	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GTI-P01-F-20
	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	VERSIÓN:	1
	DECLARACION DE APLICABILIDAD	VIGENCIA:	18-12-2020
		Página 1 de 1	

SECCION ANEXO A ISO 27001:2013
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.

Objetivo: Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
5.1.1	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.	Política general de seguridad de la información Resolución 0238 de 2020.	Implementado			X	
5.1.2	Revisión de las Política de Seguridad de la Información.	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	Actualización anual de Política registrada en el PSPI.	Implementado			X	

Justificación de exclusión
Comentarios/ Observaciones / Descripción General del Control
5.1.1 Política general de seguridad de la información en actualizacion en 2023 para alinearla a la ISO27001:2022

SECCION ANEXO A ISO 27001:2013
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A.6.1. Organización Interna

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.6.1.1	Seguridad de la Información Roles y Responsabilidades.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	El INC define la asignación de roles y responsabilidades a través de las siguientes acciones: *. Política de seguridad de la información * Comité de seguridad de la información. (MIPG) *. Revisión anual de Definición de roles de Seguridad en el PSPI. *Construccion de Matrices de roles y perfiles de SAP, Incompra y AD	Implementado			X	

A.6.1.2	Separación de deberes.	Las tareas 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.	Las áreas y los deberes en la entidad se encuentran definidas por dependencias y procesos, estas dependencias y procesos se encuentran publicados en la intranet en el Sistema integrado de Gestión de la institución. Resolución No.0584 del 26 de septiembre de 2019	Implementado			X	
A.6.1.3	Contacto con las autoridades.	Se debe mantener contactos apropiados con las autoridades pertinentes.	Al ser una entidad del estado se interactúa y cuenta con el apoyo de entidades estatales relacionadas con las definiciones e implementaciones de seguridad de la información, protección de datos, privacidad, ciberseguridad e infraestructuras críticas como como lo son: *CSIRT Gobiermo * Mintic *. CCIRT Policía Nacional *. Ministerio de Defensa - CCOC (Comando Conjunto Cibernético) *. Colcert (Grupo de Respuestas a emergencias cibernéticas de Colombia). *Grupo de ciberseguridad de Minsalud	Implementado			X	
A.6.1.4	Contacto con grupos de interés especial.	Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	Participacion en reuniones de Infraestructura Crítica y Riesgo Operativo organizado por el CCOCI, donde existe participación activa del sector privado y público de Colombia.	Implementado			X	
A.6.1.5	Seguridad de la información en Gestión de Proyectos.	La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto	De acuerdo a la política de seguridad, las propuestas de buenas prácticas a implementar deben atender los requisitos establecidos en la Norma Técnica ISO/IEC 27001 y el Manual de Gobierno en Línea vigente. Requerimientos generales de seguridad de la información estandarizados y revisados en contratos, independiente del tipo de proyecto a contratar.	Implementado	X			

Justificación de exclusión
Comentarios/ Observaciones / Descripción General del Control

A.6.2. Dispositivos Móviles y Teletrabajo.

Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

A.6.2.1	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..	Los dispositivos móviles de propiedad personal deben cumplir con la política BYOT incluida en la política de seguridad de la información, relacionada en el numeral “A.8.1.3. Uso aceptable de los activos.	Implementado			X	
A.6.2.2	Trabajo Remoto.	Se deben implementar una política y 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 trabajo remoto	Incluida en las políticas específicas de seguridad de la información, en su sección A.6.2.2 Trabajo remoto y en casa. Firma de GTI-P01-F-18 Acuerdo de Confidencialidad para trabajo en casa Acceso Vía VPN corporativa para trabajo remoto Controles relacionados en el Manual de normas y políticas de Seguridad GTE-P04-M-03	Implementado	X			

Justificación de exclusión
Comentarios/ Observaciones / Descripción General del Control

SECCION ANEXO A ISO 27001:2013
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS

A.7.1. Antes de asumir el empleo.

Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos 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.	Se cuenta con las siguientes validaciones: Funcionarios de Planta: La selección de personal se basa en la Ley 909 de 2004, se realiza verificación de antecedentes disciplinarios, de responsabilidad fiscales y de Policía. Para Contratistas: Se valida perfil, se solicita requisitos que permiten validar la experiencia y antecedentes fiscales, judiciales, disciplinarios, por medio de las empresas de selección de personal Revision de Sarlaf por medio de aplicativo por parte del area de planeacion. Plan de anticorrupcion (Planeacion)	Implementado	X			
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.	Los aspectos específicos de seguridad de la información se indican: Personas de Planta: Los servidores públicos se deben acoger a las políticas de seguridad de la información establecidas por la entidad. Contratistas: Obligación contractual en cada contrato de cumplimiento de políticas de seguridad de la información y tratamiento de datos personales	Implementado		X		

Justificación de exclusión

Comentarios/ Observaciones / Descripción General del Control

A.7.2. Durante la ejecución del empleo

Objetivo: Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.7.2.1	Responsabilidades de la Dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	Los aspectos específicos de seguridad de la información seindican: Personas de Planta: Los servidores públicos se deben acoger a las políticas de seguridad de la información establecidas por la entidad. El incumplimiento de las políticas de seguridad de la información conlleva a un proceso disciplinario y a sanciones de acuerdo con lo plasmado en la cartilla de deberes y derechos de los servidores públicos. Contratistas: Obligación contractual en cada contrato de cumplimiento de políticas de seguridad de la información y tratamiento de datos personales Sensibilizacion de sanciones al personal por control interno	Implementado		X		
A.7.2.2	Toma de conciencia, educación y formación de la Seguridad de la Información.	Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	Ejecución Plan de Sensibilización y capacitación en seguridad de la información Curso de seguridad de la información en Campus Virtual para inducción y reinducción de personal	Implementado			X	
A.7.2.3	Proceso disciplinario.	Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Se cuenta con procesos de Oficina de control interno disciplinario Procesos disciplinarios y sanciones relacionadas con seguridad de la información informados en política de seguridad y privacidad	Implementado	X			

Justificación de exclusión

Comentarios/ Observaciones / Descripción General del Control

A.7.3. Terminación y cambio de empleo.

