Hospital local Cartagena de Indias
Tejiendo Calidad de Vida

E.S.E. HOSPITAL LOCAL CARTAGENA DE INDIAS

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

GESTIÓN TECNOLOGICA Y DE SISTEMAS DE INFORMACIÓN

INTRODUCCION

La Entidad Social del Estado Hospital Local Cartagena de Indias (ESE HLCI) reconoce la información como un activo impórtate para la atención de los pacientes y el desarrollo de sus procesos internos por lo tanto, se preocupa por definir lineamientos que permitan mitigar los posibles riesgos para la información.

El presente manual contiene lineamientos que integran el sistema de gestión de seguridad de la información, las cuales deben ser adoptadas por los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la ESE HLCI, estas se encuentran enfocadas al cumplimiento de la normatividad vigente y las buenas prácticas de seguridad de la información.

OBJETIVO GENERAL

Establecer las políticas que regulan la seguridad de la información en la ESE HLCI y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los funcionarios, contratistas, personal en comisión administrativa, asistencial, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la ESE HLCI, bajo el liderazgo del área de **GESTIÓN DE LAS TELECOMUNICACIONES Y LAS TECNOLOGÍAS.**

DEFINICIONES

CONFIDENCIALIDAD:

Consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación. Este es uno de los principales problemas a los que se enfrentan muchas empresas; en los últimos años se ha incrementado el robo de los portátiles con la consecuente pérdida de información confidencial, de clientes, líneas de negocio

DISPONIBILIDAD:
La definiremos como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia. Constantemente está recibiendo consultas, descargas a su sitio web, etc., por lo que siempre deberá estar disponible para sus usuarios.

INTEGRIDAD:
Diremos que es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente. Este objetivo es muy importante cuando estamos realizando trámites bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.

ACTIVOS DE INFORMACION:
Es la base para la gestión de riesgos de seguridad de la información y para determinar los niveles de protección requeridos. Se denomina activo a aquello que tiene algún valor para FINAGRO y por tanto debe protegerse.

Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.

Los activos se encuentran asociados, de forma directa o indirectamente, con las demás entidades.

AUTENTICACION:
La palabra autenticación es utilizada para referirse a la confirmación que se realiza a través de los medios electrónicos de la identidad de un individuo o de un organismo, así como de todas sus operaciones, transacciones y documentos además de las autorías de los mismos.

INCIDENTE DE SEGURIDAD:
Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información de la información.

LICENCIA DE SOFTWARE:

La licencia de software es, la autorización que el autor o autores, que son quienes ostentan el derecho intelectual exclusivo de su obra, conceden a otros para utilizar sus obras, en este caso los programas.

Los autores, pueden otorgar distinto tipo de licencia, pueden sólo autorizar su uso, pueden autorizar su modificación o distribución, etc.

Vamos a ver los tipos de licencia de software más comunes que podemos encontrar:

- ✓ **Freeware:** Son Programas gratuitos, sin limites ni en el tiempo ni en la funcionalidad del programa. En ocasiones podremos encontrarnos programas que son freeware para uso personal, pero no podremos utilizar en el ámbito comercial.
- ✓ **Shareware y Trial:** El autor crea un software y lo distribuye a través de diferentes medios, para que el usuario pueda evaluar de forma gratuita el producto, normalmente por un tiempo especificado, aunque a veces el programa limita las opciones. Estos programas los podemos utilizar de forma gratuita, normalmente por un tiempo limitado. Una vez el periodo de prueba termina, tendremos que comprar el programa o bien lo desinstalamos, porque el programa dejará de funcionar.
- ✓ **Evaluación y Demo:** Casi igual que el Shareware, pero en la mayoría de los casos el periodo de prueba y las funcionalidades, suelen ser más limitadas.
- ✓ **Adware:** suelen ser programas shareware que de forma automática nos muestra o nos descarga publicidad a nuestro PC, a veces sólo cuando lo ejecutamos, otras simplemente cuando lo instalamos. Cuando compramos la versión registrada o la licencia, normalmente se eliminan los anuncios. Hay que estar atentos a la hora de instalarlos, pues a veces dan opción para evitar la instalación de publicidad.
- ✓ **Software libre:** aquí el autor deja libertad a los usuarios, por tanto, el programa puede ser usado, copiado, estudiado, modificado y redistribuido libremente. Pero eso no quiere decir que tenga que ser obligatoriamente gratis, podemos encontrarnos programas bajo esta licencia que son de pago, aunque suelen ser muy económicos.

