ALCALDÍA MAYOR DE BOGOTÁ D.C.
SALUD
Subred Integrada de Servicios de Salud Sur E.S.E

SUBRED INTEGRADA DE SERVICIOS DE SALUD SUR E.S.E

DECLARACIÓN DE APLICABILIDAD (DDA) PARA SEGURIDAD DE LA INFORMACIÓN

La Alta Dirección de la Subred Sur se compromete a cumplir con el mantenimiento, sostenibilidad y aplicabilidad del Sistema de Gestión de la Información SGSI, junto con sus políticas, Normas y procedimientos definidos para proteger los activos de información de la Entidad y la tecnología utilizada para su procesamiento y uso, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información con base en la identificación, y valoración de riesgos de seguridad de la información, así como la formulación de actividades de tratamiento de riesgos, que cada líder operativo de proceso ha estimado convenientes, para mitigarlos y operar de forma segura y conforme los requisitos de los servicios ofrecidos por la entidad.

Asegurar la implementación de las medidas de seguridad establecidas en el Manual de la Política de Seguridad de la Información, identificando los recursos correspondientes, para mantener las Políticas de Seguridad de la Entidad actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

El Área de Control Interno, o en su defecto quien sea propuesto por la Alta Dirección es responsable de practicar auditorias periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por el Manual de la Política, sus normas, procedimientos y prácticas que de ella surjan.

Todos los colaboradores requieren entender que la violación a las políticas de seguridad de la información, normas y procedimientos tendrá una acción correctiva. Las acciones disciplinarias deben ser consistentes con la severidad del incidente.

Los controles aplicables para la operación del Sistema de Gestión de Seguridad de la Información, son los numerales que se relacionan a continuación en el "Detalle de la Declaración de Aplicabilidad", realizado con base en las recomendaciones de la norma NTC/ISO 27001:2013.

La presente declaración de aplicabilidad será revisada conjuntamente con los resultados de cada nuevo proceso de valoración de riesgos y/o ante cambios significativos de los elementos de la plataforma tecnológica y/o de personal. Esta información, será material de comparación en los procesos de revisión por la dirección del SGSI, en los periodos convenidos para su actualización.

No.	OBJETIVO CONTROL	ID CONTROL	CONTROL	APLICADO?	JUSTIFICACION
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACION					
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes					
1	**A5.1** Orientación de la dirección para la gestión de la seguridad de la información	**A5.1.1** Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Si	La Subred Sur ha identificado los riesgos de información, en tal sentido es necesario establecer una política de seguridad de la información para informar y concientizar a todos los colaboradores interesados sobre los riesgos que están expuestos, así como implementados para evitar la materialización de estos riesgos. Igualmente la política de Seguridad de la Información deberá definir claramente responsables de su desarrollo e implementación. El manual de la política de seguridad de la información de la Subred Sur deberá ser frecuentemente revisado para asegurar su idoneidad con respecto a los riesgos de información. Está política debe ser comunicada a todas las partes interesadas.
2		**A5.1.2** Revisión de las políticas para la seguridad de la información.	Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	Si	
A6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION					
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización					
3	**A6.1** Organización interna	**A6.1.1** Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Si	La Subred Sur mediante sus Política de Seguridad de la Información debe establecer el compromiso, organización y asignación de responsabilidades para su cumplimiento, de igual forma velar por mantener protegida su información mediante la revisión del Sistema de Gestión de Seguridad de la Información, la firma de los Acuerdos de Confidencialidad, manteniendo contacto con las Autoridades y con grupos de interés especiales y la revisión independiente de seguridad de la información, por lo anterior es importante establecer controles para la Entidad interna de seguridad de la información.
4		**A6.1.2** Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	Si	
5		**A6.1.3** Contacto con las autoridades	Se deben mantener contactos apropiados con las autoridades pertinentes.	Si	
6		**A6.1.4** Contacto con grupos de interés especial	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	Si	
7		**A61.1.5** Seguridad de la información en la gestión de proyectos.	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	Si	