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER

A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir..	Firma de acuerdos de confidencialidad, los cuales serán vigentes incluso después de la terminación laboral. Cláusula de responsabilidad en contratos (clausula decimoprimera)	Implementado		X		

Justificación de exclusión
Comentarios/ Observaciones / Descripción General del Control

SECCION ANEXO A ISO 27001:2013
A.8 GESTIÓN DE ACTIVOS.

A.8.1. Responsabilidad por los Activos.

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.8.1.1	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.	Documento de Inventario de activos de información publicado en www.datosabiertos.gov.co y Pagina Web con actualización anual	Implementado			X	
A.8.1.2	Propiedad de los activos.	Los activos mantenidos en el inventario deben ser propios.	Identificación del responsable incluido en Inventario de activos de información publicado en www.datosabiertos.gov.co y pagina web con actualización anual	Implementado			X	
A.8.1.3	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.	Se encuentra incluida en las Políticas específicas de seguridad de la información en su numeral A.8.1.3 Uso aceptable de los activos de información	Implementado			X	
A.8.1.4	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.	Para funcionarios de Planta: Como consecuencia del retiro se debe hacer entrega de los inventarios al jefe inmediato o a quien este designe y en la Subdirección de Gestión del Talento Humano el carné, la tarjeta de acceso, la declaración de Bienes y Rentas y practicarse el examen médico ocupacional de retiro. Para los contratistas: Los supervisores deben validar y verificar el recibo a satisfacción de lo relacionado en los contratos, incluyendo la devolución de activos; para ello se diligencia o verifica la siguiente documentación: -Informes de supervisión o interventoría Final -Solicitud de Liquidación de Contratos, Convenios y/o cualquier otro tipo de negocio jurídico de naturaleza contractual -Formato Pago Final -Matriz de Cumplimiento -Certificación de Pagos -Solicitud apertura procesos de incumplimiento sancionatorio. -Entrega de Equipos e información	En Proceso / Mejoramiento		X		

Justificación de exclusión

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GTI-P01-F-20
	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	VERSIÓN:	1
	DECLARACION DE APLICABILIDAD	VIGENCIA:	18-12-2020
		Página 1 de 1	

Comentarios/ Observaciones / Descripción General del Control
A.7.3.1 En 2023 se encuenra en proceso de automatizacion control de ingreso , retiro y novedades de personal con herramieta de BPM

A.8.2. Clasificación de la Información.

Objetivo: Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.8.2.1	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.	Tablas de Retención Documental, definidos por cada dependencia del INC e Implementados por el Grupo Area de Gestión Documental y Correspondencia Inventario de Activos de Información liderado por Oficial de Segruidad de la Informacion, y apoyado Grupo área gestión documental.	Implementado	X			
A.8.2.2	Etiquetado de la Información.	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización	Políticas y Procedimientos que pertenecen al Proceso de Gestión Documental: Resolución 0305 de 2020 Política de Gestión Documental Citerios definidos de Etiquetado de Confidencialidad de activos de Infromacion Aplicación de las tablas de retención documental	En Proceso			X	
A.8.2.3	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.	Descripcion de la actividad Plan de Gerencia de la información	En Proceso	X			

Justificación de exclusión

Comentarios/ Observaciones / Descripción General del Control
A.8.2.2 En proceso despliegue de carpetas sharepoint y controles de etiquetado de confidencialidad durante 2023

A.8.3. Manejo de medios de soporte.

Objetivo: Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER

A.8.3.1	Gestión de medios de Soporte Removibles	Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	DLP de endpoint para cierre de unidades usb y perifericos de almacenamiento y de conexiones de red no autorizadas Formato de Excepcion de controles con aprobacion de subdirecciones	Implementado			X	
A.8.3.2	Disposición de los medios de soporte.	Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.	En la política de seguridad se relacionan las Técnicas de borrado seguro y disposición de soportes de medios removibles A.8.3.2 Disposición final de los medios de soporte removibles, usando herramieta de borrado seguro opensource Procedimiento de Disposición Final de activos Grupo Gestión de Suministro y Almacén	Implementado			X	
A.8.3.3	Transferencia de medios de soporte físicos.	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Controles implemtados y relacionados en manual de seguridad de la información para historia clínica física y electrónica y Telesalud Uso de Herramienta para Ciframiento y compresión de medios licenciada	Implementado			X	

Justificación de exclusión

Comentarios/ Observaciones / Descripción General del Control

SECCION ANEXO A ISO 27001:2013
A.9 CONTROL DE ACCESO.

A.9.1. Requisitos del Negocio para Control de Acceso.

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.9.1.1	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 seguridad de la información.	Se encuentra incluida en las Políticas específicas de seguridad de la información. Manual de contraseñas y Control de Acceso	Implementado			X	

A.9.1.2	Propiedad de los activos.	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente	SDLAN y SDWAN controlado en Firewall de Nueva Generacion Sistema de control de acceso a la red NAC Controladoras WIFI y Portales cautivos para servicio WIFI VPN autorizadas por subdirecciones, con bloqueo por no uso despues de 40 dias.	Implementado			X	

Justificación de exclusión

Comentarios/ Observaciones / Descripción General del Control

A.9.2. Gestión de Acceso de Usuarios.

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GTI-P01-F-20
	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	VERSIÓN:	1
	DECLARACION DE APLICABILIDAD	VIGENCIA:	18-12-2020
		Página 1 de 1	

Objetivo: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.9.2.1	Registro y cancelación del registro de usuarios.	Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.	Manual de contraseñas y Control de Acceso	Implementado			X	
A.9.2.2	Suministro de acceso de usuarios.	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios	Manuales en SIAPINC: •Manual de contraseñas y Control de Acceso •Instructivo para administrar usuarios del centro de computo •Instructivo para administrar usuarios NAS •Instructivo para administrar usuarios SAP Automatizacion de ingreso , retiro y novedades de personal (En proceso 2023)	Implementado / En Proceso de mejora			X	
A.9.2.3	Gestión de derechos de acceso privilegiado.	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Verificación de Roles y Perfiles de sistemas de Información Controles incluidos en el Manual de Contraseñas y Control de Accesos: •Reglas generales de mínimos privilegios •Norma de caducidad de los permisos privilegiados •Contraseñas con mayor complejidad para mantener la confidencialidad de los datos de acceso de usuarios genéricos	Implementado			X	
A.9.2.4	Gestión de información de autenticación secreta de usuarios	. La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.	Manual de Contraseñas y Control de Accesos: •Cláusulas en contratos y condiciones de puesto de trabajo sobre el mantenimiento del secreto de las contraseñas o información de autenticación •Obligación de cambiar contraseñas iniciales después de su primer uso •Identificación al usuario antes de entregar o modificar las contraseñas •Uso de contraseñas seguras, no compartidas	Implementado			X	

