PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUTO PARA LA ECONOMÍA SOCIAL - IPES

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Comentarios (visión general de la implementación)	Responsables
Dominio	**Sección**	**Objetivo de control / control**				
5 Políticas de Seguridad	5.1	Orientación de la Dirección para la gestión de la seguridad de la información				
	5.1.1	Políticas para la seguridad de la información	SI		Definición, implementación, mantenimiento y mejora de las políticas de seguridad y privacidad de la información aprobadas por la dirección. Socializar, sensibilizar y comunicar las políticas de seguridad y privacidad de la información a todas las partes interesadas	Comité de Sistemas y Seguridad de la Información Dirección General Subdirecciones
	5.1.2	Revisión de las políticas de seguridad de la información	SI		Definición, implementación, mantenimiento y mejora de las políticas de seguridad y privacidad de la información aprobadas por la dirección. Socializar, sensibilizar y comunicar las políticas de seguridad y privacidad de la información a todas las partes interesadas	Comité de Sistemas y Seguridad de la Información Dirección General Subdirecciones
6 Organización de la Seguridad de la Información	6.1	Organización interna				
	6.1.1	Roles y responsabilidad de seguridad de la información	SI		Delegación del rol Oficial de Seguridad de la información. Delegación del Responsable del tratamiento de los datos en la entidad Socialización y aprobación del documento roles y Responsabilidades de seguridad y privacidad de la información.	Comité de Sistemas y Seguridad de la Información Subdirección de Diseño y Análisis Estratégico Subdirección administrativa y Financiera - Talento Humano
	6.1.2	Separación de deberes	SI		Revisión y mejoramiento en la segregación de tareas y areas con conflicto de responsabilidad segregada, para reducir las oportunidades de modificación no autorizada o involuntaria, o el mal uso, de los activos de la entidad.	
	6.1.3	Contacto con autoridades	SI		Definición, revision, mantenimiento y mejora de los procedimientos de contactos apropiados con las autoridades relevantes.	
	6.1.4	Contacto con grupos de interés especial	SI		Definición, revision, mantenimiento y mejora de los procedimientos de contacto apropiado con los grupos especiales de interés así como otros foros especializados en seguridad de la información y asociaciones profesionales	
	6.1.5	Seguridad de la información en la gestión de proyectos	SI		Definición, revision, mantenimiento y mejora de los procedimientos de seguridad de la Información en la gestión de proyectos.	
	6.2	Dispositivos móviles y teletrabajo				
	6.2.1	Política de dispositivos móviles	SI		Definición, implementación, mantenimiento y mejora de las políticas de seguridad y privacidad de la información aprobadas por la dirección. Socializar, sensibilizar y comunicar las políticas de seguridad y privacidad de la información a todas las partes interesadas	Comité de Sistemas y Seguridad de la Información

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Comentarios (visión general de la implementación)	Responsables
	6.2.2	Teletrabajo	SI		Definición, implementación, mantenimiento y mejora de las políticas de seguridad y privacidad de la información aprobadas por la dirección. Socializar, sensibilizar y comunicar las políticas de seguridad y privacidad de la información a todas las partes interesadas	Subdirección de Diseño y Análisis Estratégico
7 Seguridad en los Recursos Humanos	7.1	Previo al empleo				
	7.1.1	Selección	SI		Definición, revisión, mantenimiento y mejora de los procedimientos de selección del personal (competencias, antecedentes), responsabilidades de usuarios frente a seguridad de la información. Obligaciones contractuales para funcionarios y contratistas	Subdirección juridica y de Contratación Subdirección Administrativa y Financiera - Talento humano Dirección General
	7.1.2	Términos y condiciones del empleo	SI		Definición, revisión, mantenimiento y mejora de los procedimientos relacionados con recursos humanos (terminación, cambio de empleo)	
	7.2	Durante el empleo				
	7.2.1	Responsabilidades de la Dirección	SI		Definición, revisión, mantenimiento y mejora de los procedimientos de selección del personal (competencias, antecedentes), responsabilidades de usuarios frente a seguridad de la información. Obligaciones contractuales para funcionarios y contratistas Definición, revisión, mantenimiento y mejora de los procedimientos relacionados con recursos humanos (terminación, cambio de empleo)	
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	SI		Definición y ejecución del plan de sensibilización y capacitación sobre seguridad y privacidad de la información	
	7.2.3	Proceso disciplinario	SI		Definición, revisión, mantenimiento y mejora de los procedimientos de acciones disciplinarias frente a posibles fallas a la seguridad de la información	
	7.3	Terminación y cambio de empleo				
