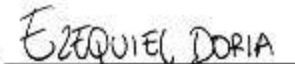
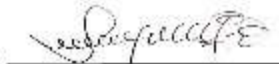


	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
			
			MODELO INTEGRADO DE PLANEACION Y GESTION
	SISTEMAS DE INFORMACION		CODIGO: SIS-INF
		PAGINA	Página 1 de 17



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2026

Elaboró: IVAN BENEDETTI R.	Revisó: EZEQUIEL DORIA LLORENTE	Aprobó: LEOANIS GONZÁLEZ MARTÍNEZ
Cargo: ING. SISTEMAS	Cargo: Planeación institucional	Cargo: Gerente
Fecha: 2026/01/24 Firma: 	Fecha: 2026/01/24 Firma: 	Fecha: 2026/01/24 Firma: 

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedeapudelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 1 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
	SISTEMAS DE INFORMACION		 MODELO INTEGRADO DE PLANEACION Y GESTION
			CODIGO: SIS-INF
		PAGINA	Página 2 de 17

Tabla de Contenido

CAPITULO I: ANALISIS SITUACIONAL DEL USO DE TECNOLOGIA EN LA ESE HOSPITAL SAN VICENTE DE PAUL.....	3
1.1. Introducción	3
1.2. Objetivos.....	3
1.3. Sistema de Red de Computadoras en la Ese Hospital San Vicente de Paul.....	4
1.4. Sistemas de Información de la Ese Hospital San Vicente de Paul.	4
CAPITULO II: PLAN DE REDUCCIÓN DE RIESGOS	5
2.1. Análisis De Riesgos.....	5
2.1.1. Valoración de los Riesgos	7
2.1.2. Riesgos.....	7
2.2. Análisis de Fallas en la Seguridad.....	12
2.3. Protecciones Actuales	13
2.3.1. Seguridad de información.....	13
2.3.2. Prevención de la seguridad.....	14
CAPITULO III: PLAN DE RESPALDO DE LA INFORMACIÓN.....	15
3.1. Actividades Previas a la seguridad	15
3.2. Plan de Acción	17

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedePauldelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 2 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
	SISTEMAS DE INFORMACION		mipg MODELO INTEGRADO DE PLANEACION Y GESTION
			CODIGO: SIS-INF
		PAGINA	Página 3 de 17

CAPITULO I: ANALISIS DE LA SITUACION ACTUAL INFORMATICA EN LA ESE HOSPITAL SAN VICENTE DE PAUL

1.1. Introducción.

Todos los Sistemas de Redes de Computadoras siempre van a estar expuestos a diferentes factores de riesgo y problemas, dichos agentes pueden llegar a ser tanto humanos como físicos. Frente a cualquier adversidad, la velocidad con que se determine la gravedad del problema depende de la capacidad y el plan a seguir para determinar con exactitud, las características principales de cada contrariedad.

A partir de diferentes fallas en componentes específicos pueden originarse pérdidas fatales, ya sea por desastres naturales o humanos que traerían consigo daños irreparables.

Este tipo de planes permiten reducir las consecuencias que se generan a partir de estos fallos y errores, y en su mayor posibilidad evitar dichos problemas, también garantizar la seguridad física de un sistema de información de datos, realizar un análisis de los riesgos, respaldo de la información y recuperación de los datos.

1.2. Objetivos.

Garantizar la continuidad de la operatividad en los diferentes procesos, de los elementos considerados críticos que componen los Sistemas de Información.

Definir actividades y procedimientos a ejecutar en caso de fallas o desastres de los elementos que componen un Sistema de Información.

Optimizar los esfuerzos y recursos necesarios para reducir los riesgos de manera oportuna y eficiente, definiendo las personas responsables de las actividades a desarrollar antes, durante y después.

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedePauldelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 3 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
	SISTEMAS DE INFORMACION		mipg MODELO INTEGRADO DE PLANEACION Y GESTION
			CODIGO: SIS-INF
		PAGINA	Página 4 de 17

1.3. Sistema de Red de Computadoras en la Ese Hospital San Vicente de Paul.

La Red de la Ese Hospital San Vicente de Paul de Loricá, no cuenta con una estructura determinada basándose en Tecnologías de la información (TI), se tiene una serie de computadores conectados entre sí con la ayuda de switches. Un sistema de información principal que es SaludSystem que maneja todo lo correspondiente a la atención de los pacientes y área financiera, que corre sobre un servidor propio de la institución. Además de este, se cuenta con un sistema de digitalización y visor de imágenes diagnósticas (RX) llamado GoTelemedicine con un servidor local alquilado, al igual que un software de manejo documental de licencia libre denominado Orfeo, en un servidor local propio.