A.9.2.5	Revisión de los derechos de acceso de usuarios	Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	Verificación de Roles y Perfiles de sistemas de Información Gestión de novedades para revisar derechos de acceso a la terminación de empleo o cambios en la organización por SIAPINC Controles incluidos en el Manual de Contraseñas y Control de Accesos: •Limitar en el tiempo los derechos de acceso con privilegios especiales	Implementado			X	
A.9.2.6	Cancelación 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 procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Gestión de novedades para revisar derechos de acceso a la terminación de empleo o cambios en la entidad por SIAPINC Gestión de novedades de proveedores de personal para revisar derechos de acceso a la terminación de empleo o cambios en la organización, usando listados enviados por correo electrónico a administradores de plataforma. Instructivo para depurar usuarios de SAP	Implementado / En Proceso de mejora			X	

Justificación de exclusión
Comentarios/ Observaciones / Descripción General del Control
A.9.2.2, A.9.2.6 En 2023 se encuenra en proceso de automatizacion control de ingreso , retiro y novedades de personal con herramieta de BPM

A.9.3. Responsabilidades de los usuarios.

Objetivo: Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.9.3.1	Uso de información secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Plan de seguridad y privacidad de la informacion Segmentacion de derechos de acceso mediante sistemas de autenticacion y el uso de perfiles y roles en cada sistema de infromacion. Integracion con Directorio Activo y Adconnect para cada nuevo aplicativo Controles incluidos en el Manual de Contraseñas y Control de Accesos •No divulgación de contraseñas •Evitar el uso de registros de contraseñas (papel, archivos etc.) •Norma para cambiar las contraseñas periódicamente •Norma para la calidad de las contraseñas •Evitar el almacenamiento de contraseñas fuera de gestor de contraseñas recomendado para administradores de plataformas •Forzar cambios de contraseñas iniciales •Evitar compartir contraseñas para distintos usos. • Responsabilidad de los usuarios en el manejo de la infromacion personal.	Implementado			X	

Justificación de exclusión
Comentarios/ Observaciones / Descripción General del Control

A.9.4. Control de Acceso a Sistemas y Aplicaciones.

Objetivo: Prevenir el uso no autorizado de sistemas y aplicaciones.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER

A.9.4.1	Restricción de acceso a 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.	Segmentacion de derechos de acceso mediante sistemas de autenticacion y el uso de perfiles y roles en cada sistema de infromacion. Manual de Contraseñas y Control de Accesos Formatos de solicitud de permisos de Firewall	Implemetado			X	
A.9.4.2	Procedimiento de Conexión Segura	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.	Sistema Nac para acceso seguro a la red Se utiliza desafío de usuario y contraseña en todos los aplicativos Portal Captivo para sistemas Wifi Doble factor de Autenticación para administración de plataformas Criticas Autenticación de nuevas aplicaciones por medio de Directorio Activo del INC.	Implemetado			X	
A.9.4.3	Sistema de Gestión de Contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	Uso de sistema de Gestión de Contraseñas para administradores de plataformas tecnológicas con generador de contraseñas aleatorias Revsiones de alineacion de sistemas de autenticacion a las politicas del Manual de control de acceso Doble factor de autenticacion de ofimatica para Administradores de plataformas	Implementado /Enproceso de Mejora			X	
A.9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Ningún funcionario o contratista del INC cuenta con permisos de administrador local de su computador para realizar instalación de software sin autorización, con excepciones justificadas debido a funcionamientos de aplicativos. Control de instalaciones de aplicaciones y utilitarios usando DLP de Endpoint y Políticas GPO	Implementado			X	
A.9.4.5	Control de Acceso a Códigos Fuente de Programas.	Se debe restringir el acceso a códigos fuente de programas.	Existe restricción de acceso a los códigos fuentes de las aplicaciones misionales a través de herramientas propias de cada contratista de desarrollo.	Implementado			X	

Justificación de exclusión
Comentarios/ Observaciones / Descripción General del Control
A.9.4.3 Se evalua despliegue de doble factor de autenticacion para todos los usuarios de sistema de ofimatica

SECCION ANEXO A ISO 27001:2013
A.10 CRIPTOGRAFÍA.

A.10.1. Controles Criptográficos.

Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.10.1.1	Política sobre el uso de controles Criptográficos.	Se debe desarrollar e implementar una política o norma sobre el uso de controles criptográficos para protección de información..	Incluida en las políticas específicas de seguridad de la información	En Proceso			X	
A.10.1.2	Gestión de Claves.	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.	Validez de llaves cripotiograficas SSL de 1 año Validez de Vpns de 1 año	Implementado			X	
Justificación de exclusión								
Comentarios/ Observaciones / Descripción General del Control								
A.10.1.1 Incluir formalizacion Manual de controles criptográficos que apoye la política de seguridad en PESI 2023								

SECCION ANEXO A ISO 27001:2013
A.11 SEGURIDAD FÍSICA Y AMBIENTAL.

A.11.1. Áreas Seguras.