SISTEMA DE INFORMACION:

Conjunto de componentes que interaccionan entre sí con el propósito de alcanzar un objetivo determinado, el cual debe satisfacer las necesidades de información de dicha empresa. Estos componentes pueden ser

actividades, recursos materiales, personas o datos, que deben además procesar la información y distribuirla de la manera más correcta para satisfacer las necesidades de la organización empresarial en cuestión.

La principal meta de un sistema de información es respaldar la toma de decisiones y gestionar todo lo que suceda en ella. Existen dos tipos de sistema de información en la empresa: los formales y los informales. Los primeros utilizan estructuras sólidas como pueden ser ordenadores, mientras que los segundos se decantan por sistemas más tradicionales y antiguos, como el boca a boca en la comunicación o el uso del papel.

SOFTWARE MALICIOSO:
El software malicioso, también conocido como programa malicioso o malware, contiene virus, spyware y otros programas indeseados que se instalan en su computadora, teléfono o aparato móvil sin su consentimiento. Estos programas pueden colapsar el funcionamiento de su aparato y se pueden utilizar para monitorear y controlar su actividad en internet. Además, con estos programas su computadora puede quedar expuesta al ataque de virus y enviar anuncios indeseados o inapropiados. Los delincuentes usan programas maliciosos para robar información personal, enviar spam y cometer fraude.

VULNERABILIDADES:
Está íntimamente relacionado con el riesgo y la amenaza y se puede definir como la debilidad o grado de exposición de un sujeto, objeto o sistema. También son aquellas fallas, omisiones o deficiencias de seguridad que puedan ser aprovechadas por los delincuentes.

DATO PÚBLICO: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

BASE DE DATOS: Conjunto organizado de datos personales que sea objeto de Tratamiento;

DATOS SENSIBLES: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales Página 3 de 16 como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los

derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
Transferencia: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

POLITICA GLOBAL DE SEGURIDAD DE LA INFORMACION

La gerencia de la **ESE HLCI**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad. Para la **ESE HCLI** la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- ✓ Minimizar el riesgo en las funciones más importantes de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de sus usuarios y empleados.
- ✓ Apoyar la innovación tecnológica.
- ✓ Proteger los activos tecnológicos.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y usuarios de **ESE HLCI**
- ✓ Garantizar la continuidad del negocio frente a incidentes.

- ✓ La **ESE HLCI** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

NIVEL DE CUMPLIMIENTO DE LA POLÍTICA

Todas las personas cubiertas por el alcance y aplicabilidad, deben dar cumplimiento del 100% de la presente política.

A continuación se establecen 12 principios de seguridad que soportan el SGSI de la **ESE HLCI**:

1. La ESE HLCI ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información (SGSI), soportado en lineamientos claros alineados a las necesidades del negocio y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades frente a la seguridad y privacidad de la información serán definidas, compartidas publicadas y aceptadas por cada uno de los empleados, contratistas o proveedores.
3. La ESE HLCI protegerá la información generada, procesada o resguardada por los procesos críticos de negocio y activos de información que hacen parte de los mismos.
4. La ESE HLCI protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. La ESE HLCI protegerá su información de las amenazas originadas por parte del personal.
6. La ESE HLCI protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. La ESE HLCI controlará la operación de sus procesos críticos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. La ESE HLCI implementará control de acceso a la información, sistemas y recursos de red.
9. La ESE HLCI garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. La ESE HLCI garantizará, a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad.
11. La ESE HLCI garantizará la disponibilidad de sus procesos críticos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
12. La ESE HLCI garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

POLITICA DE TRATAMIENTO Y PROTECCION DE DATOS

El objetivo de esta política es definir los lineamientos necesarios para la protección de datos personales e institucionales contenidos en las diferentes bases de datos de la **ESE HLCI**. La presente política es aplicable a toda base de datos que sean susceptibles de tratamiento por parte de la **ESE HLCI**, así como a toda persona que por algún motivo tenga acceso a esta información. Lo anterior, de conformidad con lo estipulado en la ley 1581 de 2012 y demás normas que la modifiquen, deroguen, sustituyan y desarrollen.

