
 HOSPITAL LOCAL NIT 846.000.253-6	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS			 TODOS JUNTOS POR LA ACREDITACIÓN
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD			
	Código:	Versión: 02	Fecha aprobación:	
RESOLUCIÓN				Página:

**RESOLUCIÓN N° 275 de 2019
 TREINTA Y UNO (31) DE OCTUBRE**

**POR LA CUAL SE ADOPTA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA
 INFORMACIÓN Y DEMAS POLITICAS REFERENTES A PRESERVAR LA
 CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN**

DE LA E.S.E. HOSPITAL LOCAL DE PUERTO ASÍS

El Gerente de la Empresa Social del Estado Hospital Local de Puerto Asís en uso de sus facultades constitucionales y legales, en especial las conferidas por la Ley 100 de 1993, Ley 1122 de 2007, Ley 610 de 2000, Ley 1438 de 2011 y,

CONSIDERANDO:

Que mediante la Ley 1273 de 2009 se creó un bien jurídico tutelado denominado de la protección de la información y de los datos, tipificando penalmente las conductas contra la confidencialidad, la integridad y la disponibilidad de los datos de los sistemas informativos.



Que el Decreto 2573 de 2014, por el cual se establecen los lineamientos generales de la estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones, en su artículo 5° establece los componentes que facilitan la masificación de la oferta y de la demanda del Gobierno en Línea.

Que el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, reglamenta el componente de seguridad y privacidad de la información tendiente a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada. Que en el artículo 2.2.9.1.3.2 del presente Decreto, estableció los plazos para la implementación del Manual de Gobierno en Línea, por parte de las entidades del orden nacional.

Que por medio de CONPES 3701 y el 3854 de 2016 se fijó los lineamientos y la política Nacional de seguridad digital, para que las entidades del Estado constituyan mecanismos para la gestión de los riesgos digitales.

Que conforme a la normatividad citada surge la necesidad de adoptar una política institucional de seguridad y privacidad de la información considerando el papel estratégico de las tecnologías de información y comunicaciones –TIC frente al Modelo de

Elaboró: Andrea Delgado Romo Oficina Jurídica	REVISÓ: Cristiam Cerón INGENIERO DE SISTEMAS	Aprobó: Julio Oswaldo Quiñones Mayoral Gerente
--	---	---

 HOSPITAL LOCAL NIT 846.000.253-6	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASIS SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		 TODOS JUNTOS POR LA ACREDITACIÓN
	Código:	Versión: 02	
RESOLUCIÓN			Página:

Seguridad y Privacidad de la Información; además de la importancia de mitigar riesgos alrededor de la información mediante la implementación de planes para el manejo de incidentes, así como las herramientas para respaldar las actividades ejecutadas en la E.S.E HOSPITAL LOCAL DE PUERTO ASIS, incentivando la cultura de seguridad de la información a los usuarios, previniendo o solucionando posibles ataques informáticos, virus, robos, uso indebido de software o pérdidas de información.

Que el fundamento de una política institucional de seguridad y privacidad de la información es buscar la gestión del conocimiento como base para la mejora continua de la misma, adaptándola a la normatividad vigente en el sector, las tendencias tecnológicas y los cambios en la gestión de procesos y procedimientos tecnológicos en la E.S.E. HOSPITAL LOCAL DE PUERTO ASIS.

RESUELVE

ARTICULO 1. ADOPTAR El "Sistema de Gestión de la Seguridad de la Información" -SGSI -de la E.S.E HOSPITAL LOCAL DE PUERTO ASIS; que se describe en documento anexo que reposa en el archivo de la Oficina de Sistemas de la Entidad y se encuentra publicado en la Página Web de la citada dependencia y que hace parte integral de la presente Resolución. El SGSI comprende la política, estructura, procesos y recursos institucionales necesarios para implantar la gestión de la seguridad de la información en la Entidad.

ARTICULO 2. ÁMBITO. La ejecución del Modelo y la Política de Seguridad y Privacidad de la Información estará a cargo de todos los colaboradores de la institución, independiente de su modelo de vinculación y demás terceros que hagan uso de los recursos físicos y lógicos de la institución



ARTÍCULO 3. Vigencia: La presente Resolución rige a partir de la fecha de su expedición y deroga todas las disposiciones que le sean contrarias.

COMUNIQUESE Y CUMPLASE

Dada en Puerto Asís (Putumayo) a los 31 días del mes de octubre


JULIO OSWALDO QUIÑONES MAYORAL
 Gerente

Elaboró: Andrea Delgado Romo Oficina Jurídica	REVISÓ: Cristlham Cerón INGENIERO DE SISTEMAS	Aprobó: Julio Oswaldo Quiñones Mayoral Gerente
--	--	---

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060-16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 1 de 51	

FICHA TÉCNICA DEL DOCUMENTO

DATOS GENERALES DEL DOCUMENTO

NOMBRE DEL DOCUMENTO: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA E.S.E. HOSPITAL LOCAL DE PUERTO ASÍS.

OBJETIVO: Establecer y difundir los criterios y comportamientos que deben seguir todos los funcionarios directos, temporales, contratistas, practicantes, terceros o cualquier persona que tenga una relación contractual con la E.S.E. Hospital Local de Puerto Asís, o que tenga acceso a los activos de información, con el propósito de preservar la Confidencialidad, Integridad y Disponibilidad de la información a fin de fortalecer la continuidad de las actividades administrativas, operativas y logísticas de la Entidad, protegiendo adecuadamente la información, reduciendo los riesgos y optimizando la inversión en tecnologías de información. Para tal efecto, se obrará en concordancia con las disposiciones legales vigentes.

ALCANCE: El presente documento define la política, lineamientos, controles y directrices para el Sistema de Gestión de Seguridad de la Información de la E.S.E. Hospital Local de Puerto Asís. La política establecida y sus posteriores actualizaciones aplican a todos los activos de información y las partes interesadas de la Entidad.

1. JUSTIFICACION
 El presente documentos busca definir la política, lineamientos, controles y directrices para el Sistema de Gestión de Seguridad de la Información de la E.S.E. Hospital Local de Puerto Asís y el cumplimiento de la ley 1266 de 2008 "Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información", ley 1273 de 2009 "Protección de la Información y de los Datos", documento CONPES 3854 de 11 de abril de 2016 "Ciberseguridad y Ciberdefensa - Política Nacional de Seguridad Digital", ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" y su decreto reglamentario 1377 del 27 de junio de 2013, decreto 2573 de 2014, Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional y territorial de la República de Colombia, y apoyados en la Norma Técnica – ISO/IEC 27000 e ISO/IEC 27001:2013.

Elabora: Coordinador de TI Cristian David Cerón Castro	Revisó: Coordinador de TI Cristian David Cerón Castro	Aprobó: Gerente Julio Oswaldo Quiñonez Mayoral
Ino. Mesa de Soporte Luis Coral Hernández	Oficina Jurídica. Andrea Delgado Romo	Nancy Johana Deaza Hernandez Subgerente Administrativa (E)



EMPRESA SOCIAL DEL ESTADO
HOSPITAL LOCAL DE PUERTO ASÍS

SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Código: SIST.PL-1080.15

Fecha aprobación: 31/10/2019

Versión: 01

Pág: 2 de 31



TODOS JUNTOS POR LA
ACREDITACIÓN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA E.S.E. HOSPITAL LOCAL DE PUERTO ASÍS

Este documento describe las generalidades de los Anexos de la Política de Seguridad de la Información de la E.S.E. Hospital Local de Puerto Asís. Para su elaboración, se toman como base los controles y requisitos identificados en el estándar ISO/IEC 27001:2013. Las políticas incluidas en este documento se constituyen como parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad y se convierten en la base para la implantación de controles, procedimientos y estándares. La Seguridad de la Información es una prioridad para la E.S.E. Hospital Local de Puerto Asís y por tanto es responsabilidad de todos los funcionarios velar por el continuo cumplimiento de las políticas definidas en el presente documento.

COPIA CONTROLADA







	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PI-1060.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 3 de 61	

TABLA DE CONTENIDO

GLOSARIO	5
1. OBJETIVOS Y ALCANCE	8
Objetivo General	8
Objetivos Específicos	8
Alcance	8
2. MARCO DE REFERENCIA	9
Antecedentes	9
Referencias Normativas	10
3. ROLES Y RESPONSABILIDADES.....	10
Alta Dirección.....	10
Oficina de Tecnología de la Información y Subgerencia Administrativa	11
Oficina de Recursos Humanos	12
Oficina de Control Interno.....	12
Líderes de los procesos o áreas	12
4. ACCIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN	12
5. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN	15
5.1. Política de Administración de Contraseñas	15
5.2. Política de Uso de Cuentas para Acceso a Recursos Tecnológicos	15
5.3. Política de Acceso a la Red por Terceros	17
5.4. Política de Gestión de Medios Removibles	19
5.5. Política de Gestión de Registros (logs)	20
5.6. Política de Sensibilización, Formación y Toma de Conciencia en Seguridad de la Información	21
5.7. Política de Bloqueo de Sesión, Escritorio y Pantalla Limpia.....	21
5.8. Política de Documentación de procedimientos operativos	22
5.9. Política de Control de Cambios Operativos	23
5.10. Política de Control de Versiones	24
5.11. Política de Seguridad de la Información en la Continuidad del Negocio.....	24
5.12. Política de Derechos de Propiedad Intelectual	25

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 4 de 51	

5.13.	Política de Sanciones Previstas por Incumplimiento	26
5.14.	Política de Seguridad física y ambiental	26
5.15.	Política de Administración y Control de usuarios al Datacenter	27
5.16.	Política de Trabajo en Áreas Protegidas	27
5.17.	Política de Seguridad y Mantenimiento de los Equipos	28
5.18.	Política de Seguridad de los equipos fuera de las instalaciones	29
5.19.	Política de intercambio de información	29
	Derechos de Propiedad Intelectual de la E.S.E. Hospital Local	30
5.20.	Política de Acuerdos de Confidencialidad	32
5.21.	Política de Uso de Dispositivos Móviles y Teletrabajo	32
5.22.	Política de Control de Acceso a Áreas Protegidas	33
5.23.	Política de Gestión de Activos de Información	34
5.24.	Política de Uso Adecuado de los Activos de Información	35
5.25.	Política de Protección contra Software Malicioso	41
5.26.	Política de Administración de Backups, Recuperación y Restauración de la información	43
5.27.	Política de Gestión de Vulnerabilidades Técnicas	44
5.28.	Política de Administración de Componentes Electrónicos de Procesamiento de Información	45
5.29.	Política de Adquisición de Hardware	48
5.30.	Política de Adquisición de Software	48
5.31.	Política de Gestión de Incidentes de Seguridad de la Información	49

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2010	
	Versión: 01	Pág.: 6 de 61	

GLOSARIO

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).



Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág: 6 de 61	

(software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datacenter: Centro de procesamiento de datos. Instalación empleada para albergar sistemas de información y componentes asociados donde generalmente incluyen espacio para hardware en un ambiente controlado, acondicionando el espacio con el aire acondicionado, extinción de incendios y diferentes dispositivos de seguridad para permitir que los equipos tengan el mejor nivel de rendimiento con la máxima disponibilidad del sistema.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).



Ley de Habeas Data: Se refiere a la Ley Estatutaria 1581 de 2012.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 7 de 61	

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información - SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).



Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Calidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág: 8 de 81	

1. OBJETIVOS Y ALCANCE

Objetivo General



Establecer y difundir los criterios y comportamientos que deben seguir todos los funcionarios directos, temporales, contratistas, practicantes, terceros o cualquier persona que tenga una relación contractual con la E.S.E. Hospital Local de Puerto Asís, o que tenga acceso a los activos de información, con el propósito de preservar la Confidencialidad, Integridad y Disponibilidad de la información a fin de fortalecer la continuidad de las actividades administrativas, operativas y logísticas de la Entidad, protegiendo adecuadamente la información, reduciendo los riesgos y optimizando la inversión en tecnologías de información. Para tal efecto, se obrará en concordancia con las disposiciones legales vigentes.

Objetivos Específicos

- Proteger los recursos de información y tecnología frente a amenazas internas y externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, mediante la implementación de controles efectivos.
- Establecer un modelo organizacional de Seguridad de la Información, definiendo claramente los roles y responsabilidades de los que intervienen en la implementación de la política.
- Promover, mantener y realizar mejoramiento continuo del nivel de cultura en Seguridad de la Información, así como lograr la concientización de todos los funcionarios, contratistas y demás personas que interactúen con la E.S.E. Hospital Local de Puerto Asís, para minimizar la ocurrencia de incidentes de Seguridad de la Información.
- Mantener la política de Seguridad de la Información actualizada, a efectos de asegurar su vigencia y eficacia.

Alcance

El presente documento define la política, lineamientos, controles y directrices para el Sistema de Gestión de Seguridad de la Información de la E.S.E. Hospital Local de Puerto Asís. La política establecida y sus posteriores actualizaciones aplican a todos los activos de información y las partes interesadas de la Entidad.

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 9 de 61	

2. MARCO DE REFERENCIA



Antecedentes

Teniendo en cuenta que la información es un activo vital para el éxito y el cumplimiento de la misión de la E.S.E. Hospital Local de Puerto Asís, este documento se encuentra alineado con la familia de normas de la serie ISO 27000 como marco de referencia para la implementación de su Sistema de Gestión de Seguridad de la Información (SGSI).

ISO 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la Seguridad de la Información utilizable por cualquier tipo de organización. Entre las distintas normas que componen la serie ISO 27000 y que fueron tomadas como referente, se resalta ISO/IEC 27001:2013 sobre los requisitos para el establecimiento del Sistema de Gestión de Seguridad de la Información. La información, así como la plataforma tecnológica que la soporta, es considerada un activo estratégico para la E.S.E. Hospital Local de Puerto Asís, por lo que es fundamental establecer políticas que definan el marco de control para brindar seguridad a los activos de información de la Entidad. Estos activos de información se constituyen en el soporte de la misión y la visión, por lo que requieren ser utilizados y manejados dentro de un adecuado entorno de seguridad, cualquiera que sea el medio y el ambiente tecnológico en el que se encuentren.

Las organizaciones tanto públicas como privadas se están tornando altamente dependientes de sus sistemas de información y de los recursos informáticos que los soportan, por lo que se convierte en una decisión estratégica el implementar un Sistema de Gestión de Seguridad de la Información que esté directamente relacionado con las necesidades, objetivos institucionales y direccionamiento estratégico.

La implementación de un SGSI está orientada a definir los aspectos necesarios para establecer, operar, mantener y dirigir de manera estandarizada, sistemática y organizada un sistema efectivo que permita el tratamiento seguro de la información.

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Página: 10 de 51	

Referencias Normativas

- Ley 1266 de 2008 "Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información".
- Ley 1273 de 2009 "Protección de la Información y de los Datos".
- Documento CONPES 3854 de 11 de abril de 2016 "Ciberseguridad y Ciberdefensa - Política Nacional de Seguridad Digital"
- Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" y su decreto reglamentario 1377 del 27 de junio de 2013.
- Decreto 2573 de 2014, Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional y territorial de la República de Colombia.
- Norma Técnica – ISO/IEC 27000
- Norma Técnica ISO/IEC 27001:2013



3. ROLES Y RESPONSABILIDADES¹

Alta Dirección²

- Verificar el cumplimiento de la presente Directiva, en particular la difusión y adopción de las políticas, normas y estándares de Seguridad de la Información.
- Apoyar los programas de sensibilización, actualización y entrenamiento técnico del personal de las áreas de tecnología en temas relacionados con Seguridad de la Información.
- Apoyar la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

¹ ISO/IEC 27001:2013, Requisito 5.3



² ISO/IEC 27001:2013, Requisito 5

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060-16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 11 de 51	

- Gestionar los recursos financieros requeridos para la apropiada protección de los activos de información y mantenimiento del SGSI.

Oficina de Tecnología de la Información y Subgerencia Administrativa

- Implementar, apoyar y soportar el Sistema de Gestión de Seguridad de la Información.
- Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de Seguridad de la Información.
- Administrar las herramientas tecnológicas para el cumplimiento de las políticas de Seguridad de la Información.
- Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.
- Definir e implementar la estrategia de concientización y sensibilización en Seguridad de la Información para los funcionarios, contratistas y terceros.
- Custodiar la información y los medios de almacenamiento bajo su responsabilidad.
- Definir, mantener y controlar la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software base y de aplicaciones.
- Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas.
- Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.
- Establecer, documentar y dar mantenimiento a los procedimientos de Seguridad de la Información que apliquen para la plataforma de tecnologías de información administrada por esta oficina.
- Gestionar los incidentes de Seguridad de la Información que se presenten en la Entidad.

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 12 de 51	

Oficina de Recursos Humanos³

Incluir en los programas de inducción y de re-inducción el tema de seguridad de la información asegurando que los funcionarios conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información o de otros recursos informáticos, haciendo énfasis en las consecuencias jurídicas que puede acarrear al servidor público y aliados de la entidad.

Oficina de Control Interno⁴

Validar la aplicación y cumplimiento de las políticas de Seguridad de la Información definidas en esta Directiva, la aplicación de controles sobre los activos de información y los requerimientos del Sistema de Gestión de Seguridad de la Información.

Líderes de los procesos o áreas⁵

Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados con sus procesos, incluyendo aquellas actividades que sean consideradas como controles de Seguridad de la Información dentro de dichos procedimientos.

4. ACCIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN



A continuación se describen algunas acciones identificadas que afectan la Seguridad de la Información, y que ponen en riesgo su disponibilidad, confidencialidad e integridad:

- I. Dejar los computadores encendidos en horas no laborables.
- II. Permitir que personas ajenas a la E.S.E. Hospital Local de Puerto Asís ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.
- III. No clasificar y/o etiquetar la información.
- IV. No guardar bajo llave documentos impresos que contengan información

³ ISO/IEC 27001:2013 Anexo A, Ítem 7



⁴ ISO/IEC 27001:2013, Requisito 9.2 - ISO/IEC 27001:2013 Anexo A, Requisito 10.1

⁵ ISO/IEC 27001:2013, Requisito 5.1

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 13 de 51	

clasificada al terminar la jornada laboral.



- V. No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
- VI. Reutilizar papel que contenga información sensible o Historias clínicas, no borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y garantizar que no queden documentos o notas escritas sobre las mesas.
- VII. Hacer uso de la red de datos de la E.S.E. Hospital Local de Puerto Asís para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.
- VIII. Instalar software en la plataforma tecnológica de la E.S.E. Hospital Local de Puerto Asís cuyo uso no esté autorizado por la Oficina de TI, y que pueda atentar contra las leyes de derechos de autor o propiedad intelectual.
- IX. Enviar información clasificada de la Entidad por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.
- X. Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca a la E.S.E. Hospital Local de Puerto Asís.
- XI. Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos de la Entidad sin la debida autorización.
- XII. Ingresar a la red de datos de Entidad por cualquier servicio de acceso remoto sin la autorización de la Oficina de TI de la institución.
- XIII. Usar servicios de internet en los equipos de la Entidad, diferente al provisto por la Oficina de TI de la institución.
- XIV. Promoción o mantenimiento de actividades personales, o utilización de los recursos tecnológicos de la E.S.E. Hospital Local de Puerto Asís para beneficio personal.
- XV. Uso de la identidad institucional digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2019	
Versión: 01	Pág.: 14 de 51		

otro funcionario o contratista.

- XVI. Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.
- XVII. Retirar de las instalaciones de la E.S.E. Hospital Local de Puerto Asís computadores de escritorio, portátiles e información física o digital clasificada, sin autorización o abandonarla en lugares públicos o de fácil acceso.
- XVIII. Entregar, enseñar o divulgar información clasificada de la E.S.E. Hospital Local de Puerto Asís a personas o entidades no autorizadas.
- XIX. Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica de la Entidad o de terceras partes.
- XX. Ejecutar cualquier acción que difame, afecte la reputación o imagen de la E.S.E. Hospital Local de Puerto Asís, o alguno de sus funcionarios, utilizando para ello la plataforma tecnológica.
- XXI. Realizar cambios no autorizados en la Plataforma Tecnológica de la Entidad.
- XXII. Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.
- XXIII. Ejecutar acciones para eludir y/o modificar los controles establecidos en la presente política de Seguridad de la Información.
- XXIV. Consumir alimentos y bebidas, cerca de la plataforma tecnológica.
- XXV. Conectar a la corriente regulada dispositivos diferentes a equipos de cómputo o equipos biomédicos.
- XXVI. Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

La realización de alguna de estas prácticas u otras que afecten la Seguridad de la Información, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo a los procedimientos establecidos para cada caso.

