
36	1	a. La información crítica de la entidad la manejo encriptada		x	
37	2	b. Me llevo trabajo de la entidad para adelantarlo en mi casa	x		
38	3	c. Envío información crítica de la entidad por correo electrónico sin encriptarla	x		
39	4	d. He recibido capacitación para el manejo de sistemas de encripción		x	
40	5	e. Existe un centro para el almacenamiento y custodia de soportes magnéticos		x	
41	6	f. Conozco alguna política para el manejo de encripción de la información			x

Calificación		**Nivel:**		**Educación**		**Nivel:**	

		3. Manejo del software			
		3.1 Control de licenciamiento de software	**SI**	**NO**	**NS/NR**
42	1	a. Todos los programas instalados están licenciados	x		
43	2	b. Conozco los tipos de licencias que puedo usar libremente sin pagar	x		
44	3	c. Tengo en mi poder algún contrato de licencia de programa instalado en el equipo		x	
45	4	d. Conozco políticas para el manejo de software licenciado		x	

45		e. Instalo software licenciado de la entidad en cualquier otro sitio diferente al autorizado		x	
46	5	f. Mantengo en mi poder los instaladores de los programas licenciados		x	
47	6	g. Utilizo software sin licencia en mi equipo		x	
48	7	h. He realizado varias copias de seguridad de los programas licenciados de la entidad		x	
49	8	i. Recibí capacitación y soporte para la utilización del software licenciado		x	
50	9	j. Utilizo programas crackeados	x		
51	10	k. Conozco las consecuencias legales por el manejo de software sin licencia		x	
52	11				

Calificación		**Nivel:**		**Educación**		**Nivel:**	

		3.2 Control de instalación de software	**SI**	**NO**	**NS/NR**
53	1	a. Informo a la división de sistemas sobre la instalación de programas en mi equipo		x	
54	2	b. Tengo instalados programas innecesarios ¿Cuáles?		x	
55	3	c. Conozco políticas para la instalación de software		x	
56	4	d. Informo a la División de sistemas en caso de formateo del equipo o desinstalación del software licenciado		x	
57	5	e. Establezco configuraciones cuando deseo, sin informar al personal encargado	x		
58	6	f. Informo cualquier fallo del software al proveedor o a la unidad encargada		x	

Calificación		**Nivel:**		**Educación**		**Nivel:**	

		4. Salida de información			
		4.1 Controles de la salida de Información	**SI**	**NO**	**NS/NR**
59	1	a. Existe control de la salida de soportes magnéticos hacia otras dependencias ¿Cuáles dependencias?		x	
60	2	b. Puedo enviar información vía e-mail a destinatarios no autorizados	x		
61	3	c. Puedo enviar información vía fax a destinatarios no autorizados	x		
62	4	d. Se radica la información que sale de mi oficina	x		
63	5	e. Existen controles		x	

		para la impresión			
6		f. Conozco el destino de la información que sale			
4	6	de mi oficina			x

Calificación		Nivel:		Educación		Nivel:	

		5. Entrada de datos			
		5.1 Controles de entrada de datos	**SI**	**NO**	**NS/NR**
6		a. Existe control de la entrada de soportes magnéticos desde otras			
5	1	dependencias ¿Cuáles dependencias?		x	
6		b. Existen políticas de control para recibir datos vía			
6	2	e-mail o Fax ¿Qué tipo de datos?		x	
6		c. Se radican los datos que			
7	3	llegan a mi oficina	x		
6		d. Conozco el origen de los datos que			
8	4	llegan a mi oficina			x
6		e. Existen políticas para el manejo de datos con			
9	5	origen desconocido		x	

Calificación		Nivel:		Educación		Nivel:	

SEGURIDAD FÍSICA	**CALIFICACIÓN TOTAL**		**NIVEL**		**Educación**		**NIVEL**	

		1. Utilización de equipos			
		1.1 Controles de uso	**SI**	**NO**	**NS/NR**
7		a. Utilizo el PC más de 4			
0	1	horas diarias	x		
7		b. Utilizo la impresora menos de 5 veces a			
1	2	la semana		x	x
7		c. Por lo menos alguna vez recibí capacitación			
2	3	para utilizar el PC		x	
7		d. Todos los periféricos que dispongo son necesarios			
3	4	para desarrollar mi labor	x		
7		e. Por lo menos alguna vez recibí capacitación			
4	5	para utilizar la impresora		x	