No.	OBJETIVO CONTROL	ID CONTROL	CONTROL	APLICADO?	JUSTIFICACION
8	A6.2 Dispositivos móviles y teletrabajo	A6.2.1 Política para dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Si	La Subred Sur restringe la conexión a redes inalámbricas de internet por parte de los dispositivos móviles y equipos de terceros
9		A6.2.2 Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	No Aplica	
	A.7 SEGURIDAD DE LOS RECURSOS HUMANOS				
	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran				
10	A7.1 Antes de asumir el empleo	A7.1.1 Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	Si	Para el desarrollo de sus procesos la Subred Sur requiere contratar personal, los cuales tienen acceso a la información de la Entidad, por tanto es importante implementar controles basándose en el manual de funciones y/o manual de contratación, la ética y las leyes pertinentes, que aseguren un proceso de verificación de antecedentes, asignación de roles y responsabilidades, términos de contratación y condiciones laborales previo acceso a la información.
11		A7.1.2 Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Si	
12	A7.2 Durante la ejecución del empleo	A7.2.1 Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Si	El personal de la Subred Sur en el desarrollo de las funciones y/o actividades para las cuales fueron contratados interactúan permanentemente con la información, en tal sentido es necesario establecer controles para asegurar que son conscientes de los riesgos, responsabilidades y deberes con respecto a la seguridad de la información, igualmente es necesario concientizar al personal permanentemente en temas de seguridad de la información según sea pertinente para sus funciones y/o actividades.
13		A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	Si	
14		A7.2.3 Proceso disciplinario	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	En Construcción	También se hace preciso establecer un proceso disciplinario que permita a la Subred Sur saber cómo actuar en caso de que los colaboradores cometan alguna violación de la seguridad, sin embargo para evitar el máximo que se presente incidentes la Dirección exigirá a los colaboradores el cumplimiento de las políticas, normas y procedimientos establecidos.
15	A7.3 Terminación y cambio de empleo	A7.3.1 Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	Si	La Subred Sur desarrolla procesos los cuales tienen un inicio y un fin, por esta razón es necesario establecer controles que permitan asegurar la devolución de los activos de la Entidad y el retiro o cambio de los derechos de acceso cuando se presentan renuncias, terminaciones o cambios de la contratación que conforman los diferentes procesos o áreas transversales de la Entidad.
	A8 GESTION DE ACTIVOS				
	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.				
16	A8.1 Responsabilidad por los activos	A8.1.1 Inventario de activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Si	La Subred Sur dentro del proceso de implementación y mantenimiento del Sistema de Seguridad de la Información debe realizar un inventario de todos los Activos de Información, los cuales le permiten desarrollar sus labores, en tal sentido es importante identificar los propietarios de estos, realizar un inventario de los más importantes, y también garantizar el uso adecuado de los mismos a través de reglas y normas documentadas e implementadas.
17		A8.1.2 Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	Si	
18		A8.1.3 Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Si	

No.	OBJETIVO CONTROL	ID CONTROL	CONTROL	APLICADO?	JUSTIFICACION
19		**A8.1.4** Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Si	Los activos de la Subred Sur deberán ser regresados por los colaboradores al finalizar su relación contractual. La Entidad debe asegurar la devolución de los Activos cuando se presenten renuncias, terminaciones o cambios de la contratación del personal que conforman los diferentes procesos y/o áreas transversales de la Entidad.
20	**A8.2** Clasificación de la información	**A8.2.1** Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Si	La Subred Sur en sus procesos tiene información de diferentes tipos, la cual tiene diferentes niveles de importancia y protección, por ejemplo la información de sus pacientes no tiene la misma protección que la información financiera, por lo anterior se deben implementar controles y procedimientos que permitan dar a la información el nivel adecuado de protección, etiquetado y manejo con base en la clasificación de información que se utilice, tomando en cuenta su valor, los requisitos legales, la sensibilidad y la importancia para la Entidad.
21		**A8.2.2** Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Si	
22		**A8.2.3** Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	En Construcción	
23	**A8.3** Manejo de medios	**A8.3.1** Gestión de medio removibles	Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Si	Para el desarrollo de las actividades se utilizan medios para el intercambio de información, tales como correo electrónico institucional, USB, CD, entre otros por lo anterior es necesario establecer controles para asegurar la que se eviten eventos como divulgación, modificación, retiro o destrucción de información no autorizada.
24		**A8.3.2** Disposición de los medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	Si	
25		**A8.3.3** Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Si	
	A9 CONTROL DE ACCESO				
	Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.				
26	**A9.1** Requisitos del negocio para el control de acceso	**A9.1.1** Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Si	La Subred Sur desarrolla actividades dentro de las cuales los activos de información son manejados por los colaboradores, en tal sentido es importante establecer controles de seguridad que permitan asegurar que los propietarios de activos de información controlan el acceso a la información.
27		**A9.1.2** Acceso a redes y a servicios en red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Si	La Subred Sur para su operación cuenta con cinco (5) redes LAN las cuales soportan las actividades de los diferentes usuarios, por lo tanto es necesario establecer controles de seguridad para asegurar que los usuarios solo tienen acceso a los servicios para los cuales están autorizados.
28	**A9.2** Gestión de acceso de usuarios	**A9.2.1** Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Si	El personal de la Subred Sur maneja diferentes tipos de información de acuerdo al área o proceso en el cual participan, por esta razón es muy importante gestionar de forma adecuada el acceso de los usuarios de acuerdo al área o proyecto. En tal sentido es importante establecer controles de seguridad aseguren el acceso de usuarios autorizados así como evitar el acceso de usuarios no autorizados a información fuera de su área o proyecto.
29		**A9.2.2** Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Si	
30		**A9.2.3** Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Si	
31		**A9.2.4** Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Si	
32		**A9.2.5** Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Si	
33		**A9.2.6** Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Si	