	7.3.1	Termino de responsabilidades o cambio de empleo	SI		Definición, revisión, mantenimiento y mejora de los procedimientos relacionados con recursos humanos (terminación, cambio de empleo)	Subdirección Administrativa y Financiera - Talento Humano Subdirección Jurídica y de Contratción Subdirección de Diseño y Análisis Estratégico
	8.1	Responsabilidad de los activos				
	8.1.1	Inventario de activos	SI		Definición, implementación, mantenimiento y mejora del inventario de activos de información. (formatos, procedimientos, guías, instructivos)	
	8.1.2	Propiedad de activos	SI		Definición, implementación, mantenimiento y mejora de controles frente a la asignación, clasificación, etiquetado, uso apropiado y acceso a los activos de información de la entidad.	Comité de Sistemas y

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Comentarios (visión general de la implementación)	Responsables
8 Gestión de Activos	8.1.3	Uso aceptable de los activos	SI		Definición, implementación, mantenimiento y mejora de controles frente a la asignación, clasificación, etiquetado, uso apropiado y acceso a los activos de información de la entidad.	Seguridad de la Información Todas las Áreas
	8.1.4	Devolución de activos	SI		Definición, implementación, mantenimiento y mejora de controles frente a la asignación, clasificación, etiquetado, uso apropiado y acceso a los activos de información de la entidad.	
	8.2	Clasificación de la información				
	8.2.1	Clasificación de la información	SI		Definición, implementación, mantenimiento y mejora de controles frente a la asignación, clasificación, etiquetado, uso apropiado y acceso a los activos de información de la entidad.	Comité de Sistemas y Seguridad de la Información Todas las Áreas
	8.2.2	Etiquetado de la información	SI		Definición, implementación, mantenimiento y mejora de controles frente a la asignación, clasificación, etiquetado, uso apropiado y acceso a los activos de información de la entidad.	
	8.2.3	Manejo de activos	SI		Definición, implementación, mantenimiento y mejora de controles frente a la asignación, clasificación, etiquetado, uso apropiado y acceso a los activos de información de la entidad.	
	8.3	Manejo de medios				
	8.3.1	Gestión de medios removibles	SI		Definición, implementación, mantenimiento y mejora de procedimientos para la gestión de medios removibles	Comité de Sistemas y Seguridad de la Información Subdirección de Diseño y Análisis Estartégico
	8.3.2	Eliminación de medios	SI		Definición, implementación, mantenimiento y mejora de procedimientos para la gestión de medios removibles	
	8.3.3	Transporte de medios físicos	SI		Definición, implementación, mantenimiento y mejora de controles para el manejo de activos de información. Seguimiento custodia de medios.	
	9.1	Requerimientos de negocio para el control de acceso				
	9.1.1	Política de control de acceso	SI		Definición, implementación, mantenimiento y mejora de las políticas de seguridad y privacidad de la información aprobadas por la dirección. Socializar, sensibilizar y comunicar las políticas de seguridad y privacidad de la información a todas las partes interesadas	Comité de Sistemas y Seguridad de la Información Subdirección de Diseño y Análisis Estartégico
	9.1.2	Acceso a redes y servicios de red	SI		Definición, implementación, mantenimiento y mejora de procedimientos para otorgar acceso a los medios de procesamiento de información	Subdirección de Diseño y Análisis Estartégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	9.2	Gestión de accesos de usuario				
	9.2.1	Registro y cancelación del registro de usuarios	SI		Definición, implementación, mantenimiento y mejora de procedimientos y controles para la gestión y administración de usuarios de los sistemas y servicios informáticos: Otorgar acceso a los medios de procesamiento de información Monitoreo a los medios de procesamiento de información	Comité de Sistemas y Seguridad de la Información Subdirección de Diseño y Análisis Estartégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	9.2.2	Suministro de acceso de usuarios	SI			
	9.2.3	Gestión de derechos de acceso privilegiado	SI			
	9.2.4	Gestión de información de autenticación secreta de usuarios	SI			
	9.2.5	Revisión de los derechos de acceso de usuarios	SI			

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Comentarios (visión general de la implementación)	Responsables
Control de Acce	9.2.6	Retiro o ajuste de los derechos de acceso	SI		Información Gestión de usuarios	Recursos Tecnológicos
	9.3	Responsabilidades del usuario				
	9.3.1	Uso de información de autenticación secreta	SI		Definición, implementación, mantenimiento y mejora de procedimientos y controles para la gestión y administración de usuarios de los sistemas y servicios informáticos: Otorgar acceso a los medios de procesamiento de información Monitoreo a los medios de procesamiento de información Gestión de usuarios Uso de contraseñas Administración de la plataforma tecnológica	Comité de Sistemas y Seguridad de la Información Subdirección de Diseño y Análisis Estartégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	9.4	Control de acceso de sistemas y aplicaciones				