1.4. Sistemas de Información de la Ese Hospital San Vicente de Paul.

La Ese Hospital San Vicente de Paul del municipio de Loricá cuenta con un (01) un sistema de información llamado SaludSystem desarrollado por la empresa barranquillera INFOTEC, que es básicamente en el que se manejan la parte documental de la entidad: contable, historias clínicas de pacientes, admisiones, facturación, laboratorio clínico, almacén, presupuesto, cartera y nómina.

CAPITULO 2: PLAN DE REDUCCIÓN DE RIESGOS

Se busca tener un amplio análisis de todas esas posibles causas por las cuales pueden estar expuestos los equipos de cómputo conectados a la Red de la Ese Hospital San Vicente de Paul, igualmente como todos los datos que se encuentran almacenados en los diferentes medios magnéticos de la entidad.

Se realizará un detallado Análisis de Riesgos para poder tener claridad del proceder en los diferentes casos.

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedePauldelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 4 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014  MODELO INTEGRADO DE PLANEACION Y GESTION
	SISTEMAS DE INFORMACION	CODIGO:	SIS-INF
		PAGINA	Página 5 de 17

2.1. Análisis De Riesgos

Mediante este análisis se pretende desglosar de una manera amplia los posibles riesgos que puedan afectar tanto los equipos como la información que a diario se procesa en la entidad.

Bienes susceptibles a un daño	Daño	Fuentes de Daño
Personal	Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas	Acceso no autorizado
Hardware		Ruptura de las claves de acceso a los sistemas computacionales

Software y utilitarios	Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, Proceso de información no deseado.	Desastres Naturales: a) Movimientos telúricos b) Inundaciones c) Fallas en los equipos de soporte (causadas por el ambiente, la red de energía eléctrica, no acondicionamiento atmosférico necesario)
Datos e información	Divulgación de información a instancias fuera de la	Fallas de Personal Clave: por los siguientes

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedeapudelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 5 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
	SISTEMAS DE INFORMACION		 MODELO INTEGRADO DE PLANEACION Y GESTION
			CODIGO: SIS-INF PAGINA Página 6 de 17

2.1.1. Valoración de los Riesgos

Documentación	institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia	inconvenientes: a) Enfermedad b) Accidentes c) Renuncias d) Abandono de sus puestos de trabajo e) Otros
Suministro de energía eléctrica		Fallas de Hardware: a) Falla en el Servidor Despacho (Hw) b) Falla en el hardware de Red (Switches, cableado de la Red, Router, Firewall)
Suministro de telecomunicaciones		Incendios
Segmentos de swiches en la Red LAN		Vulnerabilidad en el funcionamiento de la LAN Malas conexiones de red punto a punto

En la entidad se tendrá una valoración de cada riesgo (alto, mediano, bajo y muy bajo) y se identificarán las aplicaciones que representen mayor riesgo de la siguiente manera:

El objetivo de este ítem es determinar hasta qué grado es factible combatir los riesgos encontrados. Los riesgos que no queremos o podemos combatir se llaman riesgos restantes y no hay otra solución que aceptarlos.

Los riesgos serán medidos bajo la siguiente nomenclatura:

- Alto
- Mediano
- Bajo
- Muy bajo

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedeapudalorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 6 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
			 MODELO INTEGRADO DE PLANEACION Y GESTION
	SISTEMAS DE INFORMACION		CODIGO: SIS-INF
		PAGINA	Página 7 de 17

2.1.2. Riesgos

Para que un sistema se pueda definir como seguro, debe cumplir 3 características fundamentales:

- **Integridad:** La información solo puede ser modificada por quien está autorizado.
- **Confidencialidad:** la información solo debe ser legible para los autorizados.
- **Disponibilidad:** debe estar disponible cuando se necesita.

Son muchas las soluciones que se han desarrollado para contrarrestar el problema de disminución de los riesgos en los sistemas de información, pero en general se puede concluir que el problema de la inseguridad no ha sido resuelto, y la perspectiva que se tiene es que, es muy difícil hallar una salida debido a que las amenazas son evolutivas, a medida que crecen los métodos de contingencia, crecen y se crean nuevos mecanismos para hacer daño.

En la ESE Hospital San Vicente de Paul de Lorica se han identificado una serie de riesgos, que podrían llegar a causar detrimentos graves, tanto en los archivos como en los equipos informáticos de la entidad, dichos riesgos son:

Robo Común de Hardware e Información:

Se considera como un factor de frecuencia moderada, pero de un impacto grave, con una probabilidad de ocurrencia aleatoria, y al mismo tiempo con unas consecuencias altamente desastrosas.

Situación actual en la entidad:

La entidad cuenta con vigilancia permanente de cámaras de seguridad, se cuenta con personal de vigilancia.