No.	OBJETIVO CONTROL	ID CONTROL	CONTROL	APLICADO?	JUSTIFICACION
34	**A9.3** Responsabilidades de los usuarios	**A9.3.1** Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Si	
35		**A9.4.1** Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Si	
36	**A9.4** Control de acceso a sistemas y aplicaciones	**A9.4.2** Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Si	El personal de la Subred Sur maneja para acceder a los servicios de red un usuario único e intransferible al cual se le asignan las respectivas credenciales, las cuales se deben actualizar cada Treinta (30) días. Lo anterior aplica para los usuarios ubicados en todas las Sedes de la Entidad.
37		**A9.4.3** Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Si	
38		**A9.4.4** Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Si	
39		**A9.4.5** Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	Si	
	A10 CRIPTOGRAFIA				
	Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información				
40	**A10.1** Controles criptográficos	**A10.1.1** Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	En Construcción	La Subred Sur para los sistemas de información que se manejan en los diferentes procesos debe establecer controles criptográficos con el objetivo de garantizar la confidencialidad e integridad de la información.
41		**A10.1.2** Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	En Construcción	
	A11 SEGURIDAD FISICA Y DEL ENTORNO				
	Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización				
42	**A11.1** Áreas seguras	**A11.1.1** Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	Si	La Subred Sur para el desarrollo de sus actividades cuenta con una infraestructura física, ubicada en la localidad Diecinueve de Ciudad Bolívar, en la cual se ubican los activos de información, en tal sentido es importante establecer los controles de seguridad para evitar el acceso físico no autorizado, el daño a la infraestructura y activos de información de la Entidad.
43		**A11.1.2** Controles de acceso físicos	Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Si	
44		**A11.1.3** Seguridad de oficinas, recintos e instalaciones.	Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones..	Si	
45		**A11.1.4** Protección contra amenazas externas y ambientales.	Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Si	
46		**A11.1.5** Trabajo en áreas seguras.	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Si	
47		**A11.1.6** Áreas de carga, despacho y acceso público	Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Si	La infraestructura física que la Subred Sur utiliza para el desarrollo de algunas de sus actividades cuenta con áreas de carga o despacho, las sedes comprometidas no cuentan con una sola entrada principal; por tal razón se hace necesario establecer controles de seguridad para proteger las áreas de despacho o carga.
48		**A11.2.1** Ubicación y protección de los equipos	Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Si	Para el desarrollo de las actividades la Subred Sur utiliza equipos tales como servidores, computadores de escritorio, portátiles, impresoras, fotocopiadoras, faxes,
49		**A11.2.2** Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Si	
50		**A11.2.3** Seguridad en el cableado.	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Si	