PRINCIPIOS

- ✓ **Principio de la Legalidad**: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
- ✓ **Principio de finalidad**: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
- ✓ **Principio de libertad**: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
- ✓ **Principio de veracidad o calidad**: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- ✓ **Principio de transparencia**: Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.
- ✓ **Principio de acceso y circulación restringida**: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
- ✓ **Principio de seguridad**: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- ✓ **Principio de confidencialidad**: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligados a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprenden el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

RESPONSABILIDAD

Toda persona que tenga acceso a consultar y realizar cualquier tratamiento en las bases de datos de la **ESE HLCI**, es responsable a título personal, por lo cual debe dar cumplimiento a las políticas presentes.

TRATAMIENTO DE LA INFORMACION

- ✓ Se registran los datos personales, privados, semiprivados y sensibles en las bases de datos, previa autorización del titular de la misma o de la entidad con la cual la **ESE HLCI** tenga una relación contractual.
- ✓ Se almacena en un archivo físico o electrónico.
- ✓ Se utiliza para dar cumplimiento a un mandato legal o contractual.
- ✓ La información personal almacenada será actualizada cuando sea necesario o cuando la entidad con la cual la **ESE HLCI** tena relación contractual así lo notifique.
- ✓ Se realizan copias de seguridad de las bases de datos que contienen la información personal objeto de tratamiento.
- ✓ No se comparte con ninguna entidad pública o privada con la cual no se tenga una relación contractual, exceptuando solo los casos establecidos en la ley, y para atender requerimientos judiciales o de entes de control como la superintendencia de salud, superintendencia de industria y comercio, contraloría general de la república, fiscalía general de la nación, departamento administrativo distrital de salud (DADIS)
- ✓ No se usan para ofrecer servicios o productos a terceros.
- ✓ No se usa para ninguna otra finalidad diferente a la establecida en la presente política.

FINALIDADES

- ✓ Verificación de derechos.
- ✓ Asignar o reasignación de citas, gestión de cartera, recaudo demás operaciones que se deriven del cumplimiento a lo establecido en el sistema general de seguridad social en salud.
- ✓ Entrega de reportes de salud pública de obligatorio cumplimiento.
- ✓ Emisión de respuestas a los requerimientos de las entidades de control.
- ✓ Actualización de la información personal entregada por las distintas EPS.

- ✓ Informar sobre nuevos servicios o cambios en los existentes.
- ✓ Realizar encuestas o estudios internos.

POLITICA DE CONTINUIDAD DEL NEGOCIO O DEL SISTEMA DE GESTION Y CONTINUDAD DEL NEGOCIO (SGCN)

El objetivo de la Gestión de la Continuidad de la Operación de TIC es reducir la probabilidad de interrupciones del negocio. En el caso que se produjera una interrupción, asegurar que la misma no exceda los objetivos de tiempo de recuperación y garantizar la disponibilidad de todos los recursos necesarios para la recuperación.

Esta política se rige en base a las siguientes normas:

- ✓ Norma ISO/IEC 22301 de 2012
- ✓ Norma ISO/IEC 27001:2013

ALCANCE

La Gestión de la Continuidad de la Operación de TIC se implementa para el área de Gestión tecnológica de sistemas de información de la ESE HLCI, con especial atención sobre las actividades identificadas como críticas durante el Análisis de impactos en el negocio.

La ubicación de operaciones de TIC de la ESE HLCI incluidas en este alcance es:

- Sede administrativa, pie de la popa calle nueva del toril, calle 33 # 22-54

Unidad organizativa incluida en el alcance
Gestión tecnológica de sistemas de información

PRODUCTOS Y SERVICIOS CLAVES

Los siguientes productos y servicios con críticos para el correcto funcionamiento de la operación en la entidad.

Base de datos zkmhealthmanager
Base de datos zkeseadmin

Base de datos genova
Base de datos sios
Base de datos página Web
Sistema de Información healthmanager – zkeseadmin
Conectividad
Copias de seguridad de correos electrónicos.

El área de Gestión tecnológica de sistemas de información debe garantizar que los productos mencionados se recuperaran.

RESPONSABILIDAD PARA LA GESTION DE LA CONTINUIDAD DE LA OPERACIÓN TIC.

RESPONSABILIDAD GENERAL
Gerencia: Responsable de garantizar los recursos necesarios para que se lleve a cabo la implementación de los planes de recuperación de desastres.

Coordinación de sistemas: Es el encargado de garantizar la implementación de los planes de recuperación ante desastres de acuerdo a la política.