Calificación		Nivel:		Educación		Nivel:	

		1.2 Controles para la optimización de los equipos	SI	NO	NS/NR
75	1	a. Comparto el PC asignado con 2 o más compañeros		x	
76	2	b. Tengo una o más impresoras asignadas para uso exclusivo		x	
77	3	c. No tengo impresora en la oficina	x		
78	4	d. Tengo PC, pero está dañado, en el momento no tengo			x
79	5	e. Tengo impresora, pero está dañada, en el momento no tengo			x
80	6	f. Utilizo impresora compartida por red	x		
81	7	g. Conozco alguna política que optimice la utilización de los equipos		x	
82	8	h. El programa que más utilizo es Office		x	
83	9	i. El PC es muy antiguo para mis necesidades, utilizo programas que exigen mucho hardware	x		
84	10	j. La impresora es muy obsoleta para mis necesidades			x

Calificación		Nivel:		Educación		Nivel:	

		2. Cuidado del equipo 2.1 Controles en el cuidado del equipo	SI	NO	NS/NR
85	1	a. Mantengo el equipo en un lugar fresco, recomendable e ideal		x	
86	2	b. Se le realiza el mantenimiento de hardware necesario por personal del área de equipos		x	
87	3	c. En el caso que no sea portátil, permanece en el mismo sitio constantemente			x
88	4	d. Permanece completamente cerrado el equipo			x
89	5	e. Evito ingerir alimentos cerca del equipo	x		
90	6	f. Instalo hardware por mi cuenta y no aviso al área de equipos		x	
91	7	g. Utilizo el equipo de forma correcta conforme indica el manual			x
92	8	h. Poseo alguna UPS que respalde la ausencia de energía	x		
99		i. He perdido información importante por causa de la		x	

3	interrupción de energía eléctrica				
91 40	j. Se ha dañado algún componente de mi equipo por causa de la interrupción de la energía eléctrica		x		
91 51	k. Conozco alguna política con respecto al cuidado del equipo		x		

Calificación		Nivel:		Educación		Nivel:	

SEGURIDAD LOCATIVA	CALIFICACIÓN TOTAL		NIVEL		Educación		NIVEL	

1. Ubicación de los equipos con respecto a las instalaciones

	1.1 Control de acceso a las instalaciones.	**SI**	**NO**	**NS/NR**
96 1	a. Hay acceso restringido a la oficina donde se encuentra ubicado mi equipo de computo	x		
97 2	b. Existen canales de comunicación físico que unan mi oficina con otras dependencias		x	
98 3	c. Comparto mi oficina con otros compañeros de trabajo	x		
99 4	d. Existen medios de autenticación de acceso físico a mi oficina	x		
100 05	e. Comparto el medio de acceso a mi oficina con personas no autorizadas	x		
101 6	f. Hay acceso restringido al edificio donde se encuentra ubicada mi oficina	x		
102 7	g. Conoce usted controles de inspección en la entrada y salida de vehículos en la zona de parqueadero		x	
103 8	h. Mi equipo, los servidores o terminales están ubicados en zonas de paso		x	
104 9	i. Mi equipo o centros de almacenamiento de soportes magnéticos, quedan próximos a ventanas accesibles desde afuera		x	
105 0	j. Considera que la construcción de su oficina posibilita el acceso no autorizado		x	

Calificación		Nivel:		Educación		Nivel:	