No.	OBJETIVO CONTROL	ID CONTROL	CONTROL	APLICADO?	JUSTIFICACION
51	A11.2 Equipos	A11.2.4 Mantenimiento de los equipos.	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Si	escáneres, entre otros, en estos equipos se procesa la información de las diferentes áreas y/o procesos de la Entidad por tal razón es necesario establecer controles que permitan evitar la ocurrencia de eventos como pérdida, daño, robo o interrupción de los equipos tanto dentro como fuera de la Entidad.
52		A11.2.5 Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa	Si	
53		A11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	Si	
54		A11.2.7 Disposición segura o reutilización de equipos	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso.	Si	
55		A11.2.8 Equipos de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Si	El personal de la Subred Sur es responsable de los activos de información que se encuentran a su cargo, así como de la protección de estos activos en cuanto confidencialidad, integridad y disponibilidad, de tal forma que se han definido responsabilidades claras en cuanto a seguridad de la información tanto en los manuales de funciones que son entregados a los funcionarios como en las obligaciones contractuales, en tal sentido es necesario establecer controles de seguridad para asegurar que se evita el acceso de usuarios no autorizados y el robo de información.
56		A11.2.9 Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	En Construcción	
	A12 SEGURIDAD DE LAS OPERACIONES				
	Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
57	A12.1 Procedimientos operacionales y responsabilidades	A12.1.1 Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	Si	La Subred Sur para el desarrollo de sus actividades utiliza herramientas ofimáticas y tecnológicas, con las cuales interactúan permanentemente el personal a través de los equipos asignados para su labor, en tal sentido es necesario establecer controles de seguridad que garanticen que todos los cambios se controlan, revisan y someten a pruebas para no comprometer la seguridad del sistema ni el entorno operativo y también evitar así la fuga de información.
58		A12.1.2 Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Si	
59		A12.1.3 Gestión de capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	Si	
60		A12.1.4 Separación de los ambientes de desarrollo, pruebas y operación	Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Si	La Subred Sur realiza antes de la instalación de software pruebas en ambientes diferentes a los de producción con el fin de reducir los riesgos de acceso y cambios no autorizados.
61	A12.2 Protección contra códigos maliciosos	A12.2.1 Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Si	Para el desarrollo de las actividades la Subred Sur se utilizan servicios como Internet, medios extraíbles, los cuales pueden afectar el correcto funcionamiento de activos de información como equipos, software entre otros, por lo tanto es importante establecer controles de seguridad que permitan detección y prevención de la acción de códigos maliciosos así como también procedimientos de concientización de los usuarios.
62	A12.3 Copias de respaldo	A12.3.1 Respaldo de la información	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Si	La información de la Subred Sur y de los diferentes procesos se encuentra ubicada en los equipos asignados a los colaboradores así como en los servidores, en tal sentido es importante establecer controles de seguridad que aseguren la ejecución de procedimientos de backup y recuperación que permitan restaurar en el menor tiempo la información ante la materialización de un riesgo, y así permitir que la entidad continué con sus actividades habituales sin ningún inconveniente.
63		A12.4.1 Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Si	