Encargado de adoptar e implementar el plan de capacitación y Concienciación que corresponda todas las personas que cumplen una función en la gestión de la continuidad de la operación TIC.

Los preparativos relacionados con la Continuidad de la Operación de TIC deben ser probados y verificados utilizando diversos métodos para establecer hasta qué punto son accesibles, para lo cual deben contar con el visto bueno del coordinador de sistemas antes de su implementación.

El coordinador de sistemas debe asegurarse de que todos los funcionarios y/o servidores públicos y contratistas de la entidad que tengan una relación con las TIC, estén familiarizados con la política.

Proveedor de Conectividad: Es el encargado de garantizar la disponibilidad del servicio de conectividad entre centros de salud y sede administrativa.
Administrador de la Red y servidores: responsables de la implementación operativa y del mantenimiento del Sistema de Gestión de la Continuidad de la Operación de TIC.

Cada vez que se activa un plan de contingencia, un plan de recuperación ante desastres, el administrador de la red es el responsable de supervisar la eficiencia de la gestión de la continuidad de la operación de TIC.

El área de Gestión tecnológica de sistemas de información debe revisar la Gestión de los Planes de Recuperación Ante Desastres de TI al menos una vez por año o cada vez que se produzca una modificación significativa, y debe elaborar un informe de la revisión y los simulacros del mismo, una vez implementado, por lo menos dos veces al año. El objetivo de la revisión es establecer la conveniencia, adecuación y eficacia de los Planes de Recuperación de Desastres implementados, en aras de lograr la funcionalidad del Sistema de Gestión de la Continuidad de la Operación de TIC.

VALIDEZ Y GESTIÓN DE DOCUMENTOS

El propietario de este documento es el Coordinador de sistemas, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- ✓ Cantidad de funcionarios y/o servidores públicos, contratistas, terceros y proveedores que no conocen este documento.
- ✓ No-conformidad de Gestión de la Continuidad de la Operación de TIC con disposiciones legales, obligaciones contractuales y demás documentos internos de la ESE HLCI.
- ✓ Ineficacia de la implementación y mantenimiento la Gestión de la Continuidad de la Operación de TIC, se mide con base en los planes de pruebas y revisión de incidentes.
- ✓ Responsabilidades ambiguas para la implementación la Gestión de la Continuidad de la Operación de TIC.

Hospital local Cartagena de Indias
Tejiendo Calidad de Vida

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

POLÍTICA USO DE CORREO ELECTRÓNICO

Esta política aplica para todo el personal, contratista, proveedores y demás usuarios que tengan acceso a este servicio a través de los equipos de cómputo, redes o canales institucionales, contratados o de propiedad de la **ESE HLCI**

- ✓ El acceso a este servicio es otorgado por la ESE HLCI a sus funcionarios, contratistas o personal suministrado y el mismo sobrelleva responsabilidades y compromisos para su uso. Los usuarios deben conservar las normas de respeto, confidencialidad y criterio ético.
- ✓ Las partes interesadas, no podrán enviar correos internos o externos, que puedan perjudicar la imagen de la entidad. Así mismo, éstos son responsables del contenido de las comunicaciones enviadas, por lo cual se debe revisar y validar la información a enviar a través del correo electrónico institucional. Todo correo saliente debe ir con firma de pie de página del remitente sin excepción.

- ✓ En el caso de que se reciba una comunicación o correo electrónico sospechoso, de alguien desconocido o spam, debe reportarlo de inmediato, sin abrirlo, al área Gestión tecnológica de sistemas de información o al correo electrónico designado y divulgado para esta labor, que actualmente son:
- ✓ coord.sistemas@esecartagenadeindias.gov.co
- ✓ administrador@esecartagenadeindias.gov.co

- ✓ La **ESE HLCI** se reserva el derecho a monitorear, auditar y vigilar los correos electrónicos institucionales para garantizar que sea utilizado sólo para propósitos laborales, mediante una herramienta controlada en su uso por el administrador de la red, sin que tenga acceso al contenido de los mismos.
- ✓ La cuenta que no presente uso durante un periodo de tiempo superior a tres meses será desactivada automáticamente y no podrá ser accedida hasta no tramitar su reactivación al **ÁREA DE GESTIÓN TECNOLÓGICA DE SISTEMAS DE INFORMACIÓN.**
- ✓ Se encuentra disponible el acceso al correo institucional a través del sitio web de la **ESE HLCI** o ingresando en gmail.com
- ✓ El correo electrónico debe ser utilizado exclusivamente para fines laborales: para la difusión o el envío de circulares, memorandos, oficios y archivos de trabajo, cuando sea necesario en cumplimiento de las funciones asignadas.
- ✓ Los mensajes enviados a través de este servicio no pueden contener material insidioso, ofensivo, obsceno, vulgar, racista, pornográfico, subversivo u otro material no-formal.