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.11.1.1	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.	Controles biométricos para ingreso al Data Center Control de Acceso a Datacenter alternativo con control remoto Sistema CCTV administrado por Grupo Área Gestión de Infraestructura Evaluación y Revisiones de seguridad de perímetro, con empresa de seguridad Controles de seguridad física de Datacenter	Implementado			X	

A.11.1.2	Controles Físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	Uso Controles biométricos para ingreso al Data Center Control de Acceso a Datacenter alternativo con control remoto Uso de sistemas de Controles de Acceso físico (Biométricos, por tarjeta, por cedula, sistema de registro para visitantes) Uso de Controles biométricos con control de puerta para ubicaciones criticas Sistema CCTV administrado por Grupo Área Gestión de Infraestructura e Ingeniería Clínica	Implementado /En proceso de Mejora			X	
A.11.1.3	Seguridad de oficinas, salones e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.	Se cuenta con vigilancia privada para las instalaciones del INC Sistema CCTV administrado por Grupo Área Gestión de Infraestructura e Ingeniería Clínica Sistema de control de acceso físico	Implementado			X	
A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Se cuenta con el servicio de vigilancia para eventos de seguridad Para inundaciones se cuenta con sistemas de bombeo y cajas de desagüe. Para incendios se cuenta con un sistema de detección de incendios y extinción. Plan de Emergencias Brigadas de emergencia y simulacros de evacuación	Implementado			X	
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Prohibición de trabajos sin supervisión por parte de terceros en Datacenter y centros de Cableado Revisión de las zonas a la finalización de las visitas Prohibición de uso de móviles / cámaras a no ser que estén expresamente autorizados por la oficina de Comunicaciones	Implementado			X	

A.11.1.6	Áreas de despacho y carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado	Servicio de vigilancia privada; CCTV con monitoreo 7*24 Ingreso de vehículos de carga en zona aislada con autorización de Grupo Área Gestión de Infraestructura e Ingeniería Clínica Autorización y Control de personal que ingresa	Implementado /En proceso de Mejora			X	

Justificación de exclusión

Comentarios/ Observaciones / Descripción General del Control

A.11.1.2 En proceso cambio de control de acceso fisico perimetral, de sistemas de huella , a sistemas de reconocimiento facial.
A.11.1.6 De acuerdo a Om de revisoria fiscal se debe implementar bitacora de visitantes adicional para el ingreso a Datacenter

A.11.2. Equipos.

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.	Se cuenta con servicio de vigilancia privada permanente, cámaras de vigilancia y controles de acceso para acceder al INC y a áreas seguras; El Datacenter local se encuentra ubicado en una zona central con baja probabilidad de inundaciones, y cuenta con los debidos controles de respaldo y redundancia eléctrica, ambientales, y de extinción de incendio. Los portátiles se entregan a con guayas de seguridad a solicitud. Los equipos controlan su acceso mediante clave de usuario. Los equipos portátiles y equipos de escritorio críticos y expuestos a publico tienen habilitado Chip TPM para Ciframiento de disco por hardware Para el caso del proveedor de Servicios de CDR certifica que cumple con los estándares para Datacenter TIER III. La protección de la información y de los equipos se rigen de acuerdo con los estándares y políticas del INC, establecidos en las Políticas de Seguridad y Privacidad de la Información, y el Manual para normas y políticas de Seguridad	Implementado			X	X

A.11.2.2	Servicios Públicos de soporte	Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte	Para el caso de los edificios del INC: se cuenta con Sistema de corriente regulada y plantas eléctricas Para el caso del proveedor de Servicios de CDR certifica que cumple con los estándares para Datacenter TIER III. Redundancia eléctrica en Datacenter local con transferencia automática y conexión a 2 subestaciones. Sistemas de UPS, y ups exclusiva para el sistema de misión crítica SAP. Planta Eléctrica con autonomía de una semana.	Implementado			X	
A.11.2.3	Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.	Todo el cableado estructurado de la infraestructura del INC se encuentra distribuido a través de escalerillas y canaletas con división interna de cableado eléctrico y de telecomunicaciones. Los cuartos Eléctricos y de cableado estructurado se y mantienen cerrados bajo llave, y en custodia del Grupo Área Gestión de Infraestructura e Ingeniería Clínica EL cableado en Datacenter se encuentra ordenado, debidamente identificado y protegido en Racks, ducteria, y resguardados en escalerillas por techo y piso falso en celulosa. Para el caso del proveedor de Servicios de CRD certifica que cumple con los estándares para Datacenter TIER III.	Implementado			X	
A.11.2.4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Todos los equipos se encuentran cobijados en contratos de garantías y de mantenimientos periódicos preventivos y correctivos, a través del Outsourcing de mesa de ayuda, y el Grupo Área Gestión de Infraestructura e Ingeniería Clínica. Para el caso del proveedor de Servicios de CRD certifica que cumple con los estándares para Datacenter TIER III.	Implementado			X	

A.11.2.5	Retiro de Activos.	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	El instituto tiene implementado un formato (GCO-P04-F-06) y un manual para el manejo administrativo de activos bienes , los cuales se encuentra registrado en SIAPINC. Se cuenta con servicio de vigilancia privada permanente y cámaras de vigilancia para validar el registro y retiro de elementos en las porterías y recepciones.	Implementado			X	
A.11.2.6	Seguridad de equipos y activos fuera del predio	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de	El instituto tiene implementado un formato (GCO-P04-F-06) y un manual para el manejo administrativo de bienes, los cuales se encuentra registrado en SIAPINC. Cifrамiento de discos para equipos portátiles y equipos criticos o expuestos al publico. VPN SSL para mantener control de actualización es de seguridad y políticas a través de internet. Seguros contratados contra robo-perdida para equipos, y para manejos indebidos por parte de los usuarios Para el caso del proveedor de Servicios de CRD certifica que cumple con los estándares para Datacenter TIER III	En Proceso			X	
A.11.2.7	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 con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o reuso.	Se establece el mecanismo de borrado seguro de información para los equipos e impresoras que se van a dar de baja o en donación con la mesa de ayuda. Para el caso del proveedor de Servicios de CRD certifica que cumple con los estándares para Datacenter TIER III Se incluyen cláusulas de Borrado de seguro de la información en todos los contratos con proveedores y terceros.	En Proceso			X	

A.11.2.8	Equipos sin supervisión de los usuarios	Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.	Bloqueo automático de pantallas de los computadores aplicado por política de directorio activo, a los 15 minutos Guayas para equipos portátiles en salas de juntas y lugares desatendidos Socialización de técnicas de higiene de seguridad en inducción y reinducción y boletines Conexion de equipos en Byod con revisión minima de aplicacion de control de bloqueo de dispositivo.	Implementado			X	
A.11.2.9	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 para las instalaciones de procesamiento de información.	Incluida en las políticas específicas de seguridad de la información Socialización de técnicas de higiene de seguridad en inducción y reinducción, y boletines	Implementado			X	

Justificación de exclusión

Comentarios/ Observaciones / Descripción General del Control

SECCION ANEXO A ISO 27001:2013
A.12 SEGURIDAD DE LAS OPERACIONES.