No.	OBJETIVO CONTROL	ID CONTROL	CONTROL	APLICADO?	JUSTIFICACION
64	A12.4 Registro y seguimiento	A12.4.2 Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Si	La Subred Sur para el desarrollo de sus actividades cuenta con colaboradores que tienen acceso a los diferentes activos de información para la ejecución de sus actividades, en tal sentido es importante establecer controles de seguridad que permitan la detección oportuna de actividades de procesamiento de información no autorizadas y herramientas para investigaciones futuras de incidentes de seguridad de la información.
65		A12.4.3 Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	Si	
66		A12.4.4 Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Si	
67	A12.5 Control de software operacional	A12.5.1 Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Si	La Subred Sur para el desarrollo de sus actividades utiliza diferentes sistemas operativos tales como, WINDOWS SERVER 2008 y 2012, WINDOWS 7, 8 y 10, LINUX, en tal sentido es importante establecer controles de seguridad para garantizar la protección, control y correcta operación de los sistemas operativos. De igual forma para los equipos asignados a los Usuarios se restringe la posibilidad de instalación de programas y/o aplicativos.
68	A12.6 Gestión de la vulnerabilidad técnica	A12.6.1 Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Si	La Subred Sur tiene activos de información tecnológicos los cuales están expuestos a vulnerabilidades de tipo técnico, por lo tanto es necesario establecer controles de seguridad para garantizar la reducción de los riesgos derivados de las vulnerabilidades técnicas.
69		A12.6.2 Restricciones sobre la instalación de software	Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Si	La Subred Sur para el desarrollo de sus actividades utiliza diferentes sistemas operativos tales como, WINDOWS SERVER 2008 y 2012, WINDOWS 7, 8 y 10, LINUX, en tal sentido es importante establecer controles de seguridad para garantizar la protección, control y correcta operación de los sistemas operativos. De igual forma para los equipos asignados a los Usuarios se restringe la posibilidad de instalación de programas y/o aplicativos.
70	A12.7 Consideraciones sobre auditorias de sistemas de información	A12.7.1 Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Si	La Subred Sur cuenta con sistemas operativos que pueden ser objeto de auditoria de seguridad de la información, por lo tanto es importante establecer controles de seguridad que garanticen un adecuado uso de las herramientas de auditoria y minimizar la interrupción de los sistemas durante el proceso.
	A13 SEGURIDAD DE LAS COMUNICACIONES				
	Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
71	A13.1 Gestión de la seguridad de las redes	A13.1.1 Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Si	La Subred Sur para el desarrollo de sus actividades cuenta con Cinco (5) redes LAN sobre las cuales se controlan todas las aplicaciones ejecutadas por los usuarios, por lo anterior es importante establecer controles de seguridad para asegurar la información en la red, protegerla de amenazas y garantizar su infraestructura de soporte.
72		A13.1.2 Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Si	
73		A13.1.3 Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	No Aplica	La Subred Sur no considera necesario este control para la protección de su información.
74	A13.2 Transferencia de información	A13.2.1 Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Si	Dentro del desarrollo normal de las actividades de la Subred Sur se presentan actividades de intercambio de información con clientes, colaboradores, entre otros como parte del desarrollo de los proyectos, por lo cual es importante establecer controles de seguridad para asegurar que se cumplen las políticas y procedimientos de la empresa para el intercambio de información y para garantizar que no se presente uso inadecuado o corrupción cuando la información sale fuera de las instalaciones de la Entidad.
75		A13.2.2 Acuerdos sobre transferencia de información	Los acuerdos sobre transferencia segura de información del negocio entre la organización y las partes externas.	Si	
76		A13.2.3 Mensajería Electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Si	

No.	OBJETIVO CONTROL	ID CONTROL	CONTROL	APLICADO?	JUSTIFICACION
77		**A13.2.4** Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	Si	La Subred Sur mediante su política de seguridad de la información establece su compromiso, organización y asignación de responsabilidades para su cumplimiento, de igual forma vela por mantener protegido sus activos de información mediante la revisión del sistema de gestión de seguridad de la información, la firma de los acuerdos de confidencialidad, manteniendo contacto con las autoridades y con grupos de interés especiales, y la revisión independiente de seguridad de la información, por lo anterior es importante establecer controles para La Subred Sur interna de seguridad de la información.
A14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.					
78	**A14.1** Requisitos de seguridad de los sistemas de información	**A.14.1.1** Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Si	La Subred Sur desarrolla actividades para las cuales utiliza herramientas ofimáticas y tecnológicas, en tal sentido es necesario establecer controles de seguridad para garantizar que tienen en cuenta los requisitos del negocio antes de implementar cambios en la tecnología de la empresa.
79		**A.14.1.2** Seguridad de servicios de las aplicaciones en redes públicas	La informacion involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Si	
80		**A.14.1.3** Protección de transaccciones de los servicios de las aplicaciones.	La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	En Construcción	La Subred Sur desarrolla actividades a través de diferentes aplicaciones por lo cual es necesario aplicar los controles de seguridad tales como llaves o encriptación para los sistemas de información de los proyectos.
81	**A14.2** Seguridad en los procesos de Desarrollo y de Soporte	**A.14.2.1** Política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	Si	La Subred Sur para el desarrollo de sus actividades utiliza herramientas ofimáticas y tecnológicas, con las cuales interactúan permanentemente el personal a través de los equipos asignados para su labor, en tal sentido es necesario establecer controles de seguridad que garanticen que todos los cambios se controlan, revisan y someten a pruebas para no comprometer la seguridad del sistema ni el entorno operativo y también evitar así la fuga de información.
82		**A.14.2.2** Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	Si	La Subred Sur para el desarrollo de sus actividades utiliza herramientas ofimáticas y tecnológicas, con las cuales interactúan permanentemente el personal a través de los equipos asignados para su labor, en tal sentido es necesario establecer controles de seguridad que garanticen que todos los cambios se controlan, revisan y someten a pruebas para no comprometer la seguridad del sistema ni el entorno operativo y también evitar así la fuga de información.
83		**A.14.2.3** Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	Si	
84		**A.14.2.4** Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	Si	
85		**A.14.2.5** Principio de Construcción de los Sistemas Seguros.	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	Si	La Subred Sur a través de la política de desarrollo de terceros establece y exige los lineamientos y buenas prácticas para el desarrollo y construcción de sistemas de información seguros.
86		**A.14.2.6** Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	No Aplica	La Subred Sur no considera necesario este control para la protección de su información.
87		**A.14.2.7** Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Si	La Subred Sur requiere para algunas de las actividades el desarrollo de software contratado externamente, por lo tanto se deben establecer controles de seguridad para proteger el acceso al código fuente de los sistemas de información, para evitar su alteración o uso malintencionado.