	9.4.1	Restricción de acceso a la información	SI		Definición, implementación, mantenimiento y mejora de procedimientos y controles para la gestión y administración de usuarios de los sistemas y servicios informáticos: Otorgar acceso a los medios de procesamiento de información Monitoreo a los medios de procesamiento de información Gestión de usuarios	Comité de Sistemas y Seguridad de la Información Subdirección de Diseño y Análisis Estartégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	9.4.2	Procedimientos de inicio de sesión seguro	SI			
	9.4.3	Sistema de gestión de contraseñas	SI			
	9.4.4	Uso de programas y utilidades privilegiadas	SI			
	9.4.5	Control de acceso al código fuente del programa	SI			
10 Criptografía	10.1	Controles criptográficos				
	10.1.1	Política en el uso de controles criptográficos	SI		Definición, implementación, mantenimiento y mejora de procedimientos y controles criptográficos	Comité de Sistemas y Seguridad de la Información Subdirección de Diseño y Análisis Estartégico Proceso de Gestión de
	10.1.2	Gestión de llaves	SI			
11 Seguridad Física y del Entorno	11.1	Áreas seguras				
	11.1.1	Perímetro de seguridad físico	SI		Definición, implementación, mantenimiento y mejora de procedimientos y controles de seguridad perimetral, acceso a áreas seguras, aseguramiento de medios de procesamiento de información, otorgar acceso a medios de procesamiento de información	Subdirección Administrativa y Financiera - Vigilancia - S&SO Terceras partes Dirección General - Contratacion
	11.1.2	Controles físicos de entrada	SI			
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	SI			
	11.1.4	Protección contra amenazas externas y del ambiente	SI			
	11.1.5	Trabajo en áreas seguras	SI			
	11.1.6	Áreas de entrega y carga	SI			
	11.2	Equipo				
	11.2.1	Instalación y protección de equipo	SI		Definición, implementación, mantenimiento y mejora de procedimientos y controles para soporte de equipos (protección de fallas eléctricas y otras disrupciones causadas por fallas en equipos de soporte). Seguridad del cableado (protección de interceptación, interferencia o daño del cableado de energía y telecomunicaciones que transporta datos o soporte los servicios de información). Mantenimiento de equipos que garantice disponibilidad e integridad continua Seguridad de equipos y activos fuera de su sitios	Subdirección Administrativa y Financiera Subdireccion de Diseño y Análisis Estratégico
	11.2.2	Servicios de soporte	SI			
	11.2.3	Seguridad en el cableado	SI			
	11.2.4	Mantenimiento de equipos	SI			
	11.2.5	Retiro de activos	SI			
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones	SI			
	11.2.7	Eliminación segura o reuso del equipo	SI			
	11.2.8	Equipo de usuario desatendido	SI			

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Comentarios (visión general de la implementación)	Responsables
	11.2.9	Política de escritorio limpio y pantalla limpia	SI		Definición, implementación, mantenimiento y mejora de las políticas de seguridad y privacidad de la información aprobadas por la dirección. Socializar, sensibilizar y comunicar las políticas de seguridad y privacidad de la información a todas las partes interesadas	Subdireccion de Diseño y Análisis Estratégico Comité de Sistemas y Segurida de la Información Sistema Integrado de Gestión
12 Seguridad de las Operaciones	12.1	Procedimientos Operacionales y Responsabilidades				
	12.1.1	Procedimientos de operación documentados	SI		Revisión, consolidación, actualización de la documentación relacionada con la plataforma tecnológica	Subdirección de Diseño y Análisis Estratégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	12.1.2	Gestión de cambios	SI			
	12.1.3	Gestión de la capacidad	SI		Roles y responsabilidades en la administración de la infraestructura tecnológica y de comunicaciones	
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	SI		Puesta en operación de ambientes controlados para pruebas, desarrollo, producción	
	12.2	Protección de Software Malicioso				
	12.2.1	Controles contra software malicioso	SI		Implementación, mantenimiento y mejora de controles de seguridad informática. Plataforma de Seguridad informática	Subdirección de Diseño y Análisis Estratégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	12.3	Respaldo				
	12.3.1	Respaldo de información	SI		Definición, implementación, mantenimiento y mejora de procedimientos y controles para el aseguramiento de la información institucional	Subdirección de Diseño y Análisis Estratégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	12.4	Bitácoras y monitoreo				
	12.4.1	Bitácoras de eventos	SI		Definición, implementación, mantenimiento y mejora de procedimientos y controles para consolidar registros de eventos	Subdirección de Diseño y Análisis Estratégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	12.4.2	Protección de información en bitácoras	SI			
	12.4.3	Bitácoras de administrador y operador	SI			
	12.4.4	Sincronización de relojes	SI			
	12.5	Control de software operacional				