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedePauldelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 7 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
	SISTEMAS DE INFORMACION		mipg MODELO INTEGRADO DE PLANEACION Y GESTION
			CODIGO: SIS-INF
		PAGINA	Página 8 de 17

La salida de los equipos informáticos es registrada por el personal de la Oficina de Despacho.

Vandalismo:

Se considera como un factor de frecuencia muy bajo, pero de un impacto grave, con una probabilidad de ocurrencia muy casual.

Situación actual en la entidad:

En la entidad actualmente este es un riesgo que no se considera que se pueda presentar, pero si ha pasado.

No se corre un peligro alto de que los equipos sean dañados con intensidad, ni que la información se pierda.

Fallas en los Equipos:

Situación actual en la entidad:

En la entidad se considera como un factor de frecuencia alto y con un impacto grave, con una probabilidad de ocurrencia muy considerable, y con unas consecuencias altamente desastrosas.

La ESE Hospital San Vicente de Paul no cuenta con un servidor que controle la red de computadores, no se cuenta con un sistema de Backups, los equipos informáticos no tienen UPS, y además se tienen muchos fallos en la Red Eléctrica ya que no existe un adecuado cableado eléctrico, debido a que las instalaciones de la ESE son antiguas.

Existe Mantenimiento tanto preventivo como correctivo de los equipos de cómputo, pero en su mayoría son dispositivos obsoletos que ya casi cumplen su ciclo de vida.

Virus Informáticos:

Para este tipo de riesgo se considera como un factor continuo de frecuencia, con un impacto grave.

Se adquirió un antivirus corporativo, asegurando la mayoría de los equipos de cómputos de la empresa, sin embargo, hay equipos que son muy pequeños en sus características y dependen de la seguridad perimetral que se posee en nuestra Vlan corporativa.

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedeapauldelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 8 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
	SISTEMAS DE INFORMACION		mipg MODELO INTEGRADO DE PLANEACION Y GESTION
			CODIGO: SIS-INF
		PAGINA	Página 9 de 17

Todos los programas y aplicativos que se instalan son manejados estrictamente por el personal encargado de Informática los cuales son instalados con su respectiva licencia.

Equivocaciones:

Las equivocaciones casi siempre son de manera involuntaria por tal razón se considera como un factor de frecuencia moderada y de probabilidad de ocurrencia moderado.

Situación actual en la entidad:

Se debe tener en consideración que al personal nuevo se debe Capacitar inicialmente para que conozca su ambiente de trabajo y dejar claro sus funciones con ayuda del Manual de Procedimiento.

Se deben convocar reuniones de capacitación, ante nuevas opciones en los sistemas o algún cambio de aplicación o al ingreso del personal nuevo.

Accesos no Autorizados:

Se considera como un factor de frecuencia aleatoria pero de un impacto grave.

Todos los usuarios deben tener un "login" o un nombre de cuenta de usuario y una clave de acceso a los equipos, esto conlleva a tener un mayor control en la información.

Situación actual en la entidad:

Algunos equipos cuentan con usuarios administrativos e invitados, pero no todos tienen esta restricción.

Cuando existe el sistema de usuarios con sus respectivos permisos, la contraseña es compartida con todos los compañeros de oficina y/o dependencia.

No se tiene un registro electrónico de Altas/Bajas de Usuarios, con las respectivas claves.

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedeapudelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 9 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
	SISTEMAS DE INFORMACION		mipg MODELO INTEGRADO DE PLANEACION Y GESTION
			CODIGO: SIS-INF
		PAGINA	Página 10 de 17

Fraude:

Se considera como un factor de media frecuencia, pero de un impacto grave, con una probabilidad de ocurrencia muy casual.

Situación actual en la entidad:

Por ser una entidad pública como su nombre lo indica la información es pública, pero puede ser utilizada para uso mal intencionados, ya que no se cuenta con restricciones en la información y cualquier funcionario o contratista tiene acceso a ella.

Fuego:

Se considera como un factor de baja frecuencia, pero de un impacto grave, con una probabilidad de ocurrencia muy casual.

Situación actual en la entidad:

La ESE Hospital San Vicente de paúl de Lorica cuenta con un sistema sencillo de prevención de incendios, basado en extintores, los cuales están ubicados estratégicamente en los pasillos de la entidad.

Se han ejecutado programas de capacitación sobre el uso de elementos de seguridad y primeros auxilios, lo que ayuda a enfrentar este tipo de situaciones y sus efectos.

Fenómenos Naturales:

Como los fenómenos naturales son eventos impredecibles, su frecuencia es aleatoria pero el impacto es muy alto dependiendo del tipo de fenómeno.

Por la zona geográfica en que se encuentra la entidad, solo podemos asociar como riesgo propenso a ocurrir, el terremoto.

Las inundaciones por causa de la lluvia no se contemplan para esta entidad ya que las instalaciones, aunque no son excelentes, se cuentan con una estructura en buen estado.