		2. Ubicación de los equipos			
		2.1 Control ambiental en el manejo de los equipos	**SI**	**NO**	**NS/NR**
106	1	a. Existen filtraciones de agua que pueden afectar mi equipo de computo		x	
107	2	b. Mi equipo de computo queda expuesto al sol		x	
108	3	c. Existen filtraciones de agua que pueden afectar los soportes magnéticos		x	
109	4	d. Los soportes magnéticos quedan expuestos al sol		x	
110	5	e. El equipo permanece siempre en el mismo sitio			Portátil
111	6	f. El PC se ha averiado por algún fenómeno natural		x	
112	7	g. La impresora se ha averiado por algún fenómeno natural		x	
113	8	h. Existen planes de contingencia ante una catástrofe de tipo natural (incendios, inundaciones y terremotos)			x

Calificación		**Nivel:**		**Educación**		**Nivel:**	

Tabla A.8. Graficas matriz de riesgos.

	Activo	Vr Económico del Activo	Integridad	Confidencialidad	Disponibilidad	Vr. Del Activo	Clasificación del VA	Impacto	Clasificación del Impacto	Vulnerabilidad	El periodo de cambio de contraseñas es muy largo (Seis Meses)	No estan aprobados los mecanismos de control de acceso físico a las instalaciones		Acceso a los servidores desde equipos de cómputo personal	No se encuentra aprobado el proceso de copias de respaldo de información	No existe cifrado de las copias de respaldo de información
										Amenaza	Acceso no autorizado	Acceso no autorizado		Espionaje remoto	Acceso no autorizado	Acceso no autorizado
										Riesgo	Fuga de información	Fuga de información	Modificación de la información	Robo de información	Pérdida de la información	Fuga de información
										TR	Lógico	Físico	Lógico	Lógico	Lógico	Lógico
										P M	29,55%	31,82%	29,55%	29,55%	29,55%	29,55%
										P A	15%	15%	65%	15%	15%	70%
										P T	19,36	20,05	54,36	19,36	19,36	57,86
										Clasif	1	1	3	1	1	3
1	Servidor WEB	1	5	5	5	16	MA	5	MA		1	1	1	1	1	1
2	Servidor Correo	2	5	5	5	17	MA	5	MA		1	1	1	1	1	1
3	Servidor DNS	1	5	5	5	16	MA	5	MA		1	1	1	1		
4	Servidor Proxy	1	5	5	5	16	MA	5	MA		1	1	1	1		
5	Servidor SIMCA	1	5	5	5	16	MA	5	MA		1	1	1	1	1	1
6	Servicio fluido eléctrico	3	5	5	5	18	MA	4	M			1	1			
7	Cableado estructurado	3	5	5	5	18	MA	5	MA			1	1			
8	Equipos de resplado eléctrico	2	2	3	5	12	M	5	MA			1	1			
9	Equipo de Cómputo personal	1	5	5	5	16	MA	3	B			1	1			

	Activo	Vr Económico del Activo	Integridad	Confidencialidad	Disponibilidad	Vr. Del Activo	Clasificación del VA	Impacto	Clasificación del Impacto	Vulnerabilidad	Ausencia de procedimientos formal para el registro y retiro de usuarios	Ausencia de procedimientos formal para el registro y retiro de usuarios	Inadecuada ubicación de los equipos de respaldo electrico	Inadecuada ubicación de los servidores
										Amenaza	Abuso de derechos	Abuso de derechos	Factores climatológicos	Factores climatológicos
										Riesgo	Fuga de información	Modificación de la información	Daño físico de los equipos de respaldo eléctrico	Daño físico de los servidores físicos
										TR	Lógico	Lógico	Lógico	Lógico
										P M	29,55%	29,55%	29,55%	29,55%
										P A	60%	60%	60%	60%
										P T	50,86	50,86	50,86	50,86
										Clasif	3	3	3	3
1	Servidor WEB	1	5	5	5	16	MA	5	MA		1	1		1
2	Servidor Correo	2	5	5	5	17	MA	5	MA		1	1		1
3	Servidor DNS	1	5	5	5	16	MA	5	MA		1	1		1
4	Servidor Proxy	1	5	5	5	16	MA	5	MA		1	1		1
5	Servidor SIMCA	1	5	5	5	16	MA	5	MA		1	1		1
6	Servicio fluido eléctrico	3	5	5	5	18	MA	4	M					
7	Cableado estructurado	3	5	5	5	18	MA	5	MA					
8	Equipos de resplado eléctrico	2	2	3	5	12	M	5	MA				1	
9	Equipo de Cómputo personal	1	5	5	5	16	MA	3	B					1