	12.5.1	Instalación de software en sistemas operacionales			Definición, implementación, mantenimiento y mejora de procedimientos y controles para la instalación de software	Subdirección de Diseño y Análisis Estratégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	12.6	Gestión de vulnerabilidades técnicas				
	12.6.1	Gestión de vulnerabilidades técnicas	SI		Realización de pruebas de vulnerabilidad técnicas sobre la infraestructura de la entidad.	Subdirección de Diseño y Análisis Estratégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	12.6.2	Restricciones en la instalación de software	SI		Definición, implementación, mantenimiento y mejora de controles de restricción de instalación de software. (AD, PcSecure)	
	12.7	Consideraciones de auditoria de sistemas de información				
	12.7.1	Controles de auditoría de sistemas de información	SI			
	13.1	Gestión de seguridad en red				
	13.1.1	Controles de red	SI		Definición, implementación, mantenimiento y mejora	Subdirección de Diseño y

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Comentarios (visión general de la implementación)	Responsables
13 Seguridad en las Comunicaciones	13.1.2	Seguridad en los servicios en red	SI		de controles en las redes de datos de la entidad. Administarcion, configuración, respaldo de activos de infraestructura tecnológica, acuerdos de confidencialidad, proteccion de medios de	Análisis Estratégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	13.1.3	Segregación en redes	SI			
	13.2	Transferencia de información				
	13.2.1	Políticas y procedimientos para la transferencia de información	SI		Definición, implementación, mantenimiento y mejora de las políticas de seguridad y privacidad de la información aprobadas por la dirección. Socializar, sensibilizar y comunicar las políticas de seguridad y privacidad de la información a todas las partes interesadas	e Sistemas y Seguridad de la Infc
	13.2.2	Acuerdos en la transferencia de información	SI		de controles en las redes de datos de la entidad. Administarcion, configuración, respaldo de activos de infraestructura tecnológica, acuerdos de confidencialidad, proteccion de medios de procesamiento de información	Comité de Sistemas y Seguridad de la Información Subdirección Jurídica y de Contratación Subdirección Administrativa y Financiera
	13.2.3	Mensajería electrónica	SI			
	13.2.4	Acuerdos de confidencialidad o no-revelación	SI			
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14.1	Requerimientos de seguridad en sistemas de información				
	14.1.1	Análisis y especificación de requerimientos de	SI			Subdirección de Diseño y Análisis Estratégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	SI			
	14.1.3	Protección de transacciones en servicios de aplicación	SI			
	14.2	Seguridad en el proceso de desarrollo y soporte				
	14.2.1	Política de desarrollo seguro	SI		Definición, implementación, mantenimiento y mejora de las políticas de seguridad y privacidad de la información aprobadas por la dirección. Socializar, sensibilizar y comunicar las políticas de seguridad y privacidad de la información a todas las partes interesadas	Subdirección de Diseño y Análisis Estratégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	14.2.2	Procedimientos de control de cambios del sistema	SI		Definicion, implementación mantenimiento y mejora de procedimientos y controles para seguridad de la información en los nuevos sistemas o de cambios en los existentes, aseguramiento de la información asociada a servicios, aplicaciones, protección de transacciones en servicios de aplicaciones, desarrollo de software y sistemas, control de cambios, restricciones a cambios en software, aplicación de principios para la ingeniería de sistemas seguros, establecimiento y protección de ambientes seguros de desarrollo, pruebas y producción	
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	SI			
	14.2.4	Restricción de cambios en paquetes de software	SI			
	14.2.5	Principios de seguridad en la ingeniería de sistemas	SI			
	14.2.6	Entorno de desarrollo seguro	SI			
	14.2.7	Desarrollo tercerizado	SI			
	14.2.8	Pruebas de seguridad del sistema	SI			
	14.2.9	Pruebas de aceptación del sistema	SI			
	14.3	Datos de prueba				
	14.3.1	Protección de datos de prueba	SI		Definicion, implementación mantenimiento y mejora de procedimientos y controles para los datos de prueba	Subdirección de Diseño y Análisis Estratégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	15.1	Seguridad de la información en relaciones con el proveedor				

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Comentarios (visión general de la implementación)	Responsables
15 Relaciones con Proveedores	15.1.1	Política de seguridad de la información en las relaciones con el proveedor	SI		Definición, implementación, mantenimiento y mejora de las políticas de seguridad y privacidad de la información aprobadas por la dirección. Socializar, sensibilizar y comunicar las políticas de seguridad y privacidad de la información a todas las partes interesadas	Comité de Sistemas y Seguridad de la Información Todas las áreas
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	SI		Definicion, implementación mantenimiento y mejora de procedimientos y controles con terceras partes.	