A.12.1. Procedimientos operacionales y responsabilidades.

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.12.1.1	Procedimientos de operación documentadas	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.	Los procesos y procedimientos se encuentran publicados en SIAPINC, integrados en el Sistema Integrado de Gestión de la institución.	Implementado			X	

A.12.1.2	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.	Se cuenta con Formato de requerimientos y necesidades a sistemas GTI-P01-F-17 en Siapinc, que incluyen pruebas de seguridad Sistema de gestion de tickets centralizado para registrar los cambios y requerimeintos. Solicitudes de requermientos vpn con aprobacion previa de subdirecciones Formatos de aprobacion de cambios de Firewall RFI para planeación y ejecución de cambios que requieren ventanas de mantenimiento	Implementado			X	
A.12.1.3	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	Monitor PRTG implantado para monitorear la disponibilidad capacidad y salud de la infraestructura y servicios tecnológicos del INC Monitor Airwave para infraestructura de Red Ejecucion de ejercicos anualaes de consolidacion de datacenter	Implementado / en porceso de mejora			X	
A.12.1.4	Separación de los ambientes de desarrollo, ensayo y operación.	Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional	Para cada desarrollo contratado se solicitan contractualmente entornos de desarrollo y/o calidad separado de producción. Los entornos de desarrollo, código fuente y herramientas de desarrollo, no están disponibles para los entornos de producción.	Implementado			X	

Justificación de exclusión

Comentarios/ Observaciones / Descripción General del Control
A.12.1.3 Se encuentra en proceso de construcción y formalización el procedimiento de Gestión de Capacidad como Accion de mejora .

A.12.2. Protección contra códigos maliciosos.

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER

A.12.2.1	Controles contra códigos maliciosos.	Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	IPS, antivirus perimetral, porteccion de aplicaciones y navegacion, en Firewaal de nueva generacion Se cuenta con consola de antivirus de segunda generación con Deep Learning, para equipos y servidores Antivirus con Deeplearning nivel 2 Herramienta operativa de Analítica de amenazas y vulnerabilidades Antispam Avanzado, para control de phishing y adjuntos maliciosos WAF para pagina web tipo bussines y para servcios publicados a internet. XDR para equipos y servidores	Implementado			X	
Justificación de exclusión								
Comentarios/ Observaciones / Descripción General del Control								

A.12.3. Copias de Respaldo.

Objetivo: Proteger contra la pérdida de datos.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.12.3.1	Copias de 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.	Instructivos de Backup y Restauración registrados en SIAPINC (GTI-P01-I-03, GTI-P01-I-04, GTI-P01-I-05, GTI-P01-I-06, GTI-P01-I-07, GTI-P01-I-08) Herramientas de backup especializadas, con tareas programas de manera automática. Contrato de almacenamiento seguro de Cintas Externo al instituto. Bitácoras de Backup (GTI-P01-F-13, GTE-P04-F-12, P04-F-06) Nube corporativa para el respaldo de información equipos de cómputo de usuario Final CRD con sincronizacion cada 5 minutos de la informacion del sistema SAP Sincronizacion de información de equipos de computo a One Drive y Sharepint Control de Backups revisado semestralmete	Implementado			X	
Justificación de exclusión								

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GTI-P01-F-20
	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	VERSIÓN:	1
	DECLARACION DE APLICABILIDAD	VIGENCIA:	18-12-2020
		Página 1 de 1	

Comentarios/ Observaciones / Descripción General del Control

A.12.4. Registro y Seguimiento.

Objetivo: Registrar eventos y generar evidencia.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.12.4.1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.	Se almacenans logs del sistema con los eventos y actividades de los usuarios en cada máquina. Herramienta operativa de Analítica de amenazas y vulnerabilidades para registro, clasificación y atención de eventos. Alertas configuradas con envio a correso electronicos en caso de detectar comportamientos inusuales Correlacion de incidentes con plataforma XDR	Implementado			X	
A.12.4.2	Protección de la información de registro.	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Los registros de logs se protegen con nivles de acceso para evitar pérdidas, corrupción o cambios no autorizados Se guardan copias de seguridad de los registros de eventos para sistemas críticos misionales Controles de acceso instalados para restringir el acceso físico solo a personal autorizado	Implementado		X	X	
A.12.4.3	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.	Los registros de logs de administradores tienen nivel de protección apropiado para evitar pérdidas, corrupción o cambios no autorizados Logs de sistema activados en todas las plataformas tecnológicas y sistemas de información. Revsiones periodicas de roles y perfiles de administración Se guardar copias de seguridad de los registros de eventos para sistemas críticos misionales	Implementado			X	
A.12.4.4	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.	Equipos y servidores sincornizados con servicio de NTP Network Time Protocol - Sincronizado contra la hora legal para Colombia del Instituto Nacional de Metrología (172.16.0.15) Modificación de opciones de cambio de fecha y hora deshabilitadas en los equipos mediante GPO	Implementado			X	

Justificación de exclusión
Comentarios/ Observaciones / Descripción General del Control

A.12.5. Control de Software Operacional

Objetivo: Asegurarse de la integridad de los sistemas operacionales.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.12.5.1	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Retiro de privilegios de administración sobre equipos de computo para usuarios, definido mediante roles y perfiles Se controla las instalaciones usando DLP de Endpoint y políticas de GPO, con elevacion de permisos de mesa de ayuda. La coordinacion de aplicaciones /oficial de segruidad autoriza la instalación de software con base en control de licenciamiento adquirido por el INC. Revision de licenciamiento de uso de software opensource y demos por oficial de segruidad de la información Actualizaciones de sistemas operativos en equipos y servidores se prueban 1 semana antes de despliegue definitivo.Grupo de pruebas de WSUS 129 equipos	Implementado	X		X	X

Justificación de exclusión
Comentarios/ Observaciones / Descripción General del Control

A.12.6. Gestión de vulnerabilidad técnica.