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 15 de 51	

5. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1. Política de Administración de Contraseñas⁶

Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:



- a. Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
- b. Las contraseñas no deberán ser reveladas.
- c. Las contraseñas no se deberán escribir en ningún medio.
- d. Los funcionarios y contratistas deben digitar siempre su usuario y contraseña para acceder a las diferentes aplicaciones de la Entidad; la contraseña no se deben guardar de forma automática en los inicios de sesión de las aplicaciones; igualmente al terminar la jornada deben cerrar las sesiones abiertas antes de apagar el equipo.
- e. Es deber de cualquier funcionario y contratista reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece, y debe catalogarse como un incidente de seguridad.

5.2. Política de Uso de Cuentas para Acceso a Recursos Tecnológicos⁷

- a. Todas las personas que tengan acceso a la infraestructura tecnológica o a los sistemas de información, deben contar con una definición clara de los roles y funciones sobre estos, para reducir y evitar el uso no autorizado o modificación no intencional sobre los activos de información.
- b. La segregación de funciones sobre la infraestructura tecnológica y sobre los sistemas de información deberá ser revisada periódicamente por la



⁶ ISO/IEC 27001:2013 Anexo A, Ítem 9.2

⁷ ISO/IEC 27001 Anexo A, Ítem 9.2.2

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 18 de 51	

oficina de TI con el fin de mantener actualizada dicha información y acorde con la realidad de cada una de las dependencias de la Entidad.

- c. Toda persona, Sistema de Información o componente de procesamiento de información que requiera tener acceso a un componente de procesamiento de Información, contará con una cuenta única de uso exclusivo e intransferible que permite el acceso a la información de acuerdo con la necesidad de uso aprobada por el responsable de la información
- d. El responsable de la información almacenada en el componente tecnológico será el responsable de aprobar los privilegios que se asignaran a la cuenta de usuario, considerando para ese fin la necesidad de acceso a información de acuerdo con las funciones que desempeñara el usuario o componente electrónico de procesamiento de información que utilizará la cuenta de acceso.
- e. La asignación de toda cuenta de acceso a un componente electrónico de procesamiento de información debe cumplir con controles que permitan identificar los responsables de las actividades de: solicitud, aprobación, creación, modificación, inactivación o eliminación autorizada de la cuenta de acceso, así como el mantenimiento de la veracidad y trazabilidad de la actividades realizadas para la asignación de la cuenta de acceso.
- f. Toda acción realizada empleando la cuenta de acceso debe ser registrada mediante controles que permitan mantener la trazabilidad de las mismas.
- g. Toda cuenta de acceso empleará como mínimo una contraseña como mecanismo de autenticación seguro.
- h. Toda contraseña para cuenta de acceso debe cumplir con los estándares de contraseña segura que adopta la E.S.E. Hospital Local de Puerto Asís, dependiendo de la criticidad de la información. El estándar básico debe incluir mínimo 8 caracteres, una letra mayúscula, letras minúsculas y un número. Para sistemas de información con información crítica, se debe incluir la obligatoriedad de un símbolo especial (*%/ñ, etc.)
- i. Toda cuenta de acceso es personal e intransferible.
- j. Toda cuenta de acceso debe ser asignada formalmente a una persona quién responderá por su uso y acciones realizadas con la misma en el componente electrónico de procesamiento de información o con la información del componente de procesamiento de información.



	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2019	
Versión: 01		Pág.: 17 de 51	

- k. Toda cuenta de acceso que no cuente con un responsable en un momento en el tiempo de manera temporal o definitiva debe ser inhabilitada para evitar su uso por parte de otros usuarios o componentes electrónicos de procesamiento de información que no estén formalmente autorizados y permanecerá inhabilitada hasta tanto no esté disponible el responsable de la cuenta de acceso o se decida su inactivación definitiva.

5.3. Política de Acceso a la Red por Terceros⁸



- a. Por ningún motivo se permitirá el ingreso a la Red de Área Local (LAN) de equipos personales de funcionarios, contratistas o terceros.
- b. La Red de Área Local (LAN) es de uso exclusivo de los equipos de la E.S.E. Hospital de Puerto Asís.
- c. Deben establecerse, mantenerse y actualizarse medidas de control de acceso a nivel de red, instalaciones, sistemas operativos, bases de datos y aplicaciones; los controles deben limitar el acceso de los usuarios hacia los activos de información al mínimo requerido (Principio de Mínimo privilegio) para la realización de su trabajo. Además, deben permitir identificar de manera inequívoca cada usuario y hacer seguimiento de las actividades que éste realiza.
- d. Toda persona, proceso o sistema de información que realice actividades para la E.S.E. Hospital Local de Puerto Asís deberá tener acceso únicamente a la información necesaria para el desempeño de las actividades que le han sido autorizadas.
- e. Todo acceso a la información deberá ser autorizado formalmente por el área responsable de la información. Para la autorización de acceso a la información se debe contemplar un análisis previo de la justificación de la necesidad de uso de la misma y las actividades a realizar con el acceso a la información.
- f. Todo acceso a la información debe considerar el nivel de clasificación definido por la E.S.E. Hospital Local de Puerto Asís o por el Custodio de la información cuando se trate de información de un Tercero.
- g. Todo acceso a la información debe cumplir con los requisitos legales,

⁸ ISO/IEC 27001 Anexo A, Ítems 13.1 y 15

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág. 18 de 61	

normativos, reglamentarios, procedimentales o de cualquier otra índole que haya definido el responsable de la información.

- h. El acceso a la información de la Entidad debe estar sujeto a controles que garanticen la trazabilidad de las acciones realizadas sobre la misma, considerando la identificación de la persona, proceso o sistema que realiza el acceso, acciones realizadas, instante de tiempo en que se realizan las acciones y ubicación desde la cual se realiza el acceso a la misma.
- i. Cualquier evento que implique un riesgo para la preservación de la Confidencialidad, Integridad, Disponibilidad, Autenticidad o Trazabilidad de la información debe ser notificado al responsable de la misma mediante conductos autorizados.
- j. El acceso a la información obliga a la aceptación formal por parte del usuario o el responsable del componente electrónico de procesamiento de información de la reglamentación de acceso y tratamiento de la información que defina las leyes de Colombia, Acuerdos internacionales suscritos por Colombia, normas del sector, políticas, estándares o cualquier tipo de control establecido para la protección o tratamiento de la información.
- k. En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica y que deban desarrollarse dentro de las instalaciones de la E.S.E. Hospital Local de Puerto Asís, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar para el acceso a información sensible.
- l. En ningún caso se otorgará acceso a terceros a la información sensible, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.
- m. Los equipos destinados a labores "in house" por las empresas jurídicas que tengan una relación contractual con la E.S.E. Hospital Local de Puerto Asís, deben tener una protección que incluya: Antivirus, Antispyware, Antimalware, Anti-bot y protección contra ataques de día cero como el Ransomware.
- n. Se deben exigir criterios de selección que contemplen la historia y

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1050.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 19 de 51	



reputación de la tercero, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, procesos de selección de personal, seguimiento de estándares de gestión de calidad y seguridad, criterios que resulten de un análisis de riesgos de la selección y los criterios que tenga establecidos la Entidad para los procesos de contratación.

- o. Deben existir contratos, convenios, acuerdos o mecanismos formalmente aprobados por la Entidad para proteger a información o servicios que se compartan con terceros. Los mecanismos administrativos formales definirán claramente el tipo de información, su clasificación, acuerdos para uso y protección de la información. Los terceros deben aceptar y cumplir las Políticas de Seguridad de la Información de la Entidad y de manera particular la política de intercambio de información.
- p. Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadores, contemplarán como mínimo los siguientes aspectos:
 - Forma en los que se cumplirán los requisitos legales aplicables.
 - Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conocen sus responsabilidades en materia de seguridad.
 - Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos.
 - Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible.
 - Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
 - Niveles de seguridad física que se asignará al equipamiento tercerizado.
 - Derecho a la auditoría por parte de la E.S.E. Hospital Local de Puerto Asís.

5.4. Política de Gestión de Medios Removibles⁹

- a. Se encuentra restringida la conexión no autorizada a la infraestructura tecnológica de la E.S.E. Hospital Local de Puerto Asís, de cualquier elemento de almacenamiento como dispositivos personales USB, discos

⁹ ISO/IEC 27001:2013 Anexo A, Ítem 8.3.1

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Página 20 de 61	



duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales.

- b. Los medios de almacenamiento removibles como cintas, discos duros removibles, CDs, DVDs, medios impresos y dispositivos USB, entre otros, que contengan información institucional, deben ser controlados y físicamente protegidos.
- c. La Entidad definirá los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas, estas serán definidas por la Oficina de TI y/o Subgerencia Administrativa, en la plataforma tecnológica si es requerido para el cumplimiento de sus funciones.
- d. Cada medio removible de almacenamiento deberá estar identificado de acuerdo con el tipo de información que almacene.
- e. Para los procesos de baja, reutilización o garantías de los dispositivos que contengan medios de almacenamiento, se debe cumplir según sea el caso con la destrucción física del mismo y/o borrado seguro.
- f. El tránsito o préstamo de medios removibles deberá ser autorizado por el propietario del activo de información.

5.5. Política de Gestión de Registros (logs)¹⁰

- a. Tanto los sistemas de información que manejan información crítica, como los dispositivos de procesamiento, de red y de seguridad informática deberán generar registros de eventos (logs) que serán verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información.
- b. El tiempo de retención de los logs estará dado por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red y por las leyes, normativas o regulaciones vigentes.
- c. Todo aquel evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica deberá ser reportado a la Oficina de TI y/o Subgerencia Administrativa.

¹⁰ ISO/IEC 27001:2013 Anexo A, Ítem 12.4.2

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080-16	Fecha aprobación: 31/10/2019	
	Versión: 01	PÁG.: 21 de 51	

5.6. Política de Sensibilización, Formación y Toma de Conciencia en Seguridad de la Información¹¹



- a. La E.S.E. Hospital Local de Puerto Asís debe mantener un programa anual de concientización y sensibilización para los funcionarios y contratistas que interactúen con la información institucional y desarrollen actividades en sus instalaciones. Esto con el fin de proteger la información y la infraestructura tecnológica que la soporta.
- b. Todos los funcionarios y contratistas al servicio de la Entidad deben ser informados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.
- c. Todos los funcionarios, servidores públicos, contratistas y terceros que prestan sus servicios a la E.S.E. Hospital Local de Puerto Asís deben mejorar continuamente sus habilidades y competencias con relación a la seguridad de la información.
- d. La E.S.E. Hospital Local de Puerto Asís dispone oportunamente de los medios para desarrollar actividades que fomenten y garanticen la difusión, conocimiento, sensibilización, formación y educación del subsistema de gestión de seguridad de la información.
- e. Las actividades de difusión, conocimiento, sensibilización, formación y educación del subsistema de gestión de seguridad de la información se realizarán tomando en cuenta las responsabilidades, conocimientos y necesidades específicas de las áreas y funcionarios a las que van dirigidas.