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	SI			
	15.2	Gestión de entrega de servicios de proveedor				
	15.2.1	Monitoreo y revisión de servicios del proveedor	SI		Definicion, implementación mantenimiento y mejora de procedimientos y controles con terceras partes.	Comité de Sistemas y Seguridad de la Información
	15.2.2	Gestión de cambios a los servicios del proveedor	SI			
16 Gestión de Incidentes de Seguridad de la Información	16.1	Gestión de incidentes de seguridad de la información y mejoras				
	16.1.1	Responsabilidades y procedimientos	SI		Definicion, implementación mantenimiento y mejora de procedimientos y controles para: Gestion de Incidentes de seguridad de la informacion (identificación, reporte, tratamiento, lecciones aprendidas) Metodología para la gestión de riesgos de seguridad de la información (identificación, valoració, tratamiento) Contacto con grupos de interés (COLCERT, MINTIC; ACDTIC) Manejo de información	Comité de Sistemas y Seguridad de la Información Todas las áreas
	16.1.2	Reporte de eventos de seguridad de la información	SI			
	16.1.3	Reporte de debilidades de seguridad de la información	SI			
	16.1.4	Valoración y decisión de eventos de seguridad de la información	SI			
	16.1.5	Respuesta a incidentes de seguridad de la información	SI			
	16.1.6	Aprendizaje de incidentes de seguridad de la información	SI			
	16.1.7	Colección de evidencia	SI			
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17.1	Continuidad de la seguridad de la información				
	17.1.1	Planeación de la continuidad de la seguridad de la información	SI		Diseño, desarrollo, implementación y pruebas del Plan de Continuidad de Seguridad de la Información Definición y puesta en operación de un plan de recuperación ante desastres (DRP) y plan de continuidad de la operación informática	Comité de Sistemas y Seguridad de la Información Subdirección Administrativa y Financiera Subdirección de Diseño y Análisis Estratégico
	17.1.2	Implementación de la continuidad de la seguridad de la información	SI			
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI			
	17.2	Redundancias				
	17.2.1	Disponibilidad de instalaciones de procesamiento de información	SI		Definicion, implementación mantenimiento y mejora de controles para las instalaciones de procesamiento de información	Comité de Sistemas y Seguridad de la Información Subdirección Administrativa y Financiera Subdirección de Diseño y Análisis Estratégico Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos
	18.1	Cumplimiento con Requerimientos Legales y Contractuales				
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales	SI		Definición, implementación, mantenimiento y mejora de las políticas de seguridad y privacidad de la información aprobadas por la dirección. Socializar, sensibilizar y comunicar las políticas de seguridad y privacidad de la información a todas las partes interesadas	Comité de Sistemas y Seguridad de la Información
	18.1.2	Derechos de propiedad intelectual (IPR)	SI			
	18.1.3	Protección de registros	SI			

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Comentarios (visión general de la implementación)	Responsables
18 Cumplimiento	18.1.4	Privacidad y protección de información personal identificable (PIR)	SI		interesadas. Seguimiento al cumplimiento de la normatividad vigente Participación en iniciativas distritales y Nacionales,	Todas las áreas
	18.1.5	Regulación de controles criptográficos	SI			
	18.2	Revisiones de seguridad de la información				
	18.2.1	Revisión independiente de seguridad de la información	SI		Desarrollo de auditorias externas	Asesoría de Control Interno Entes Distritales y Nacionales
	18.2.2	Cumplimiento con políticas y estándares de seguridad	SI		Desarrollo de auditorias externas	
	18.2.3	Revisión del cumplimiento técnico	SI		Mantenimiento y mejora de controles, lineamientos, políticas, directrices relacionadas con la seguridad de la información. Verificaciones de acciones de mejora, seguimiento al plan de implementación de la gestión de seguridad y privacidad de la información	Comité de Sistemas y Seguridad de la Información Todas las áreas