- ✓ La información propia de la **ESE HLCI**, secretos o información sensible de la entidad no debe ser enviada por medio de canales no seguros (no codificados) como es Internet y/o las cuentas de correo de uso público (gmail, hotmail, yahoo, etc.).
- ✓ Los usuarios no pueden hacer publicaciones de los servicios de la **ESE HLCI** o de los productos de los clientes o proveedores sin el debido consentimiento escrito de los mismos.
- ✓ Los usuarios no pueden descargar, enviar, imprimir o copiar documentos o contenidos en contra de las leyes de derechos de autor.
- ✓ Los usuarios no pueden copiar ilegalmente o reenviar mensajes sin tener la autorización del remitente original para hacerlo.
- ✓ Los usuarios no pueden descargar cualquier software o archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.
- ✓ Los usuarios no pueden enviar correos SPAM de cualquier índole.
- ✓ Los usuarios no pueden usar seudónimos y enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales
- ✓ Los usuarios no pueden intentar o modificar los sistemas y parámetros de la seguridad de los sistemas de la red de la **ESE HLCI**
- ✓ Para el envió y transferencia sobre el servicio de correo electrónico se recomienda el uso del campo CCO: para mantener la privacidad de los correos electrónicos de los destinatarios. Este campo hace que los destinatarios reciban el mensaje sin aparecer en ninguna lista ni ser visibles a los demás.
- ✓ No se deben distribuir listas de direcciones de correo personales sin expresa autorización de sus dueños.
- ✓ No se permite enviar archivos con extensión .exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta, .dll debido a que este tipo de extensiones son propensas a ser utilizadas para propagación de virus. Este tipo de archivos serán eliminados automáticamente por el sistema de correo.
- ✓ No se permiten enviar contenidos multimedia (video o audio) con extensión .wav, .mp3, .mpge, .wma, .mov, .asf, .flv ya que estos documentos son muy pesados y ralentizan la red de comunicaciones. Igualmente este tipo de archivos serán eliminados automáticamente.

POLITICA USO DE INTERNET

El servicio de internet estará limitado únicamente a asuntos laborales, el uso inadecuado o abuso del servicio de internet por las partes interesadas, dará lugar a procesos sancionatorios.

A continuación se describen las políticas adoptadas para el uso adecuado de este servicio.

- ✓ El acceso a internet en horas laborales es de uso solo laboral no personal, con el fin de no saturar el ancho de banda y así poder hacer buen uso del servicio

- ✓ No acceder a páginas de entretenimiento, pornografía, terrorismo, contenido xenófobo, racista, o ilícito que atenten contra la dignidad e integridad humana.
- ✓ No descargar programas, demos, tutoriales, que no sean de apoyo para el desarrollo de las tareas diarias de cada empleado.
- ✓ Solo el área Gestión tecnológica de sistemas de información está autorizado para instalar software en los ordenadores de la entidad.
- ✓ No debe usarse el Internet para realizar llamadas internacionales (Dialpad, skipe, NET2PHONE, FREEPHONE, etc.)
- ✓ Ningún empleado debe instalar ningún programa para ver vídeos o emisoras de televisión vía Internet y de música. (Ares, REAL AUDIO, BWV, etc.).
- ✓ El uso de redes sociales está restringido dentro de la Entidad, teniendo en cuenta que esto puede generar problemas de seguridad. La **ESE HLCI** garantizara que las dependencias responsables de publicar información institucional a través de estos medios lo pueda hacer adecuadamente.
- ✓ El acceso a sitios de video, streaming o descarga de aplicaciones con extensión .iso. está restringido.
- ✓ El personal de la entidad, suministrado, contratista o visitante que requiera tener acceso a los servicios que se encuentren restringidos deben contar con la autorización de manera formal por parte de la gerencia, subgerencia o coordinación de sistemas de la **ESE HLCI.**
- ✓ El uso personal de los recursos para fines distintos a los permitidos está restringido.
- ✓ El uso para generar ganancias monetarias personales o propósitos comerciales está restringido.
- ✓ Enviar copias de documentos o inclusión de trabajos de otros en el correo electrónico como propios violando las leyes de derechos de autor. (suplantación de identidad), está restringido.
- ✓ Descargar servicios broadcast como audio y video, está restringido.
- ✓ Compartirse archivos, carpetas y otros servicios, por fuera de la entidad y sin el visto bueno del coordinador del proceso, gerencia o sistemas, está restringido.
- ✓ Usar programas “peer to peer” (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen, está restringido.
- ✓ Extender el servicio de acceso a más equipos por medio de una sola conexión a la red inalámbrica (ej: por medio de NAT, túneles, conexión compartida, DHCP, etc.) sin autorización previa de la gerencia, subgerencia o coordinación de sistemas, está restringido.
- ✓ Utilizar software de acceso remoto sin previa autorización de la coordinación de sistemas.
- ✓ Utilizar proxy para acceder a los servicios restringidos en la entidad.
- ✓ Extender el alcance de la red por medio de cualquier dispositivo físico o lógico.
- ✓ El uso del servicio para interferir o molestar a otros usuarios o entorpecer asuntos propios de la **ESE HLCI**.
- ✓ El uso del servicio para violar las políticas de uso aceptable del correo electrónico o plataformas colaborativas.