	Activo	Vr Económico del Activo	Integridad	Confidencialidad	Disponibilidad	Vr. Del Activo	Clasificación del VA	Impacto	Clasificación del Impacto	Vulnerabilidad	debilidades conocidas en el software del sistema operativo usado			Aun no se aprueba el uso de sistema de deteccion de intrusos	
										Amenaza	Acceso no autorizado			Acceso no autorizado	
										Riesgo	Modificación de la información	Fuga de la información	Eliminación de la información	Fuga de la información	Eliminación de la información
										TR	Lógico	Lógico	Lógico	Lógico	Lógico
										P M	29,55%	29,55%	29,55%	29,55%	29,55%
										P A	60%	60%	60%	60%	60%
										P T	50,86	50,86	50,86	50,86	50,86
										Clasif	3	3	3	3	3
1	Servidor WEB	1	5	5	5	16	MA	5	MA		1	1	1	1	1
2	Servidor Correo	2	5	5	5	17	MA	5	MA		1	1	1	1	1
3	Servidor DNS	1	5	5	5	16	MA	5	MA		1	1	1	1	1
4	Servidor Proxy	1	5	5	5	16	MA	5	MA		1	1	1	1	1
5	Servidor SIMCA	1	5	5	5	16	MA	5	MA		1	1	1	1	1
6	Servicio fluido eléctrico	3	5	5	5	18	MA	4	M						
7	Cableado estructurado	3	5	5	5	18	MA	5	MA						
8	Equipos de resplado eléctrico	2	2	3	5	12	M	5	MA						
9	Equipo de Cómputo personal	1	5	5	5	16	MA	3	B		1	1	1	1	1

ANEXO B: Políticas y procedimientos de seguridad

B.1. Políticas y procedimientos de seguridad para el servicio CORREO ELECTRONICO.

POLITICAS PARA LOS ***USUARIOS***

PU1. Cualquier persona que certifique su vínculo con la Universidad del Cauca ya sean funcionarios, docentes, administrativos, estudiantes, ex-alumnos y pensionados, tendrán derecho a la creación de una *cuenta de correo electrónico institucional individual*.

PU2. Cualquier grupo institucional que certifique su vínculo con la Universidad del Cauca ya sean funcionarios, docentes, administrativos, estudiantes, ex-alumnos y pensionados, tendrán derecho a la creación de una *cuenta de correo electrónico institucional para ese grupo*.

PU3. Cualquier ente académico-administrativo que certifique su vínculo con la Universidad del Cauca ya sean funcionarios, docentes, administrativos, estudiantes, ex-alumnos y pensionados, tendrá derecho a la creación de una *lista de correo electrónico institucional*, donde se agruparán el listado de las respectivas cuentas individuales.

PU4. El responsable de cada cuenta de correo electrónico al recibir la respectiva contraseña, deberá inmediatamente cambiarla y mantener la confidencialidad de la misma.

PU5. El responsable de cada cuenta de correo electrónico deberá guardar copias de respaldo de su información que considere conveniente.

PU6. El uso de la cuenta de correo electrónico institucional será únicamente para actividades académicas y/o administrativas relacionadas con el quehacer de la institución.

PU7. Se prohíbe el envío de correos masivos que no cuenten con la debida autorización escrita de la Rectoría de la Universidad del Cauca.

PU8. Todo usuario que acceda al servicio de correo electrónico institucional conoce, acepta y debe cumplir las políticas relacionadas con la prestación del servicio de correo electrónico institucional.

PU9. El uso indebido del servicio de correo electrónico institucional acarreará las sanciones reglamentarias, legales o jurídicas según el caso y generará la suspensión inmediata del servicio al usuario involucrado.