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.12.6.1	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.	Herramienta operativa de Analítica de amenazas y vulnerabilidades. Relaizacion de pruebas de vulnerabilidades y Ethical Hacking periódicos. Herramienta de Gestión controlada de actualizaciones de seguridad. Pruebas de envio de phishing controlado	Implementado			x	

A.12.6.2	Restricciones sobre la instalación de Software	Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.	Herramienta de Bloqueo y control de instalaciones DLP de Endpoint y/o por políticas GPO. La Coordinacion de Aplicaciones y el responsable de control de licencimiento es quien autoriza la instalación de software con base en el licenciamiento adquirido por el INC.	Implementado			x	
Justificación de exclusión								
Comentarios/ Observaciones / Descripción General del Control								

A.12.7. Consideraciones sobre auditorías de sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.12.7.1	Controles sobre auditorías de Sistemas de Información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Ejecucion de auditorias Iso 27001 periodicas contratadas externamente Ejecución de revisiones periodicas de la Gestion de Ti y seguridad de la informacion	Implementada			X	
Justificación de exclusión								
Comentarios/ Observaciones / Descripción General del Control								

SECCION ANEXO A ISO 27001:2013
A.13 SEGURIDAD DE LAS COMUNICACIONES

A.13.1. Gestión de Seguridad de Redes

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.13.1.1	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones	Se cuenta con segmentación de vlans, separando las capas de servicio en Servidores, administradores, usuarios, sistemas biomédicos, Movilidad y Wifi, y Control de Acceso a la red NAC Monitores de redes especializados para switches. Monitor de redes especializado para Elementos activos de red, sistemas y aplicaciones. Controladora de red Wifi	Implementado			X	

A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Se encuentra separado el control de la red de las tareas de operación. Se implanta arquitectura en HA para mantener las conexiones en canales y sistemas de red críticos. Se utiliza monitoreo y registro de las actividades en la red para establecer medidas preventivas y correctivas Control de acceso y privilegios a la red con NAC ANS establecidos para contratos de redes comunicaciones, los cuales son supervisados por la coordinación de Hardware y Redes	Implemetado			X	
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Arquitectura de Segmentación de redes aplicada de forma lógica separando, servidores, administradores de plataforma, usuarios, dispositivos móviles, redes Wifi y dispositivos y sistemas biomédicos.	Implementado			X	
Justificación de exclusión								
Comentarios/ Observaciones / Descripción General del Control								

A.13.2. Transferencia de información.

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.13.2.1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.	Incluida en las políticas específicas de seguridad de la información	Implementado	X		X	
A.13.2.2	Acuerdos sobre transferencia de información	. Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	La transferencia segura de la información con las partes externas se define en los convenios o en la normatividad de los anexos técnicos de contratos. Formato de Contrato de transmisión de datos	Implementado, en proceso de mejora			X	
A.13.2.3	Mensajes electrónicos	Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	Apropiacion de Microsoft teams como herramieta de comunicación de mensajeria. Cierre de redes sociales de uso no laboral, aprobados por subdirecciones.	Implementado			X	

A.13.2.4	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.	Se cuenta con el formato de acuerdo de confidencialidad y deber de secreto para VPN Se cuenta con el formato de acuerdo de confidencialidad y deber de secreto para los contratos de trabajadores y colaboradores Se cuenta con cláusulas de confidencialidad y deber	Implementado		X	X	
Justificación de exclusión								
Comentarios/ Observaciones / Descripción General del Control								
A.13.2.2 Codificar formato de contrato de trasmision de datos en 2023								

SECCION ANEXO A ISO 27001:2013
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

A.14.1. Requisitos de seguridad de los sistemas de información.

Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
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.	Documento de requisitos estándar para contratos de criterios de seguridad de la información, que es personalizado para cada tipo de estudio previo y/o contrato. Procesos de compras formales que incluyan periodos de garantía, validación del producto y pólizas de seriedad y cumplimiento Revisiones de seguridad requeridas por una aplicación o sistema antes de su fase de desarrollo o implantación.	Implementado			X	
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Se cuentan con certificados de sitios seguros SSL estándar para las aplicaciones misionales y de apoyo. Sistemas de doble autenticación para administración de sistemas críticos de seguridad, Firewall, antivirus, antispam. Uso de túneles virtuales cifrados VPN SSL para comunicación remota DLP de sistemas de ofimática y correo	Implementado, En Proceso de mejora			X	

A.14.1.3	Protección de transacciones de servicios de aplicaciones	La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados	Uso de firma digital para garantizar las comunicaciones extremo a extremo Uso de canal de comunicación cifrado VPN para garantizar la confidencialidad de las transmisiones La utilización de protocolos seguros para correo electrónico y VPN Plataforma antispam para servcio de correo	Implementado			X	
Justificación de exclusión								
Comentarios/ Observaciones / Descripción General del Control								
A.14.1.2 En evaluacion despliegue de multiple factor de autenticacion para todos los usuarios dentro de arquitectura Zero trust								

A.14.2. Seguridad en los procesos de desarrollo y de soporte

Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.14.2.1	Política de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.	Incluida en las políticas específicas de seguridad de la información	Implementado			X	
A.14.2.2	Procedimiento de control de cambios en sistemas.	. Los cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas a los desarrollos dentro de la organización	Los cambios que se requieren para los sistemas de información se documentan en un control de cambios de los contratistas de desarrollo. La especificación y documentación de la implantación de cambios se realiza en los formatos establecidos con cada contratista de desarrollo. Uso de aplicaciones de versionamiento de cada	Implementado			X	
A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacionales.	En todas las aplicaciones críticas y no críticas, se realizan pruebas de funcionamiento previo y posterior a la publicación.	Implementado			X	
A.14.2.4	Restricciones sobre los cambios de paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente	Se implantan solamente los cambios a software autorizados por la Coordinadora de desarrollo y aplicaciones Se verifican las licencias o consentimientos del propietario del software Se verifica instalación siempre de versiones estables y corporativas del software Se valida compatibilidad de software a instalar con el software existente	Implementado			X	
A.14.2.5	Principios de construcción de sistemas de seguros	Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.	Se exige a los proveedores de desarrollo y aplicaciones emplear procedimientos seguros para el diseño y codificación desde la parte contractual.	Implementado			X	