5.7. Política de Bloqueo de Sesión, Escritorio y Pantalla Limpia¹²

- a. En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica protegida bajo llave.
- b. Los usuarios deberán bloquear su estación cada vez que se retiren de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del usuario.

¹¹ ISO/IEC 27001:2013 Anexo A, ítem 7.2.2

¹² ISO/IEC 27001:2013 Anexo A, ítems 11.2.8 y 11.2.9



	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 22 de 61	

- c. Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por la E.S.E., el cual se activará automáticamente después del tiempo de inactividad definido por el responsable de Seguridad de la Información, y se podrá desbloquear únicamente con la contraseña del usuario.
- d. Los usuarios deberán retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
- e. No se deberá reutilizar papel que contenga información sensible.
- f. Los usuarios no deberán almacenar en el escritorio de sus estaciones de trabajo documentos, accesos directos a los mismos o a sistemas de información sensibles.
- g. Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.

5.8. Política de Documentación de procedimientos operativos¹³

- a. La ejecución de cualquier actividad asociada con la infraestructura tecnológica para el procesamiento de información, comunicaciones y seguridad informática debe estar soportada por instrucciones o procedimientos operativos documentados, los cuales siempre deben estar a disposición de todos los usuarios que los necesiten para el desarrollo de sus labores.
- b. La elaboración, publicación y modificación que se realice de los documentos debe ser autorizada por la Oficina de TI y/o Subgerencia Administrativa.
- c. Los procedimientos operativos deben contener instrucciones para el manejo de errores que se puedan presentar en la ejecución de las actividades, contactos de soporte, procedimientos de reinicio y recuperación de sistemas y aplicaciones, forma de procesamiento y manejo de la información, copia de respaldo de la información y los demás

¹³ ISO/IEC 27001:2013 Anexo A, Ítem 12.1



	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060-15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 23 de 51	

a los que hubiere lugar.

5.9. Política de Control de Cambios Operativos¹⁴

- a. Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte de la Oficina de TI y/o Subgerencia Administrativa; debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.
- b. Todos los cambios que se realicen sobre los sistemas de información y la infraestructura tecnológica deberán estar precedidas de la definición de los requerimientos, especificaciones y controles definidos en el procedimiento "PROCEDIMIENTO CONTROL DE CAMBIOS".
- c. Todos los cambios a la infraestructura de Información y Tecnología deben estar plenamente justificados.
- d. Los cambios deben ser propuestos e implementados sin perjuicio de la calidad de los servicios de Información y Tecnología de Comunicaciones de la E.S.E. Hospital Local de Puerto Asís.
- e. Todos los cambios deben ser formalmente documentados.
- f. Todos los cambios deben incluir un análisis de los riesgos de su implementación y de su no implementación.
- g. Todos los cambios deben ser sometidos a algún mecanismo de prueba que permita verificar si su planificación está completa antes de su ejecución.
- h. Solamente se ejecutan los cambios que han sido aprobados por debidamente autorizados por la E.S.E. Hospital Local de Puerto Asís.
- i. Todos los cambios deben estar formalmente registrados, clasificados y documentados siguiendo los procedimientos adoptados por la E.S.E. Hospital Local de Puerto Asís.
- j. Todos los cambios debe poderse deshacerse mediante planes de "retirada

¹⁴ ISO/IEC 27001:2013 Anexo A, Ítem 12.1.2

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 24 de 61	

del cambio" en caso de un incorrecto funcionamiento tras su implementación.

- k. Cuando se realicen cambios a la infraestructura de información y tecnología de comunicaciones de la Entidad se debe verificar la necesidad de actualizar los planes de contingencia y continuidad de negocio.

5.10. Política de Control de Versiones¹⁵



- a. Antes de la puesta en producción de una aplicación nueva, o de la modificación de las plataformas existentes, se debe asignar un número de edición o versión a la misma. Así, el número de versión se irá incrementando en cada cambio que se genere sobre la misma aplicación.
- b. El método de enumeración de las versiones deberá distinguir entre versiones en producción, en etapa de desarrollo, en etapa de pruebas o versión archivada.
- c. Todas las versiones deben ser almacenadas en bibliotecas, repositorios o directorios y deben contar con controles de acceso lógicos donde sólo se permita el acceso al personal autorizado.
- d. Periódicamente, las versiones que se encuentran en los ambientes de producción deben ser verificadas contra los repositorios y la documentación de los controles de cambio con el fin de determinar si los dos son congruentes. Si llegase a presentarse incongruencia en la revisión realizada, esto será identificado como un incidente de seguridad y se atenderá de acuerdo con el procedimiento de Gestión de Incidentes de seguridad.

5.11. Política de Seguridad de la Información en la Continuidad del Negocio¹⁶

- a. La Seguridad de la Información es una prioridad y se incluye como parte de la gestión general de la continuidad del negocio y del compromiso de la Alta Dirección.
- b. La Entidad deberá contar como mínimo con un Plan de Recuperación ante Desastres (DRP) que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.

¹⁵ ISO/IEC 27001:2013 Anexo A, Ítems 14.2.2 y 15.2.2

¹⁶ ISO/IEC 27001:2013 Anexo A, Ítem 17.1



	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 28 de 61	

- c. Para la E.S.E. su activo más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal establecer las estrategias para mantenerlo.
- d. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, estarán incorporados y definidos en el Plan de Recuperación ante Desastres.
- e. Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio al responsable de la gestión del Plan de Recuperación ante Desastres.

5.12. Política de Derechos de Propiedad Intelectual¹⁷

- a. No se permitirá el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.
- b. La E.S.E. cumplirá con la reglamentación de propiedad intelectual, para lo cual implementarán los controles necesarios que garanticen el cumplimiento de dicha reglamentación.
- c. Se permitirá el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.
- d. Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.
- e. El desarrollo de software a la medida adquirido a terceras partes o realizados por funcionarios de la Entidad, serán de uso exclusivo de la E.S.E. Hospital Local y la propiedad intelectual será de quien lo desarrolle.

¹⁷ ISO/IEC 27001:2013 Anexo A, Ítem 18.1.2

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 29 de 61	

5.13. Política de Sanciones Previstas por Incumplimiento¹⁸

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente política de seguridad, conforme a lo dispuesto por las normas que rigen al personal de la E.S.E. y en caso de corresponder, se realizarán las acciones correspondientes ante el o los organismos pertinentes.



Las sanciones solo pueden imponerse mediante un acto administrativo que así lo disponga, cumpliendo las formalidades impuestas por los preceptos constitucionales, la ley de procedimientos administrativos y demás normativas específicas aplicables. Además de las sanciones disciplinarias o administrativas, la persona que no da debido cumplimiento a sus obligaciones puede incurrir también en responsabilidad civil o patrimonial, cuando ocasiona un daño que debe ser indemnizado y/o en responsabilidad penal cuando su conducta constituye un comportamiento considerado delito por el código penal y leyes especiales.

5.14. Política de Seguridad física y ambiental¹⁹

- a. Las áreas protegidas y el Centro de Datos se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por la Oficina de Tecnologías de la Información y/o Subgerencia Administrativa, a fin de permitir el acceso solo a personal autorizado.
- b. Para la selección de las áreas protegidas y la ubicación del Centro de Datos se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad de las instalaciones.
- c. Las plataformas tecnológicas serán ubicadas y protegidas de tal manera que reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.
- d. El cableado de datos que se incluya en cualquier proyecto en las instalaciones de la Entidad debe ser mínimo de categoría 6.
- e. El cableado de energía eléctrica y comunicaciones que transportan datos o brindan apoyo a los servicios de información estarán protegidos contra interceptación o daños.

¹⁸ ISO/IEC 27001:2013 Anexo A, Ítem 18.1 e ISO/IEC 27001:2013 Anexo A, Ítem 7.2.3

¹⁹ ISO/IEC 27001:2013 Anexo A, Ítem 11

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 27 de 51	

f. Se deberá garantizar la seguridad física del Centro de Datos, incluyendo entre otros los siguientes subsistemas:

- Sistema Eléctrico suplementario.

5.15. Política de Administración y Control de usuarios al Datacenter²⁰



- a. Los funcionarios y contratistas deben contar con un carnet de identificación para el ingreso a las diferentes instalaciones de la E.S.E., Los carnets institucionales deberán ser controladas por el área de Personal de la institución.
- b. En la entrada principal se encuentra la recepción con vigilantes, encargados del control del acceso de las personas a la Entidad.
- c. Todas las puertas que garanticen control de acceso deberán permanecer cerradas, y es responsabilidad de todos los funcionarios y contratistas evitar que las puertas se dejen abiertas. Las personas que tengan acceso al Datacenter serán definidas única y exclusivamente por la Oficina de Tecnologías de la Información y/o Subgerencia Administrativa.
- d. Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado para ellos por la E.S.E. mientras permanezcan dentro de sus instalaciones.
- e. Es responsabilidad de todos los funcionarios y contratistas borrar la información sensible escrita en los tableros o pizarras al finalizar las reuniones de trabajo y garantizar que no queden documentos o notas escritas sobre las mesas.
- f. Es responsabilidad de todos los funcionarios y contratistas acatar las normas de seguridad y mecanismos de control de acceso de la Entidad, dispuestos por la empresa de seguridad privada contratada para tal fin.

5.16. Política de Trabajo en Áreas Protegidas²¹

- a. En las áreas donde se encuentren activos informáticos, se debe cumplir como mínimo con los siguientes lineamientos:
 - No se deben consumir alimentos ni bebidas.