PROCEDIMIENTOS PARA LOS ***USUARIOS***

Convención: PUxpy, la **PU** equivale a **Política de Usuario**, ***x*** equivale al ***número de la política***, **p** equivale al ***procedimiento*** y "***y***" equivale al ***número del procedimiento***.

PU1p1: Para la creación de una cuenta de correo electrónico institucional individual.

- Dirigirse a la Oficina CONTACTO55 adscrita a la División de las TIC.
- Solicitar personalmente y presentar el carnet institucional actualizado que certifique su vínculo con la Universidad del Cauca por la persona interesada.
- El funcionario de la oficina CONTACTO55 verificará la validez del carnet institucional.

PU2p1: Para la creación de una cuenta de correo electrónico de grupo institucional.

- Dirigirse a la Oficina CONTACTO55 adscrita a la División de las TIC.
- Solicitar personalmente y presentar el carnet institucional actualizado que certifique su vínculo con la Universidad del Cauca por la persona representante del grupo institucional y los objetivos del grupo avalados por su jefe inmediato.
- El funcionario de la oficina CONTACTO55 verificará la validez del carnet institucional y el aval del jefe inmediato.

PU3p1: Para la creación de una lista de correo electrónico institucional.

- Dirigirse a la Oficina CONTACTO55 adscrita a la División de las TIC.
- Solicitar personalmente y presentar el carnet institucional actualizado que certifique su vínculo con la Universidad del Cauca por la persona representante del ente académico-administrativo.
- El funcionario de la oficina CONTACTO55 verificará la validez del carnet institucional y el cargo del solicitante.

PU4p1: Para la Administración de la cuenta.

- El usuario solicitante es el responsable de la administración de la cuenta de correo electrónico.
- El usuario debe ingresar a la aplicación respectiva y seguir los pasos sugeridos por la administración del servicio.
- La aplicación verificará las sugerencias y recomendaciones para cambiar la contraseña con un alto nivel de seguridad. (Se sugiere que la división debe asignar el tiempo de vida y manejar el histórico de la contraseña en la aplicación)

PU5p1: Para realizar copias de respaldo.

- El usuario de la cuenta de correo electrónico es el responsable de realizar las copias de respaldo.
- El usuario de la cuenta de correo electrónico debe guardar sus copias de respaldo con los mecanismos y procedimientos que considere pertinentes.
- El usuario definirá la periodicidad de ejecución de este proceso.

PU6p1: Para el uso de la cuenta de correo.

- El usuario de la cuenta de correo electrónico es el único responsable de su utilización.
- El usuario de la cuenta de correo electrónico tiene el deber de utilizar el servicio institucional con fines únicamente académicos y/o administrativos.
- La administración del servicio de correo electrónico de la institución verificará periódicamente la utilización del servicio de correo.

PU7p1: Para la difusión de correo masivo de interés institucional.

- El usuario de la cuenta de correo electrónico es el único responsable de la difusión.
- El usuario de la cuenta de correo electrónico solicitará la autorización escrita a la Rectoría de la Universidad del Cauca.
- La administración del servicio verificará la validez de la autorización.

PU8p1: Sobre el cumplimiento de las políticas del servicio de correo electrónico.

- Los usuarios de las cuentas de correo electrónico son los responsables del cumplimiento de las políticas del servicio.
- La administración del servicio de correo electrónico socializará las políticas relacionadas con la prestación del servicio.
- Los administradores del servicio de correo electrónico verificaran el cumplimiento de cada política en los registros del servicio.

PU9p1: Sobre el uso indebido del servicio de correo electrónico.

- Los usuarios de las cuentas de correo electrónico son los únicos responsables del uso indebido del servicio.
- La administración del servicio de correo electrónico socializará el funcionamiento y uso adecuado del servicio.
- La administración del servicio de correo electrónico verificará el uso adecuado del servicio en los registros.

POLITICAS PARA LOS ***ADMINISTRADORES***

PA1. Cada uno de los administradores y operadores del servicio de correo electrónico institucional deben tener una cuenta individual con sus correspondientes privilegios.

PA2. Únicamente los operadores del *servicio de correo electrónico institucional* están autorizados para crear las cuentas individuales, de grupo y las listas de correo.