A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas	Se cuenta con un ambiente de Desarrollo y calidad para las aplicaciones misionales Uso de aplicaciones de versionamiento de cada proveedor de desarrollo.	Implementado			X	
A.14.2.7	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.	Se realizan reuniones de seguimiento, presentación de informes de avance, pruebas al desarrollo contratado y verificación de cumplimiento de obligaciones contractuales	Implementado	X			
A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad	Se mantienen disponibles ambientes de calidad de aplicativos misionales, para que verifiquen su integración con seguridad y su funcionamiento.	Implementado			X	
A.14.2.9	Pruebas de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados	Los administradores de plataformas y personal de calidad realizan las pruebas funcionales y de seguridad planificadas. Se vinculan los usuarios funcionales, en la realización de pruebas y verificación de resultados de las pruebas, previos a la publicación de nuevas versiones. Formato GTI-P01-F-17 de Necesidades de TIC modificado para registrar pruebas de seguridad	Implementado			X	
Justificación de exclusión								
Comentarios/ Observaciones / Descripción General del Control								

A.14.3. Datos de Pruebas

Objetivo: Asegurar la protección de los datos usados para pruebas.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.14.3.1	Protección de datos de pruebas	Los datos de pruebas se deben seleccionar, proteger y controlar cuidadosamente	Los datos se pueden utilizar en pruebas siempre únicamente si son públicos, de lo contrario se utilizan datos no reales. Los datos de pruebas se resguardan en ambientes controlados y separados de ambiente de producción	Implementado			X	
Justificación de exclusión								
Comentarios/ Observaciones / Descripción General del Control								

SECCION ANEXO A ISO 27001:2013
A.15 RELACIONES CON LOS PROVEEDORES

A.15.1. Seguridad de la información en las relaciones con los proveedores.

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.15.1.1	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.	Incluida en las políticas específicas de seguridad de la información	Implementado			x	
A.15.1.2	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 puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	Se establecen los requisitos de seguridad de la información con los proveedores a través de: *. Contratos, *. Pliegos de condiciones, *. Acuerdos Marcos de Precios Documeto con requisitos estandar de segruidad para contratos, revisados de acuerdo a cada contrato o convenio.	Implementado			x	
A.15.1.3	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.	Se establecen los requisitos de seguridad de la información con los proveedores a través de: *. Contratos, *. Pliegos de condiciones, *. Acuerdos Marcos de Precios	Implementado			x	

Justificación de exclusión

Comentarios/ Observaciones / Descripción General del Control

A.15.2. Gestión de la prestación de servicios de proveedores.

Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.15.2.1	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.	Se realiza a través de la supervisión de los contratos. (Manual de supervision de contratos)	Implementado			X	
A.15.2.2	Gestión de cambios a los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.	Se realiza a través de la supervisión de los contratos. (Manual de supervision de contratos)	Implementado			X	

Justificación de exclusión

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GTI-P01-F-20
	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	VERSIÓN:	1
	DECLARACION DE APLICABILIDAD	VIGENCIA:	18-12-2020
		Página 1 de 1	

Comentarios/ Observaciones / Descripción General del Control

SECCION ANEXO A ISO 27001:2013
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

A.16.1. Gestión de incidentes y mejoras en la seguridad de la información

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 debilidad.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.16.1.1	IResponsabilidades 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.	Se cuenta con una guía de gestión de incidentes de seguridad de la información	Implementado, En Proceso de mejora			X	
A.16.1.2	Informe 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.	El registro de eventos se encuentra centralizado en la mesa de ayuda. Línea 7000, correo sima@cancer.gov.co Árbol configurado de Incidentes y requerimiento de seguridad en herramienta de gestión de incidentes de la mesa de ayuda se cuenta con el correo electrónico: seguridaddigital@cancer.gov.co para comuncacion de incidentes de seguridad Canal establecido para recepción de eventos de habeas data pqrs@cancer.gov.co	Implementado			X	
A.16.1.3	Informe 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 se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Obligación de reporte de eventos de seguridad por parte de los usuarios, incluida en Política de Seguridad y Privacidad de la Información Obligación de reporte de eventos de seguridad por parte de los proveedores y terceros, incluida en requerimientos de seguridad para contratos	Implementado			X	
A.16.1.4	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	Se cuenta con una guía de gestión de incidentes de seguridad de la información Se cuenta con una herramienta de análisis de amenazas y vulnerabilidades que clasifica la criticidad y prioridad de los eventos de seguridad de la información	Implementado, en proceso de mejora			X	
A.16.1.5	. 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.	Se cuenta con una guía de gestión de incidentes de seguridad de la información Se Mantiene registro indicador de incidentes de seguridad cerrados durante el mes en SIAPINC	Implementado			X	
A.16.1.6	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 el impacto de incidentes futuros.	Se realiza análisis de eventos críticos y frecuentes y se exponen las actividades para solucionarlos en los Grupos Primarios de Mejoramiento Formato de eventos de incidentos criticos de Csirt Gobierno incluye analis de causa raiz, planes de mejoramiento y lecciones aprendidas	Implementado			X	

A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Se adopta formato de recolección de incidentes de csrit Gobierno Preparación de Oficial de seguridad de la información como primer respondiente ante eventos de seguridad Se Mantiene logs de eventos en herramienta de amenazas y vulnerabilidades	Implementado	X		X	

Justificación de exclusión

Comentarios/ Observaciones / Descripción General del Control

A.16.1.1 Se debe actualizar r Manual de gestion de incidentes y SDP de segruidad incluido en catalogo de sistemas tecnologicos

SECCION ANEXO A ISO 27001:2013
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