²⁰ ISO/IEC 27001:2013 Anexo A, Ítem 11.1

²¹ ISO/IEC 27001:2013 Anexo A, Ítem 11.1.5

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág. 28 de 51	

- No se deben ingresar elementos inflamables.
- No se debe permitir el acceso de personal ajeno sin que este acompañado por un funcionario durante el tiempo que dure su visita.
- No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
- No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
- No se permite el ingreso de equipos electrónicos, así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.



b. Las áreas protegidas deben contar con las condiciones ambientales que garanticen la correcta operación de los equipos y el estado de los medios que contienen información, así como un sistema de detección y control de incendios.

c. Debe existir un extintor tipo C, verificando las especificaciones de seguridad contra incendios de medios eléctricos y electrónicos.

5.17. Política de Seguridad y Mantenimiento de los Equipos²²

- a. Los equipos que hacen parte de la infraestructura tecnológica de la E.S.E. deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado a los mismos.
- b. La E.S.E. adoptará los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo entre otros.
- c. Los funcionarios y contratistas velarán por el uso adecuado de los equipos de escritorio, portátiles y móviles que les hayan sido asignados, por lo tanto, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.
- d. Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se realicen mantenimientos periódicos con el fin de que dichas actividades no se vean afectadas por obsolescencia. Por lo tanto, revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de

²² ISO/IEC 27001:2013 Anexo A, Ítem 11.2

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 29 de 51	

sus fabricantes.

- e. Los equipos portátiles deberán estar asegurados con la guaya o el mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones de la E.S.E.



5.18. Política de Seguridad de los equipos fuera de las instalaciones²³

- a. Los usuarios que requieran usar los equipos fuera de las instalaciones de la E.S.E. deben velar por la protección de los mismos sin dejarlos desatendidos en lugares públicos o privados en los que se puedan ver comprometidos.
- b. En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información sensible, se deberá realizar inmediatamente el respectivo reporte y se deberá poner la denuncia ante la autoridad competente, si aplica.
- c. Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones de la E.S.E. deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieren o puedan poner en riesgo la información que contiene.

5.19. Política de intercambio de información

- a. La información propiedad de la E.S.E. Hospital Local o que se encuentra bajo su custodia se debe controlar siguiendo las políticas de seguridad de la información de la Entidad y la reglamentación a la cual está sometida la Entidad.
- b. El intercambio de información con terceros debe ser aprobado formalmente por los custodios de la información.
- c. En cumplimiento de Decreto 235 de 2010 del Ministerio del Interior y de Justicia, por el cual se regula el intercambio de información entre Entidades públicas, los requerimientos de información que se hagan por Entidades estatales en cumplimiento de una función administrativa o en ejercicio de una facultad legal, o por los particulares encargados de una función administrativa, a otras Entidades del Estado, no constituyen solicitud de un servicio y, por ende, no generan costo alguno para la Entidad solicitante.

²³ ISO/IEC 27001:2013 Anexo A, Ítem 11.2.5

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Página 30 de 81	

- d. Para el intercambio de información se deben establecer mecanismos magnéticos, electrónicos o telemáticos para integrar, compartir o suministrar la información que por mandato legal se requiere, o permitir el acceso total dentro del marco de la Constitución y el derecho fundamental a la intimidad, a las bases de datos completas que requieran otras Entidades para el ejercicio de sus funciones.
- e. Cuando se apruebe el intercambio de información con un tercero, se deberá suscribir previamente contratos o acuerdo de confidencialidad en el cuales se señalarán los términos y condiciones para la entrega de la información requerida.
- f. Cuando se intercambie información clasificada como RESERVADA o SENSIBLE, se debe cifrar siguiendo la política y controles definidos por la E.S.E. Hospital Local para la protección de dichos tipos de información.
- g. La entrega de información, no concede autorización expresa o implícita, o permiso o licencia de uso de marcas comerciales, patentes, derechos de autor o de cualquier otro derecho de propiedad industrial o intelectual sobre la información que sea suministrada por la E.S.E. Hospital Local a un tercero.



Derechos de Propiedad Intelectual de la E.S.E. Hospital Local

Los documentos, datos, estudios técnicos y toda la información que puedan contener los medios análogos, los soportes físicos y los archivos entregados por la E.S.E., son propiedad de la Entidad y en consecuencia se encuentran protegidos por la leyes de propiedad intelectual vigentes en Colombia, así como por los convenios y tratados internacionales aplicables a la materia. En la medida de lo anterior el receptor de la información se obliga a no exportar o reproducir los archivos o datos relacionados a ningún otro sitio diferente al que se especifique con la Entidad al momento del recibo de la información.

Reserva de propiedad de la E.S.E. Hospital Local y concesión de licencia con derechos limitados para el uso de la información de la E.S.E.:

Al momento de la entrega de la información, la E.S.E. definirá la limitación de derechos para el uso de la información. La E.S.E. mantendrá en todos los casos los derechos de autor de la información generada por la Entidad.

La información, datos o documentos entregados a TERCERAS PARTES no se podrá comercializar, ni prestar, ni copiar, ni compartir, ni reproducir, ni

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 31 de 51	

arrendar, ni enajenar, ni prestar servicios a TERCEROS no autorizados expresamente por la E.S.E. y sólo podrá ser copiada, compartida, reproducida o utilizada exclusivamente para realizar las actividades que sean expresamente autorizadas por la entidad al momento de la entrega de la información.

Los documentos o Información suministrada por la E.S.E. se utilizarán exclusivamente para las actividades propias del acuerdo que se establezca con el TERCERO. En el caso que objeto genere algún tipo de documento o publicación estos deberán contener la siguiente atribución de derechos de propiedad de la E.S.E., "Este documento incluye información de propiedad de la E.S.E. Hospital Local y se utiliza bajo su autorización, todos los derechos sobre la información propiedad de la E.S.E. Hospital Local están reservados a la Entidad".



Para el cumplimiento de la Política de intercambio de Información, las áreas responsables de la información deben coordinar sus esfuerzos con el Comité de Tecnologías de Información y Comunicaciones para lograr implementación de los controles que se identifiquen como necesarios para el intercambio de información.

Todos los funcionarios y contratistas de la Entidad que en el desarrollo de sus tareas habituales u ocasionales deban realizar actividades relacionadas con el intercambio de información dentro de la Entidad o con terceros son responsables del cumplimiento y seguimiento de esta política.

La información de la Entidad de ser empleada para servir a una finalidad operativa y administrativa en relación con la E.S.E., Cualquier Información de la Entidad es susceptible de ser auditada para propósitos de control interno, control de calidad o investigación de incidentes de seguridad de la información, en consecuencia el usuario reconoce y acepta que la información institucional que sea objeto de intercambio puede ser analizada siguiendo los procedimientos administrativos a los que está sujeta la Entidad.

Los terceros que reciban información de la E.S.E. se deben comprometer a proteger toda información que les sea suministrada por parte de la E.S.E., sin importar su nivel de clasificación para evitar su divulgación no autorizada aplicando los procedimientos administrativos, técnicos o legales que se acuerden con la E.S.E. Hospital Local al momento de recibir la información.

Los documentos o Información suministrados por la E.S.E. no pueden ser utilizados por el tercero en detrimento de la Entidad o para fines diferentes a

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 32 de 51	

los establecidos en el acuerdo que se establezca con el tercero para intercambio de información ya que la información o documentos sólo podrán utilizarse para cumplir las obligaciones acordadas.

Los terceros que reciban información de la E.S.E. Hospital Local deben informar a cada uno de sus empleados o colaboradores debidamente autorizados para recibir documentos o Información, de los niveles de clasificación de la Información definidos por la E.S.E. y de la existencia de acuerdos de confidencialidad con la Entidad. Igualmente el tercero debe instruir a quién reciba la información o documentos, acerca de las medidas de protección y mecanismos para manejar la información y la obligatoriedad de no utilizarla sino para los temas necesarios para el desarrollo del acuerdo suscrito entre la E.S.E. y el tercero quién será enteramente responsable por cualquier uso inadecuado de la información suministrada por la Entidad

Los terceros que reciban información de la E.S.E. deben garantizar que aplicarán todas medidas de seguridad razonables a su alcance, para evitar divulgación, fuga o uso no autorizado de información y deben aceptar que protegerán la información suministrada aplicando los controles que se especifiquen al momento de la entrega de la información.

5.20. Política de Acuerdos de Confidencialidad²⁴



Todos los funcionarios, contratistas y demás terceros deben firmar la cláusula y/o acuerdo de confidencialidad y este deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o entidades externas.

5.21. Política de Uso de Dispositivos Móviles y Teletrabajo²⁵

- a. Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se deben implementar controles de acceso y mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la Seguridad de la Información.
- b. La conexión de los dispositivos móviles a la infraestructura tecnológica

²⁴ ISO/IEC 27001:2013 Anexo A, Ítem 15.1.2

²⁵ ISO/IEC 27001:2013 Anexo A, Ítem 11.2.6

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 33 de 81	



institucional deberá ser autorizada por la Oficina de TI y/o Subgerencia Administrativa, previa verificación de que cuenten con las condiciones de seguridad y estableciendo mecanismos de control necesarios para proteger la infraestructura de la Entidad.

- c. El Comité de Tecnologías de Información y Comunicaciones de la E.S.E. de acuerdo a la tecnología existente definirá las directrices necesarias para la aprobación de conexión de equipos de tecnología móviles tales como celulares, portátiles, tabletas y teléfonos inteligentes entre otros, a las redes de la entidad.
- d. La Entidad adopta un estándar que permite identificar los tipos de equipos pertenecientes a terceros, así como los mecanismos de control de seguridad de la información que se debe cumplir para tener acceso a la información, componentes electrónicos de procesamiento de información o servicios de tecnología de información de la Entidad.
- e. El Comité de Tecnologías de Información y Comunicaciones de la E.S.E. de acuerdo a las necesidades misionales definirá las directrices necesarias para la aprobación de actividades de teletrabajo de acuerdo a las necesidades de la Entidad, características de trabajo dentro o fuera de la Entidad, modalidades (trabajadores con contrato laboral, trabajadores independientes, trabajadores que utilizan dispositivos móviles), beneficios y obstáculos de acuerdo a la ley 1221 de 2008, al decreto 0884 de 2012, los requerimientos del subsistema de gestión de seguridad de la información de la Entidad y los resultados de los análisis de riesgos.