PA3. Los operadores del *servicio de correo electrónico institucional* deberán garantizar la confidencialidad de las contraseñas de las respectivas cuentas creadas.

PA4. Los operadores del *servicio de correo electrónico institucional* deberán realizar copias de respaldo periódicas de los buzones de todos los usuarios del correo electrónico institucional.

PA5. Los operadores del *servicio de correo electrónico institucional* deberán analizar que los servidores no sean utilizados para el envío de correos masivos a menos que cuenten con la debida autorización.

PA6. Los administradores del *servicio de correo electrónico institucional* deberán realizar procesos de capacitación dirigidos a toda la comunidad universitaria con el propósito de socializar las políticas relacionadas con la prestación del servicio de correo electrónico.

PA7. Los administradores y operadores del *servicio de correo electrónico institucional* deberán informar del uso indebido del servicio de correo por parte de cualquier usuario al jefe inmediato quién se encargará de hacer efectivas las sanciones a que haya lugar, además se le suspenderá el servicio al usuario(s) involucrado(s).

PA8. Todos los procedimientos relacionados con la prestación del *servicio de correo electrónico institucional* deben estar debidamente documentados.

PA9. Planear y ejecutar procesos de mantenimiento preventivo, correctivo y predictivo sobre el servicio del correo electrónico institucional.

PA10. Todos los administradores y operadores del *servicio de correo electrónico institucional* deberán conocer, aceptar y cumplir las políticas relacionadas con la administración del servicio de correo electrónico.

PA11. El no cumplimiento de las Políticas relacionadas con la administración del servicio correo electrónico institucional acarreará las sanciones reglamentarias, legales o jurídicas según el caso y generará la suspensión inmediata del cargo a la persona involucrada.

BIBLIOGRAFIA

[1] LARA MUÑOZ, Hernán; REYES REINA, José Humberto; NAVARRETE MERA, Washington . *"Diseño De Sistema De Gestión De Seguridad De Información Para Ecuacolor"*. Disponible en: http://www.dspace.espol.edu.ec/bitstream/123456789/6962/8/Tesis%20de%20grado.pdf

[2] LAMILLA, Erick. *"Desarrollo De Políticas De Seguridad Informática E Implementación De Cuatro Dominios En Base A La Norma 27002 Para El Área De Hardware En La Empresa Uniplex Systems S.A. En Guayaquil"*. Disponible en: http://www.dspace.espol.edu.ec/bitstream/123456789/5247/1/Desarrollo%20de%20Pol%C3%ADticas%20de%20Seguridad%20Inform%C3%A1tica%20e%20Implementaci%C3%B3n.pdf

[3] ARANDA SEGOVIA, José Alfonso. *"IMPLEMENTACION DEL PRIMER SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION, EN EL ECUADOR, CERTIFICADO BAJO LA NORMA ISO 27001:2005"*. Disponible en: https://www.dspace.espol.edu.ec/bitstream/123456789/7718/1/D-39433.pdf

[4] ALVAREZ ZURITA, Flor María; GARCIA GUSZMAN, Pamela Anabel. *"Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001, para la intranet de la Corporación Metropolitana de Salud"*. Disponible en: bibdigital.epn.edu.ec/bitstream/15000/565/1/CD-1077.pdf

[5] FLORES ESTEVEZ, Fanny Paulina; JIMENEZ NUÑEZ, Diana Carolina. *"Diseño de un sistema de gestión de seguridad de la información para la empresa MEGADATOS S.A. en la ciudad de Quito, aplicando las normas ISO 27001 e ISO 27002"*. Disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/2414/1/CD-3144.pdf

[6] PALLAS, Gustavo; CORTI, María Eugenia. *"Metodología de implantación de un SGSI en un grupo empresarial jerárquico"*. Disponible en: http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

[7] DE FREITAS, Vidalina. "*Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar*". Revista Venezolana de información, tecnología y conocimiento (2009). Disponible en: www.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1690-75152009000100004&lng=en&nrm=iso