- ✓ Transgredir cualquier recurso informático, sistema o sitios de telecomunicaciones a los que no le está permitido acceder.
- ✓ Cualquier conducta que viole las normas generalmente aceptadas dentro de la **ESE HLCI**.

POLITICA PANTALLA Y ESCRITORIO LIMPIO

En aras de reducir los riesgos por el acceso no autorizado, perdida o daño de la información, la **ESE HLCI** establece las siguientes pautas para preservar la misma por medio de buenas prácticas en el manejo de documentos físicos y lógicos, USB y pantallas de los dispositivos de procesamiento de información durante y fuera de la jornada laboral.

- ✓ Cuando el usuario se retire del puesto debe bloquear su equipo estación de trabajo.
- ✓ Los equipos de cómputo estarán obligados a utilizar de protector de pantalla y fondo de pantalla el logo o imagen estipulada por la coordinación de sistemas.
- ✓ Los equipos deben contar con un usuario y contraseña.
- ✓ Los equipos que son compartidos deben contar con sesiones distintas para cada usuario.
- ✓ Los documentos que contienen información confidencial deberán ser retirados inmediatamente de la impresora, fotocopiadora o fax, por las partes interesadas responsables, no se deben dejar sin custodia o abandonadas, si esto sucede será tratado como un incidente de seguridad de la información.

POLITICA DE CONTROL DE ACCESO

Se deberá asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información. Se usará para la asignación de las credenciales de accesos a los diferentes sistemas, un formulario con el nombre del sistema, nombre usuario, contraseña temporal y la asignación de derechos al sistema y/o los servicios.

Ningún usuario podrá instalar o conectar al computador de escritorio, computador portátil y demás recursos informáticos asignados, elementos adicionales a los entregados con estos. Dichos elementos, incluyen, pero no se limitan a: cámaras web, cámaras digitales, grabadoras de sonido, impresoras, escáner, reproductores multimedia, puntos de acceso inalámbricos, dispositivos móviles, etc. En caso de requerir el uso de cualquier elemento adicional, deberá solicitar autorización al coordinador de Sistemas o al coordinador del proceso. Los usuarios no deberán usar medios de almacenamiento no autorizados para el manejo de la información, donde se

incluyen, pero no se limitan a: disquete, memorias USB, memorias flash directamente o a través de dispositivos móviles, CD's, DVD's, discos externos, que no sean de propiedad de la **ESE HLCI** y que no hayan sido entregados con fines y autorización específicos.

Uso de Contraseñas

Los usuarios deben cumplir las siguientes normas:

- ✓Mantener los datos de acceso en secreto.
- ✓Contraseñas fáciles de recordar y difíciles de adivinar.
- ✓Que las contraseñas no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
- ✓Notificar de acuerdo a lo establecido cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Equipos Desatendidos en Áreas de Usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

- ✓ Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.
- ✓ Bloquear el equipo de cómputo tras abandonar el puesto de trabajo.
- ✓ Bloqueo automático de la sesión en el equipo de cómputo tras inactividad superior a 5 minutos.
- ✓ Apagar los equipos de cómputo al finalizar la jornada laboral.