5.22. Política de Control de Acceso a Áreas Protegidas²⁶

- a. El Data Center debe contar con un sistema de control de acceso biométrico (huella dactilar), tarjeta de proximidad y/o clave para el ingreso de personal autorizado.
- b. Los sistemas de información, dispositivos de procesamiento y comunicaciones definidos por la Oficina de TI y/o Subgerencia Administrativa contarán con mecanismos de identificación de usuarios y procedimientos para el control de acceso a los mismos.
- c. Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad informática de la Entidad deberá estar autorizado con el respectivo control de cambios por la respectiva Oficina de TI y/o Subgerencia Administrativa.

²⁶ ISO/IEC 27001:2013 Anexo A, Ítem A.9

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.15	Fecha aprobación: 31/10/2019	
Versión: 01	PÁG. 34 de 51		



- d. Todas las conexiones remotas deberán ser autenticadas y seguras antes de conceder el acceso y el tráfico de datos deberá estar cifrado.
- e. Todo identificador de usuario establecido para un tercero o contratista, debe tener una fecha de vencimiento especificada, la cual en ningún caso debe superar la fecha de sus obligaciones contractuales.
- f. La asignación de privilegios en las aplicaciones para los diferentes identificadores de usuario estarán determinados por el Área dueña del sistema de información en la E.S.E. y aprobados por la Oficina de TI y/o Subgerencia Administrativa, y deben revisarse mínimo una vez al año; de igual forma se deben modificar o reasignar cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.²⁷
- g. Los equipos de contratistas y demás terceros que hayan sido autorizados para acceder de forma permanente a la red de la Entidad deben permanecer dentro de las respectivas instalaciones hasta la finalización del contrato o las labores para las cuales estaba definido.
- h. Los accesos a la red inalámbrica deberán ser autorizados por la respectiva Oficina de TI y/o Subgerencia Administrativa, previa verificación de que cuenten con las condiciones de seguridad, estableciendo mecanismos de control necesarios para proteger la infraestructura de la Entidad.

5.23. Política de Gestión de Activos de Información²⁸

- a. La E.S.E. tiene la custodia sobre todo dato, información y mensaje generado, procesado y contenido por sus sistemas de cómputo, así como también de todo aquello transmitido a través de su red de telecomunicaciones o cualquier otro medio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a la información.
- b. La Entidad debe identificar los activos asociados a cada sistema de información y tabla de retención documental, sus respectivos propietarios y su ubicación a fin de elaborar y mantener un inventario actualizado de los activos de información.
- c. La Entidad debe realizar la clasificación y control de activos con el objetivo de garantizar que los mismos reciban un apropiado nivel de protección, clasificar la información para señalar su sensibilidad y criticidad y definir los niveles de protección y medidas de tratamiento, evaluando las tres características de la información en las cuales se basa la Seguridad de la Información: confidencialidad, integridad y disponibilidad.

²⁷ ISO/IEC 27001:2013 Anexo A, Ítem 9.2

²⁸ ISO/IEC 27001:2013 Anexo A, Ítem 8.1

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 35 de 51	

- d. La Entidad deberá definir procedimientos para el rotulado y manejo de información de acuerdo al esquema de clasificación definido.

5.24. Política de Uso Adecuado de los Activos de Información²⁹



La información, los sistemas, las aplicaciones, los servicios y los equipos (equipos de escritorio, portátiles, impresoras, redes, Internet, dispositivos móviles, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) de todas y cada una de las dependencias de la Entidad, son activos de información que se proporcionan a los funcionarios y contratistas para cumplir con sus respectivas actividades laborales. La E.S.E. se reserva el derecho de monitorear y supervisar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en la presente política, así como en la legislación vigente.

Uso de Internet

Internet es una herramienta de trabajo que permite navegar en sitios relacionados o no con las actividades diarias, por lo cual el uso adecuado de este recurso se controla, verifica y monitorea, considerando para todos los casos, las siguientes políticas:

- a. La navegación en Internet estará controlada de acuerdo con las restricciones de navegación definidas para los usuarios en grupos, sin embargo, en ningún caso se considerarán aceptables los siguientes usos:
 - Navegación en sitio de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.
 - Publicación, envío o adquisición de material sexualmente explícito, discriminatorio, que implique un delito informático o de cualquier otro contenido que se considere fuera de los límites permitidos.
 - Publicación o envío de información confidencial sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.
 - Utilización de otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados por la Oficina de TI y/o Subgerencia Administrativa.
 - Publicación de anuncios comerciales o material publicitario, salvo la oficina de Comunicaciones cuando lo requiera. Estas solicitudes, deben ser justificadas por el jefe de la oficina de Comunicaciones y avaladas por la Gerencia.

²⁹ ISO/IEC 27001:2013 Anexo A, ítem 8.1.3



	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 38 de 51	

- Promover o mantener asuntos o negocios personales.
- Descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.
- Uso de herramientas de mensajería instantánea no autorizadas por la Oficina de TI y/o Subdirección Administrativa.
- b. Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por los funcionarios, contratistas y demás terceros autorizados. Así mismo, se puede inspeccionar, registrar e informar las actividades realizadas durante la navegación.
- c. El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.

Uso del correo electrónico



La asignación de una cuenta de correo electrónico de la E.S.E. se da como herramienta de trabajo para cada uno de los funcionarios que la requieran para el desempeño de sus funciones, así como a contratistas y otros terceros previa autorización; su uso se encuentra sujeto a las siguientes reglas:

- a. La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas en la E.S.E.
- b. Los mensajes y la información contenida en los buzones de correo son de propiedad de la Entidad y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones. Por este motivo la información y tráfico de la misma se considera de interés para la E.S.E.
- c. El tamaño de los buzones y mensajes de correo serán determinados por la Oficina de TI y/o Subgerencia Administrativa.
- d. No se considera aceptado el uso del correo electrónico de la Entidad para los siguientes fines:
 - Enviar o retransmitir cadenas de correo, mensajes con contenido racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 37 de 61	

ilícitas o promuevan actividades ilegales.

- Enviar mensajes no autorizados con contenido religioso o político.
- El envío de archivos adjuntos con extensiones como .mp3, .wav, .exe, .com, .dll, .bat, .msi o cualquier otro archivo que ponga en riesgo la Seguridad de la Información; en caso que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por la Oficina de TI.
- El envío masivo de mensajes corporativos deberá ser solicitado a Comunicaciones por el Jefe del Área que lo requiere y debe contar con la aprobación de la respectiva Oficina de TI y/o Subgerencia Administrativa.
- e. Toda información generada que requiera ser transmitida fuera de la E.S.E., y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables (PDF) y con mecanismos de seguridad (contraseñas). Sólo puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.
- f. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido y deben conservar, en todos los casos, el mensaje legal institucional de confidencialidad.
- g. Todo correo electrónico deberá tener al final del mensaje un texto en español e inglés en el que se contemplen, mínimo, los siguientes elementos:
 - El mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley.
 - El mensaje sólo puede ser utilizado por la persona o empresa a la cual está dirigido.
 - En caso de que el mensaje sea recibido por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata.
 - Prohibir la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Página 38 de 61	

Uso de Redes Inalámbricas



- a. La Oficina de TI y/o Subgerencia Administrativa será la responsable de validar a quien se le asignarán los servicios a través de redes inalámbricas, así como los perfiles, horarios, accesos y demás condiciones para la prestación del servicio a los funcionarios y contratistas en las instalaciones de la E.S.E.
- b. Los usuarios de las redes inalámbricas deben ser sometidos a las mismas condiciones de seguridad de las redes cableadas en lo que respecta identificación, autenticación, control de contenido de internet y cifrado entre otros.
- c. En ningún caso se podrá dejar configuraciones y contraseñas por defecto en los equipos inalámbricos.

Uso de Computación en la Nube

La E.S.E. podrá implementar servicios privados en la nube, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.

Sistemas de Acceso Público

- a. La información pública producida por las dependencias de la Entidad deberá estar resguardada de posibles modificaciones que afecten la imagen institucional.
- b. El portal institucional deberá contener la política de privacidad y uso, así como la política de seguridad del mismo.
- c. La Entidad deberá garantizar el derecho de Habeas Data al público que hace uso de los servicios de sus respectivos portales institucionales y propender por la Seguridad de la Información ingresada a través de ellos, aclarando que no se es responsable de la veracidad de la misma.
- d. Toda la información publicada en el portal institucional o cualquier otro medio, deberá contar con la revisión y aprobación de la Oficina de Comunicaciones.



 <p>HOSPITAL LOCAL</p>	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		 <p>TODOS JUNIOS POR LA ACREDITACIÓN</p>
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 39 de 61	

Política de Acceso y Uso de Componentes Electrónicos de Procesamiento de Información

La asignación de los diferentes recursos tecnológicos se da como herramientas de trabajo para uso exclusivo de los funcionarios y contratistas.



El uso adecuado de estos recursos se encuentra sujeto a las siguientes reglas:

- a. La E.S.E. únicamente a través del personal debidamente autorizado, instalará copias de los programas que han sido adquiridos legalmente en los equipos asignados, en las cantidades necesarias para suplir sus necesidades del servicio. El uso de programas obtenidos a partir de otras fuentes no autorizadas por la Entidad, implica riesgos legales y de seguridad de la información, por lo que dicho uso está estrictamente prohibido. Los funcionarios y contratistas de la E.S.E., reconocen y aceptan que son enteramente responsables por la utilización de software en sus estaciones de trabajo que no cuente con la respectiva autorización de la Entidad.
- b. El uso de dispositivos de almacenamiento extraíbles como DVD, CD, memorias USB, Agendas Electrónicas, celulares, tabletas y teléfonos inteligentes que no han sido debidamente autorizados por la Entidad para su uso dentro de su infraestructura tecnológica, pueden implicar riesgos de seguridad de la información cuando se conectan a los computadores. Los usuarios de estos dispositivos deben informarse de los procedimientos formales necesarios para la utilización de esos dispositivos dentro de la Entidad.
- c. El software instalado en los equipos de E.S.E. Hospital Local es de propiedad de la Entidad, la copia no autorizada del software de la Entidad o de su documentación, implica una violación a las leyes de derechos de autor y las políticas de seguridad de la información de la Entidad que será tratada mediante los mecanismos legales a los que está sujeta la E.S.E.
- d. La E.S.E. se reserva el derecho de proteger su reputación y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso y las copias no autorizadas de su software e información institucional. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas con propósitos de control interno, control de calidad, atención de incidentes de seguridad de la información o investigaciones. El usuario de equipos conectados a la

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pag.: 40 de 51	

redes de la E.S.E. reconoce y acepta que su estación de trabajo o dispositivo de comunicación puede ser analizados para evaluar el cumplimiento de las políticas de seguridad de la información de la Entidad.