No.	OBJETIVO CONTROL	ID CONTROL	CONTROL	APLICADO?	JUSTIFICACION
88		**A.14.2.8** Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	Si	La Subred Sur no considera necesario este control para la protección de su información.
89		**A.14.2.9** Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Si	La Subred Sur válida los nuevos sistemas de información en un servidor de prueba antes de ser puestos a producción. Además está establecido en la política de desarrollo por terceros los criterios y pruebas de aceptación para los nuevos sistemas de información que adquiera la Entidad.
90	**A14.3** Datos de prueba	**A.14.3.1** Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Si	La Subred Sur realiza pruebas a los sistemas de información con datos no válidos. Además está establecido en la política de desarrollo por terceros los criterios y pruebas de aceptación para los nuevos sistemas de información que adquiera la Entidad.
	A15 RELACIONES CON LOS PROVEEDORES				
	Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.				
91	**A15.1** Seguridad de la información en las relaciones con los proveedores.	**A15.1.1** Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	Si	La Subred Sur desarrolla actividades para las cuales requiere realizar diferentes tipos de compras, en tal sentido es necesario establecer controles de seguridad para garantizar que tienen en cuenta los requisitos del negocio antes de gestionar compras de bienes o servicios que afecten la seguridad de la información de La Subred Sur y la infraestructura que sobre la cual esta soportada
92		**A15.1.2** Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	Si	
93		**A15.1.3** Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Si	La Subred Sur requiere para algunos de sus proyectos el desarrollo de sistemas de información, por lo cual al momento de contratarlos exige el cumplimiento de las buenas prácticas y cumplimiento de las políticas de La Subred Sur para su desarrollo.
94	**A15.2** Gestión de la prestación de servicios de proveedores	**A15.2.1** Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Si	La Subred Sur desarrolla actividades para las cuales requiere realizar diferentes tipos de compras, en tal sentido es necesario establecer controles de seguridad para garantizar que tienen en cuenta los requisitos del negocio antes de gestionar compras que de bienes o servicios que afecten la seguridad de la información e La Subred Sur y la infraestructura que sobre la cual esta soportada.
95		**A15.2.2** Gestión del cambio en los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la rrevaluación de los riesgos.	Si	
	A16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION				
	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
96		**A16.1.1** Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Si	La Subred Sur mediante su política de seguridad de la información establece su compromiso, organización y asignación de responsabilidades para su cumplimiento, de igual forma vela por mantener protegido sus activos de información mediante la revisión del sistema de gestión de seguridad de la información, la firma de los acuerdos de confidencialidad, manteniendo contacto con las autoridades y con grupos de interés especiales, y la revisión independiente de seguridad de la información, por lo anterior es importante establecer controles para La Subred Sur interna de seguridad de la información.
97		**A16.1.2** Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	Si	La Subred Sur tiene activos de información a los que se les ha realizado su respectivo