CONTROL DE ACCESO A LA RED

El área de Gestión tecnológica de sistemas de información debe asegurar el bloqueo al acceso de páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la Entidad mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. Excepciones de acceso, serán aprobados por el jefe inmediato, según la necesidad del cargo y verificación previa de que las paginas solicitadas no contengan código malicioso con el visto bueno del coordinador de sistemas.

AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS

La autenticación de usuarios remotos deberá ser aprobada por el coordinador del área, la gerencia o la subgerencia administrativa.

CONTROL DE CONEXIÓN A REDES

La infraestructura de la **ESE HLCI** deberá estar separada por Vlans para garantizar la confidencialidad de los datos que se transmitan.

SEGURIDAD EN LOS SERVICIOS DE RED

Mantener instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la entidad.

Controlar el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en el firewall de la entidad.

CONTROL DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de Usuario) solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.

CONTROL DE ACCESO POR CONTRASEÑAS

Los sistemas de información de la **ESE HLCI** y estaciones de trabajo deben utilizar usuarios y contraseñas individuales para determinar responsabilidades cuando se presenten incidentes informáticos.

Así mismo debe permitir que los usuarios seleccionen y cambien sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de las mismas o cuando consideren que la misma ha sido comprometida e incluir un procedimiento de confirmación para contemplar los errores de ingreso, también deben obligar a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información.

Igualmente no permitir mostrar las contraseñas en texto claro cuando son ingresadas y que las mismas estén cifradas.

SESIONES INACTIVAS

Si el usuario debe abandonar la estación de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que Terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

Si los sistemas de información detectan inactividad por un periodo igual o superior a treinta (30) minutos, deben automáticamente aplicar, "timeout" es decir, finalizar la sesión de usuario

LIMITACIÓN DEL TIEMPO DE CONEXIÓN

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo:

Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.

Documentar los funcionarios o contratistas que no tienen restricciones horarias y los motivos y evidencia de la autorización expedida por el coordinador de sistemas.

POLITICA RESPALDO Y COPIA DE SEGURIDAD

La **ESE HLCI** garantiza la generación continua de copias de respaldo y almacenamiento seguro de la información crítica, proporcionando los recursos para medios de respaldo adecuados y estableciendo los procedimientos y mecanismos para la realización de estas actividades de manera efectiva, con el fin de asegurar que toda la información esencial de la entidad pueda ser restaurada en caso de ser necesario.

El almacenamiento de la información de la **ESE HLCI** se debe realizar de manera interna y externa, de acuerdo a su clasificación y con previa validación del Oficial de Seguridad de la Información.

Las copias de respaldos se deben almacenar en un sitio lejano con protección física, lógica y ambiental, a una distancia suficiente para escapar a cualquier daño causado por desastres. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados y en lo posible estar certificados en la gestión de seguridad de la información.

Se recomienda usar otra locación externa o ver la viabilidad de uso de empresas en el mercado que se dedican a esto de manera segura y confiable.

Se definen procedimientos de restauración para los medios de respaldo, se verificarán y probarán trimestralmente para garantizar la disponibilidad de la información.

Nota: Actualmente los Backup se realizan de manera local en los servidores y se suben a la nube, utilizando el servicio contratado con telefónica Movistar (Azure Backup).

ESTRATEGIA DE COMUNICACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Como estrategia de comunicación y divulgación del Plan de Seguridad y Privacidad de la Información se realizara a través de inducciones generales y página web institucional www.esecartagenadeindias.gov.co para ser conocido por los funcionarios, usuarios y/o colaboradores

Elaborado por:

EDWIN JAVIER LÓPEZ CORRALES
Jefe de Oficina de IT

LUIS MARIMÓN SÁNCHEZ
Profesional Administrativo

Aprobado por:

Miembros de comité institucional de gestión y desempeño:

JORGE SUAREZ
Gerente

AURA MORENO ORTIZ
Subgerente Administrativo

EMPERATRIZ CARDOZO MEZA
Subgerente Científico

LUZ MERY CIFUENTES CALIFA
Profesional Universitario

JOSE PAZ
Director Financiero

Dando cumplimiento con el Decreto 612 del 4 de abril de 2018, "...las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión (MIPG), al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año. El área de Gestión Tecnológica y de Sistemas de Información de la ESE Hospital Local Cartagena de Indias, publica el Plan de Seguridad y Privacidad de la Información correspondiente a la vigencia 2021-2023.

Enero de 2021