- e. Los equipos de propiedad de la Entidad que se encuentren fuera de las instalaciones de la E.S.E. deben ser protegidos mediante los controles definidos por la Entidad. Los usuarios de dichos equipos se deben informar de los procedimientos formales necesarios para la utilización de esos dispositivos fuera de la Entidad.
- f. La instalación de cualquier tipo de software en los equipos de cómputo es responsabilidad exclusiva de la oficina de TI, por tanto son los únicos autorizados para realizar esta labor.
- g. Ningún activo de información adquirido y que sea configurable, debe ser instalado con la configuración por defecto del fabricante o proveedor, incluyendo cuentas y claves de administrador.
- h. Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido. Estos cambios pueden ser autorizados únicamente por la Oficina de TI.
- i. Los equipos de cómputo deberán ser bloqueados, por los usuarios que los tienen a cargo, cada vez que se retiren del puesto de trabajo.
- j. Los equipos de cómputo que no requieran realizar actividades adicionales en horario nocturno deberán ser apagados al finalizar la jornada laboral.
- k. Los requerimientos de recursos tecnológicos de las diferentes áreas deben ser avalados por la Oficina de TI.
- l. Los usuarios no deben realizar cambios físicos en las estaciones de trabajo, tales como cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física. Estas actividades sólo podrán ser autorizadas y/o realizadas por la Oficina de TI.
- m. Los equipos de cómputo asignados deben ser devueltos a la dependencia responsable una vez sean reemplazados o cuando el funcionario o contratista responsable de dicho equipo finalice su vinculación con la E.S.E.
- n. De acuerdo con el literal anterior, la Entidad no debe almacenar equipos de

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 41 de 51	



cómputo en las oficinas una vez haya cesado el uso de los mismos.

- o. Todo componente de procesamiento electrónico de la información debe servir al cumplimiento de los propósitos misionales de la Entidad, el uso por parte de personas, procesos u otros componentes electrónicos de procesamiento de la información debe someterse al uso definido por la Entidad.
- p. Todo componente electrónico de procesamiento de la información debe contar con mecanismos que permitan llevar registro y control de las solicitudes de accesos de creación, modificación, inactivación, bloqueo y eliminación de accesos autorizados al componente electrónico de procesamiento de información.
- q. Al momento de la desvinculación o cambio de roles en la Entidad, todo funcionario o contratista debe hacer entrega de todos los activos de información que le hayan sido asignados.
- r. Los siguientes usos se consideran usos no autorizados sobre componentes de procesamiento de información. Los usos no autorizados constituyen un incidente de seguridad de la información.
 - Modificación del componente sin contar con la autorización formal para dichas modificaciones
 - Uso del componente para fines diferentes a los formalmente definidos por la Entidad.
 - Impedir el acceso al componente de procesamiento de información sin justificación real.
 - Modificación o Eliminación de los controles de seguridad que protegen al componente de procesamiento de información.
 - Todas las acciones sobre el componente de procesamiento de información que sean contrarias a leyes, regulaciones, normas o procedimientos a los que está sujeta la Entidad.



5.25. Política de Protección contra Software Malicioso³⁰

- a. Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y Seguridad de la Información deberán estar protegidos mediante herramientas y software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos dados por código malicioso.

³⁰ ISO/IEC 27001:2013 Anexo A, Item 12.2.1

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 42 de 61	



- b. Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de la Oficina de TI y/o Subgerencia Administrativa, y deberán ser actualizados permanentemente.
- c. No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional.
- d. Todos los medios de almacenamiento que se conecten a equipos de la infraestructura de la Entidad deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la Seguridad de la Información.
- e. La Entidad será responsable de que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas Web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.
- f. Los sistemas, equipos e información institucionales deberán ser revisados periódicamente para verificar que no haya presencia de código malicioso.
- g. Los siguientes usos se consideran usos no autorizados del servicio de antivirus y constituyen un incidente de seguridad de la información:
- Desactivar, eliminar o modificar la configuración de los programas antivirus o de detección de software malicioso en los equipos o sistemas en que estén instalados.
 - Instalar o emplear programas de antivirus no autorizados por la Entidad.
 - Intercambiar o transmitir archivos que hayan sido identificados como infectados por el software antivirus o de detección de código malicioso o sean calificados como sospechosos de estar infectados.
 - Abrir o descargar archivos o documentos que hayan sido identificados como infectados por el software de antivirus o de detección de código malicioso o sean calificados como sospechosos de estar infectados.

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060-16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 43 de 61	

5.26. Política de Administración de Backups, Recuperación y Restauración de la Información³¹

- a. La información de los diferentes procesos, procedimientos y actividades que forman parte de las funciones de la Entidad se respalda de acuerdo a requisitos legales, nivel de clasificación, procedimiento y requerimientos de uso establecidos por la E.S.E. Hospital Local de Puerto Asís.
- b. Toda información que soporte, procesos, procedimientos o actividades definidas por la E.S.E. debe tener una definición formalmente documentada de las necesidades de respaldo de información, que debe ser aprobada por el responsable del proceso que incluya mínimo: información a respaldar, periodicidad del respaldo, nivel de clasificación de la información y período de retención de las copias de respaldo.
- c. El respaldo de la información almacenada en computadores personales, dispositivos móviles u otros medios de procesamiento de información diferentes a la infraestructura tecnológica de la E.S.E. debe ser solicitado formal y expresamente utilizando los procedimientos de soporte a usuario adoptados por la Entidad. Los responsables de la realización de las copias de respaldo evaluarán con el solicitante, la estrategia que mejor se ajuste a la solicitud considerando como mínimo: requisitos de negocio, clasificación de la información, necesidades de recuperación y medios tecnológicos disponibles.
- d. Los períodos de retención de la información respaldada se deben definir de acuerdo a los requisitos legales, objetivos de los procesos, niveles de riesgo identificados por los procesos de gestión de riesgo y retroalimentación de los usuarios y custodios de la información.
- e. Los procedimientos específicos para la realización de las copias de respaldo deben establecer los mecanismos que permitan mantener y realizar trazabilidad de la ejecución de la copia de respaldo, su resultado, responsables, medios usados, información respaldada y trazabilidad de las acciones realizadas durante la ejecución de la copia de respaldo o su restauración.
- f. Las copias de respaldo se almacenarán en sitios seguros con controles físicos y tecnológicos que permitan el cumplimiento de los estándares mínimos necesarios para preservar las copias durante los períodos definidos, limitar su acceso a los debidamente autorizados y garantizar su

³¹ ISO/IEC 27001:2013 Anexo A, Item 12.3.1

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 44 de 61	



disponibilidad cuando el responsable de la información los requiera.

- g. Las copias de respaldo se deben someter a pruebas periódicamente para certificar que cumplen con los propósitos para las cuales fueron realizadas. Los resultados se deben usar para actualizar los procedimientos de respaldo, recursos tecnológicos necesarios, evidenciar oportunidades de mejora o riesgos en la realización de copias de respaldo y restauración de información. Los responsables de la información deben participar en las pruebas para certificar formalmente que las estrategias de respaldo y restauración se ajustan a las necesidades de sus procesos.
- h. Cuando los requisitos legales, requisitos de retención o condiciones de los medios de respaldo de información así lo dictaminen, se debe proceder a la destrucción o disposición final de medio, garantizando que la información contenida en los mismos ya no será accesible.

5.27. Política de Gestión de Vulnerabilidades Técnicas³²

- a. La oficina de TI de la Entidad se encargará de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios.
- b. La Oficina de TI y/o Subgerencia Administrativa será responsable de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma tecnológica de la Entidad.
- c. No se permite a los usuarios de los activos informáticos, sin la autorización expresa de la Oficina de TI y/o Subgerencia Administrativa, realizar o participar por iniciativa propia o de terceros, en pruebas de acceso o ataques activos o pasivos a los activos informáticos de la E.S.E., o a la utilización de los mismos para efectuar pruebas de vulnerabilidad o ataques a otros equipos o sistemas externos.
- d. Los administradores de las plataformas y sistemas de información serán responsables de mantener protegida la infraestructura a su cargo de los riesgos derivados de las vulnerabilidades técnicas identificadas.
- e. El responsable de la Seguridad de la Información realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.



³² ISO/IEC 27001:2013 Anexo A, Item 12.6.1

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		 TODOS UNIDOS POR LA ACREDITACIÓN
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080-16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 45 de 51	

- f. El responsable de la Seguridad de la Información realizará una verificación de alertas de seguridad emitidas por organizaciones y foros de Seguridad de la Información de orden nacional y/o internacional, con el fin de verificar la información más reciente que se encuentre disponible respecto a vulnerabilidades y eventos de seguridad que se hayan presentado o que sean susceptibles de ocurrencia.



5.28. Política de Administración de Componentes Electrónicos de Procesamiento de Información

- a. Todos los funcionarios y contratistas de la E.S.E. Hospital Local de Puerto Asís responsables de administración de componentes de información están obligados al cumplimiento y seguimiento de esta política y demás políticas de seguridad de la información que adopta la Entidad.
- b. Las labores de administración de componentes y servicios de información y tecnología deben estar formalmente documentadas mediante procedimientos que se deben actualizar cuando se presenten cambios sobre dichos componentes o sobre los procedimientos de administración o de operación de dichos componentes o servicios.
- c. Los administradores y operadores de componentes y servicios de información y tecnología son responsables de generar, mantener, actualizar, preservar y garantizar la seguridad de la información referente a la configuración de los diversos componentes o servicios de información y tecnología.
- d. Las modificaciones a los componentes de información y tecnología de la Entidad, deben cumplir con la política de control de cambios y los procedimientos definidos por la Entidad para la gestión del cambio.
- e. Los administradores y operadores de componentes de tecnología deben reportar mediante los canales autorizados y a las instancias definidas, sin demoras injustificadas cualquier evento que pueda afectar en forma potencial o real la prestación de servicios de información y tecnología de la Entidad.
- f. El administrador de componentes o servicios de información y tecnología es responsable de garantizar y mantener un registro detallado de todos los eventos que sucedan sobre los equipos o servicios a su cargo.
- g. Los administradores y operadores de componentes de tecnología deben

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060-16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág: 48 de 51	



garantizar que los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la Entidad o ámbito de seguridad se sincronicen con una única fuente de referencia de tiempo para asegurar la consistencia de todos registros de auditoría.