A.17.1. Continuidad de seguridad de la información

Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.17.1.1	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 seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres	Se cuenta con procedimientos de contingencia para tecnologías En construcción BIA de Tecnología Documento de controles de segruidad de Historia Clinica y Telesalud en Fisico y electronico	En Proceso			x	
A.17.1.2	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.	Planes de contingencia para SAP Centro de Recuperación de desastres CDR para SAP, nivel TIER III Planes de Contingencia y continuidad de negocio de Outsourcing de Sistemas Manual de controles de Historia Clinica en fisico y electronico	En Proceso			x	
A.17.1.3	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 implementados con el fin de asegurar que los válidos y eficaces durante situaciones adversas	Pruebas semestrales de Centro de recuperación de desastres (CRD) para SAP	Implementado			x	

Justificación de exclusión

Comentarios/ Observaciones / Descripción General del Control

A.17.1.1 Formalizar BIA (Analisis de impacto de negocio) de tecnología.
A.17.1.2 Se registra en PSPI actualizar planes de contingencia infomática, ejecucion de consultoria liderada por Subdireccion Administrativa

A.17.2. Redundancia

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GTI-P01-F-20
	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	VERSIÓN:	1
	DECLARACION DE APLICABILIDAD	VIGENCIA:	18-12-2020
		Página 1 de 1	

Objetivo: Asegurarse de la disponibilidad de instalaciones de procesamiento de información.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Se cuenta con un contrato de Centro de recuperación de desastres CDR para SAP que tiene la capacidad de operar con una capacidad del 50% de los usuarios con una disponibilidad es del 99.95% Implantación de sistemas HA para servicios críticos de operación;	Implementado			X	
Justificación de exclusión								
Comentarios/ Observaciones / Descripción General del Control								

SECCION ANEXO A ISO 27001:2013
A.18 CUMPLIMIENTO INTERNO Y REGULATORIO

A.18.1. Cumplimiento de requisitos legales y contractuales.

Objetivo: Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.18.1.1	Identificación de los requisitos de legislación y contractuales aplicables	Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.	Se cuenta con definición de requisitos reglamentarios, estatutarios en las políticas de seguridad y privacidad de la información, política de tratamiento de datos personales, y plan de seguridad y privacidad de la información., publicados en Siapinc y Página Web del INC	Implementado	X			
A.18.1.2	Derechos de Propiedad Intelectual	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 licenciados.	Clausula Propiedad Intelectual de acuerdo con la indicación en los estudios previos, contratos y convenios. Lineamientos de cumplimiento sobre licenciamiento, derechos de autor y propiedad intelectual en el INC incluidas en la política de seguridad y privacidad de la información .	Implementado	X			
A.18.1.3	Protección de registros	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio	Inventario de Activos de Información, actualizado anualmente EL INC cuenta con un contrato suscrito para almacenamiento, custodia y consulta de la información, cumpliendo con las normas establecidas por el Archivo General de Nación.	Implementado			X	
A.18.1.4	Privacidad y protección de la información identificable personalmente	Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable	Política de Tratamiento de Datos Personales Canal de recepción de solicitudes de tratamiento de datos personales a través de pqrs@cancer.gov.co y oficina de correspondencia Consentimiento Informado integrado en Historia	En Implemtacion	X		X	

A.18.1.5	Reglamentación de Controles Criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos	Reglamentado en Politica de seguridad y privacidad de la información. El INC ha implantado los siguientes controles criptograficos: •Uso de firma electrónica •Uso de servicio de Correo electrónico Certificado •Uso de Certificados SSL web •Canales cifrados para las comunicaciones y herramientas de cifrado en el tratamiento de la información sensible al contratar servicios. •Ciframinento de las credenciales de acceso cuando se solicitan desarrollos web o de apps que impliquen login de usuarios •Acceso desde el exterior estableciendo canales VPN cifrados para usuarios y proveedores •Uso de Herramientas de cifrado de información local en equipos •Cifrado de la wifi institucional con el estándar de cifrado más seguro, actualmente WPA2.	En Proceso	X		X	

Justificación de exclusión

A.18.1.3 El INC está evaluando la implantación de un SGDC para la protección de registros y control documental.
A.18.1.5. Se debe evaluar controles para cifrado de backups, cifrado de dispositivos móviles, y la verificaion de protocolos seguros de comunicación a los servidores para administración y transferencia de ficheros.

Comentarios/ Observaciones / Descripción General del Control

A.18.2. Revisiones de seguridad de la información

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.

ID Control	Objetivo de Control	Control Norma Iso 27001:2013 27002-2013	Controles	Estado	Seleccion Controles Y razón de la selección			
					RL	OC	RN / MP	RER
A.18.2.1	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, la políticas, los procesos y los procedimientos para seguridad de la información se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos	Se cuenta con procesos de Auditorias de seguridad de la información con frecuencia cada 2 años, contratada por oficina de control Interno.	Implementado			x	
A.18.2.2	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.	Monitoreos trimestrales de gestión de riesgos de seguridad digital Revisiones en Comité de Seguridad de la Información MIPG Seguimiento de seguridad en equipos primarios de Mejoramiento	Implementado			x	
A.18.2.3	Revisión del Cumplimiento Técnico	Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Se cuenta con el monitoreo 7x24 de disponibilidad y salud de servicios, aplicaciones, redes y plataformas tecnológicas Revisión de informes técnicos de proveedores por supervisores de contrato	Implementado			x	

Justificación de exclusión

Comentarios/ Observaciones / Descripción General del Control

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	**CÓDIGO:**	**GTI-P01-F-20**
	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	**VERSIÓN:**	**1**
	DECLARACION DE APLICABILIDAD	**VIGENCIA:**	**18-12-2020**
		Página 1 de 1	

A.18.2.2 Deben definirse los indicadores de cumplimiento de políticas
A.18.2.3 Debe evaluarse la adquision de un sistema tipo UEBA o de IA para validar anomalías en el comportamientos de los usuarios y el cumplimiento de políticas , y la correlacion de riesgo basico.

ELABORÓ		**REVISÓ**		**APROBÓ**	
Cargo:	Profesional Especializado	Cargo:	Coordinadores de Grupo	Cargo:	Coodinador Grupo Area
Dependencia:	Sistemas	Dependencia:	Aplicaciones, Hardware y redes	Dependencia:	Sistemas
Fecha:	26/07/2023	Fecha:	27/07/2023	Fecha:	27/07/2023