No.	OBJETIVO CONTROL	ID CONTROL	CONTROL	APLICADO?	JUSTIFICACION
98	A16.1 Gestión de incidentes y mejoras en la seguridad de la información	A16.1.3 Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Si	análisis, evaluación y tratamiento del riesgo, los cuales pueden ser objeto de incidentes de seguridad de la información, por lo cual es importante establecer controles que aseguren que los eventos y debilidades de seguridad de la información son comunicados oportunamente a través de los canales de gestión apropiados al área de seguridad de la información para su respectiva gestión tan pronto como sea posible.
99		A16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	Si	
100		A16.1.5 Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Si	
101		A16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	Si	La Subred Sur tiene XX grupos de activos de información los cuales pueden ser objeto de incidentes de seguridad de la información y deben ser analizados por el personal designado por la gerencia para identificar acciones de mejora, en tal sentido es necesario establecer controles de seguridad para garantizar un manejo eficaz y consistente de los incidentes de seguridad de la información.
102		A16.1.7 Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Si	
A17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO					
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.					
103	A17.1 Continuidad de Seguridad de la información	A17.1.1 Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Si	La Subred Sur como empresa está comprometida con sus clientes a través de los contratos a garantizar el cumplimiento total del objeto de estos, en tal sentido ante cualquier interrupción en las actividades del negocio por fallas tecnológicas importantes o desastres, la empresa debe contar una gestión de continuidad del negocio que permita minimizar el impacto generado en su capacidad de ejecución de los proyectos, por lo anterior es necesario establecer controles para asegurar una adecuada gestión de continuidad del negocio.
104		A17.1.2 Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Si	
105		A17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Si	
106	A17.2 Redundancias	A17.2 Redundancias	Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Si	La Subred Sur cuenta con equipos de respaldo para aquellos servicios críticos, como firewall e internet, entre otros para garantizar la disponibilidad de las instalaciones de procesamiento de información.
A18 CUMPLIMIENTO					
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.					
107	A18.1 Cumplimiento de requisitos legales y contractuales	A18.1.1 Identificación de la legislación aplicable.	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Si	La Subred Sur desarrolla sus actividades en el marco del cumplimiento de la legislación Colombiana, los requisitos contractuales y los propios, en tal sentido es importante establecer controles de seguridad que garanticen el cumplimiento de todos los requisitos legales, contractuales y propios.
108		A18.1.2 Derechos propiedad intelectual (DPI)	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Si	
109		A18.1.3 Protección de registros	Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Si	

No.	OBJETIVO CONTROL	ID CONTROL	CONTROL	APLICADO?	JUSTIFICACION
110		**A18.1.4** Privacidad y protección de información de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	Si	
111		**A18.1.5** Reglamentación de controles criptográficos.	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	Si	La Subred Sur para los sistemas de información que se manejan en los diferentes procesos debe establecer controles criptográficos con el objetivo de garantizar la confidencialidad e integridad de la información.
112	**A18.2** Revisiones de seguridad de la información	**A18.2.1** Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	Si	La Subred Sur mediante su política de seguridad de la información establece su compromiso, organización y asignación de responsabilidades para su cumplimiento, de igual forma vela por mantener protegido sus activos de información mediante la revisión del sistema de gestión de seguridad de la información, la firma de los acuerdos de confidencialidad, manteniendo contacto con las autoridades y con grupos de interés especiales, y la revisión independiente de seguridad de la información, por lo anterior es importante establecer controles para La Subred Sur interna de seguridad de la información.
113		**A18.2.2** Cumplimiento con las políticas y normas de seguridad	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	Si	El personal de la Subred Sur interactúa permanentemente con los activos de información para los cuales se han diseñado políticas y controles en materia de seguridad de la información, en tal sentido es importante establecer controles de seguridad que garanticen que todo el personal de la empresa conoce y aplica las políticas de seguridad de la información y los respectivos controles.
114		**A18.2.3** Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Si	

Total controles implementados	105	92,11%
Total controles en construcción	6	5,26%
Total controles que No Aplican	3	2,63%
Total controles sin implementar	0	0,00%

JHON ALEXANDER CEPEDA ZAFRA
Jefe Oficina sistemas de información TICS