- h. Los administradores de servicios y componentes de información y tecnología de la Entidad deben coordinar con los dueños de los procesos que usan los componentes y servicios de tecnología las actividades de mejoramiento de los servicios así como cualquier cambio que afecte los niveles acordados para la prestación de los servicios.
- i. Los administradores de servicios y componentes de información y tecnología de la Entidad deben coordinar con la Oficina de TI y/o Subgerencia Administrativa la implementación de todos los controles de seguridad de la información necesarios para el tratamiento de los riesgos de seguridad de la información que se identifiquen sobre los componentes o servicios a su cargo.
- j. Los administradores de servicios y componentes de información y tecnología deben incluir dentro de sus actividades de gestión mínimo:
 - Mantenimiento y aplicación de las responsabilidades para la administración y operación de componentes, sistemas o servicios a su cargo.
 - Mantenimiento y aplicación de los procedimientos necesarios autorizar las actividades de procesamiento de información sobre los componente bajo su responsabilidad.
 - Mantenimiento y aplicación de los procedimientos de operación de los equipos o servicios a su cargo.
 - Mantenimiento de los acuerdos de confidencialidad sobre la información a su cargo.
 - Mantenimiento del registro de riesgos de los componentes o servicios a su cargo.
 - Mantenimiento y aplicación de los procedimientos que se definan para el acceso de terceros a los componentes a su cargo en situaciones como mantenimiento o garantía.
 - Mantenimiento de inventario actualizado de los componentes a su cargo,

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060-16	Fecha aprobación: 31/10/2019	
Versión: 01	Pág.: 47 de 61		

así como de la configuración detallada de los mismos.

- Mantenimiento de registros del desempeño de los equipos o servicios a su cargo.
- Mantenimiento de registros que muestren las actividades realizadas por los administradores o los operadores de los equipos o servicios a su cargo.
- Mantenimiento de los registros de las fallas sobre los equipos o servicios a su cargo
- Mantenimiento de registros de los usuarios a los cuales se les ha otorgado acceso a los servicios o componentes.
- Revisión periódica de los privilegios de acceso otorgados a los usuarios de los servicios o componentes a su cargo.
- Mantenimiento y aplicación de los procedimientos definidos para asignación de cuentas de usuario y contraseñas de acceso a servicios y componentes.
- Revisión periódica de los reportes de análisis de vulnerabilidades que se realicen sobre los equipos a su cargo.
- Implementación y mantenimientos de las medidas de mitigación que se definan para contrarrestar las vulnerabilidades que se identifiquen sobre los componentes o servicios a su cargo.
- Mantenimiento y aplicación de los procedimientos de respaldo de la información contenida en los equipos a su cargo.
- Mantenimiento y prueba de los procedimientos de contingencia, recuperación ante desastres y continuidad en la prestación de servicios que se definen.
- Mantenimiento de registros sobre las actividades de atención de eventos, incidentes, problemas e incidentes de seguridad de la información que se presenten sobre los equipos o servicios a su cargo.
- Implementar y mantener los procedimientos que se definan para la asignación, actualización o retiro de los derechos de acceso de los usuarios de los componentes o servicios bajo su responsabilidad.

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTÍA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Página: 49 de 51	

- Implementación y mantenimiento de los controles de protección física lógica o procedimental que se definan para la protección de los componentes o servicios a su cargo.

5.29. Política de Adquisición de Hardware

La E.S.E. debe seleccionar metodologías para adquisición de hardware que consideren mínimo los siguientes aspectos de seguridad y control:



- Hardware compatible con IPv6.
- Garantía tanto del proveedor como del fabricante debidamente documentado.
- Soporte tanto del proveedor como del fabricante debidamente documentado.

La especificación detallada de los requerimientos de Hardware en los procesos de contratación debe incluir:

- Identificación y documentación de las funciones específicas que deben cumplir las soluciones de hardware para responder a los requerimientos de la Entidad.
- Identificación y documentación de los requerimientos de seguridad de la información para cumplir con la normatividad a la que está sujeta la Entidad.
- Identificación y documentación de requerimientos de infraestructura de información y comunicaciones para el correcto funcionamiento de la solución de hardware.
- Identificación de los acuerdos de niveles de servicio indispensables para soportar el uso de la solución de hardware.
- Identificación de cláusulas contractuales para soportar garantías y soporte.

5.30. Política de Adquisición de Software

Para la E.S.E, la adquisición de software debe cumplir con unas etapas formalmente documentadas que permitan mantener la trazabilidad de los

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1080.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 49 de 51	

requerimientos, decisiones tomadas e información recolectada para el proceso de selección y adquisición de software.

Este proceso cubre la definición de las necesidades, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de costo-beneficio y concluye con una decisión final de “desarrollar” o “comprar”³³ cuando se desarrollen proyectos.

5.31. Política de Gestión de Incidentes de Seguridad de la Información³⁴

Un incidente de seguridad de la información (“incidente”) es cualquier evento que daña o representa una amenaza seria para toda o una parte de la infraestructura de información y tecnología de la E.S.E. (sistemas de cómputo, sistemas de información, sistemas de telefonía), como pueden ser: ausencia de servicios, inhibición para el uso de sistemas de información, incluyendo cambios no autorizados al hardware, firmware, software o datos, delitos definidos en la ley 1273 de 2009 u otras normas que cobijen a la Entidad.



La política permite establecer las directrices para gestionar, dar respuesta, documentar y reportar los incidentes de seguridad de la información que afectan a la infraestructura de información y comunicaciones de la E.S.E., Los incidentes incluyen eventos como: sustracción de información, intrusión a sistemas de información, uso no autorizado de datos, denegación de servicios, violación a las políticas de uso de servicios como correo, y otras actividades contrarias a las políticas de uso adecuado de recursos de información y tecnología de la Entidad.

La política de gestión de incidentes de seguridad de la información de la E.S.E. y sus procedimientos de apoyo definen los métodos estándar para identificar, realizar seguimiento y responder a los incidentes de seguridad de la información de la Entidad:

- a. Cualquier funcionario de la E.S.E., contratista o Entidades externas deben reportar eventos relacionados con la seguridad de la información a la Oficina de TI de la E.S.E. Hospital Local. La oficina de TI por sí misma también puede identificar incidentes a través de supervisión proactiva de los sistemas de información y tecnología de la Entidad. Una vez identificado el incidente la Oficina de TI utilizará los procedimientos internos aprobados para registrar y realizar seguimiento a los incidentes y trabajar con otros funcionarios u organizaciones para tomar las acciones



³³ Proceso A11 Cobit 4.1 Identificar soluciones automatizadas.

³⁴ ISO/IEC 27001:2013 Anexo A, ítem 16

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.16	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 80 de 81	

apropiadas como investigar, escalar, remediar, referenciar el incidente a otras organizaciones como lo establecen los procedimientos de respuesta a incidentes de seguridad de la información.

- b. Cualquier dispositivo de uso personal como teléfonos inteligentes, computadores portátiles, tabletas, u otros dispositivos de cómputo que estén implicados en incidentes de seguridad pueden ser sometidos a cadena de custodia o protección para fines de investigación o evidencia ante procesos administrativos o legales. En caso de usar estos tipos de dispositivos, sus propietarios aceptan formalmente las políticas de seguridad de la E.S.E. Hospital Local de Puerto Asís.
- c. La Oficina de TI es la dependencia responsable por el aislamiento y recuperación de los accesos a sistemas de comunicaciones y cómputo afectados por el incidente. La oficina de TI debe conformar un equipo para la atención y respuesta a incidentes. De acuerdo con la naturaleza del incidente pueden ser convocados: Niveles directivos de la Entidad, áreas de control interno de la Entidad, equipos jurídicos o técnicos especializados.
- d. La oficina de TI debe garantizar que los incidentes sean apropiadamente registrados y almacenados de acuerdo con los procedimientos de control de registros del sistema integrado de gestión. Los reportes de incidentes deben ser remitidos por la oficina de TI al Comité de Sistemas de la Entidad, la Oficina de TI, son responsables de comunicar al personal pertinente las etapas y acciones que se siguen para dar respuesta al incidente.
- e. El plan de respuesta o remediación específico para un incidente pueden ser suministrado por requerimiento específico o por iniciativa de la E.S.E. a organismos de seguridad, control o respuesta a incidentes de seguridad del estado con el fin de evaluar su efectividad, solicitar apoyo, demostrar debida diligencia u otros propósitos definidos por la E.S.E.
- f. Cuando sea factible, la E.S.E. adoptará procedimientos para llevar a cabo actividades de prevención de incidentes, supervisión y filtrado de anomalías que puedan afectar a la seguridad de la información o los recursos de información y tecnología de la Entidad.
- g. La Oficina de TI mantendrá los procedimientos para la respuesta e investigación de los diferentes tipos de incidentes de seguridad de la información, así como asegurar la custodia de las evidencias obtenidas

	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE PUERTO ASÍS		
	SISTEMA OBLIGATORIO DE GARANTIA DE CALIDAD		
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
	Código: SIST-PL-1060.15	Fecha aprobación: 31/10/2019	
	Versión: 01	Pág.: 61 de 61	

durante la investigación.

- h. Los funcionarios y contratistas de la Entidad deberán informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información.
- i. Para los casos en que los incidentes reportados requieran judicialización se deberá coordinar con los organismos que cuentan con función de policía judicial.
- j. Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.
- k. El responsable de Seguridad de la Información debe propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de Seguridad de la Información.
- l. Los resultados de las investigaciones que involucren a los funcionarios de la Entidad deberán ser informados oportunamente.

CONTROL DE COPIAS Y MODIFICACIONES.

VERSION	DESCRIPCION	TIPO COPIA	AREA O SECCIÓN	FECHA DE ENTREGA	FECHA DE REVISIÓN
1	Creación de Documento	CONTROLADA	TODO	31/OCTUBRE/2019	31/OCTUBRE/2022

APROBACIÓN.

ELABORO	REVISO	APROBO	FECHA APROBACIÓN
Cristian David Cerón C Coordinador de	Cristian David Cerón Castro Coordinador de	Julio Oswaldo Quiñones Mayoral Gerente	31/OCTUBRE/2019
Luis Goral Hernández Ing. Responsables	Andrea K Delgado Romo Oficina Jurídica	Nancy Johana Peas Arriandaz Subgerente Administrativa (e)	