Estos riesgos explicados anteriormente los podemos clasificar según su

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedeapudelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 10 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
	SISTEMAS DE INFORMACION		 MODELO INTEGRADO DE PLANEACION Y GESTION
			CODIGO: SIS-INF PAGINA Página 11 de 17

Probabilidad de ocurrencia, de la siguiente manera:

Tipo de Riesgo	Probabilidad de Ocurrencia	Causa Controlable	Intensidad del Daño (1-10)
Segmentos con switch en la Red LAN	Alto	Si	10
Robo de hardware e información	Alto	Si	5
Vandalismo	Mediano	Si	10
Fallas en los equipos	Mediano	No	8
Virus Informáticos	Alta	Si	10
Equivocaciones	Mediano	Si	5
Accesos no autorizados	Alta	Si	5
Fraude	Bajo	Si	3
Fuego	Muy Bajo	Si	10
Fenómenos Naturales	Muy Bajo	No	10

2.2. Análisis de Fallas en la Seguridad

El estudio que se ha realizado sobre las posibles fallas en la seguridad de la información implican muchos factores en la entidad, principalmente de que en la planta de cargos de la entidad no existe un ingeniero de sistemas o una persona con conocimientos de informática, igualmente no se tiene un departamento o proceso de Sistemas de Información, razón por la cual no se cuenta con un área especializada o responsable para que maneje y lidere todo lo relacionado con información que se encuentra digitalmente y con la parte física de los equipos de cómputo.

Se maneja un inventario de Hardware y Software, por lo cual se tiene un conocimiento muy preciso de lo que posee la entidad en cuanto a equipos y programas de cómputo que necesitan licencia.

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedeapudelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 11 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
	SISTEMAS DE INFORMACION		 MODELO INTEGRADO DE PLANEACION Y GESTION
			CODIGO: SIS-INF PAGINA Página 12 de 17

La Seguridad de la Información en la Ese Hospital San Vicente de Paul de Lorica se ve fácilmente vulnerada puesto que no existe una red bien establecida y existen más de 41 dispositivos tipo concentradores (switches) en las diferentes áreas conectadas con una topología de anillo y bus, ocasionando unas caídas súbitas en cascada debido a su tipo de conexión.

La empresa tiene una red con un cableado tipo 5e lo cuales es obsoleta y el problema mayor es que hay demasiadas segmentaciones por cada área de servicio.

También tiene repetidores WIFI que hacen multiplicar direccionamiento IP conectándose equipos celulares no autorizados, que poco a poco hemos configurado con el servidor/proxy y disminuyendo ese inconveniente. Aparte que las impresoras utilizan IP e incrementa el número de dispositivos dentro de la red.

2.3. Protecciones Actuales

En la Ese Hospital San Vicente de Paul del Municipio de Lorica se realizan las siguientes protecciones:

Al Robo de Información: Algunos equipos cuentan con claves de usuario

Al Vandalismo: Se mantienen vigilancia por parte de seguridad privada en las entradas de la entidad y se cuenta con un circuito cerrado de video.

A la Protección de la Información y Equipos: el servidor principal cuenta con sistema de discos en caliente en espejo, a la base de datos principal se le realiza copia de seguridad a diario.

Fuego: se tienen instalados extintores, en sitios estratégicos y se ha brindado entrenamiento en el manejo de los extintores al personal.

Actualmente el área de sistemas posee un antivirus legal para los equipos de cómputos y seguridad perimetral directamente en el microtik de internet.

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedePauldelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 12 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
	SISTEMAS DE INFORMACION		 MODELO INTEGRADO DE PLANEACION Y GESTION
			CODIGO: SIS-INF PAGINA: Página 13 de 17

2.3.1. Seguridad de información

Para todas las empresas la información es uno de los bienes más preciados con que se cuenta, por esta razón muchas de estas no se miden en gastos en cuanto a Seguridad de la información y de los equipos informáticos, ya que este es un tema que puede llegar a afectar la imagen de cualquier institución, inclusive la vida privada de las personas.

La mejor manera de protección contra la pérdida o la modificación no autorizada de los datos de la entidad es realizar copias de seguridad (Backups), y almacenar dichas copias en un lugar seguro.

Para realizar estos Backups, se debe tener un estudio previo, que le permita definir, que sistema de Backups se va a utilizar, si es necesario utilizar algún dispositivo electrónico especializado para realizar estas copias de seguridad, con qué frecuencia se va a realizar y sobre todo cuales son los archivos a los cuales se les hará la respectiva copia, también donde se almacenaran estas copias.

La implementación de un Sistema de Backups debe ir acompañada de ciertas directrices que deben seguirse paso a paso para que su objetivo final tenga un buen resultado. Crear una política de seguridad donde se incluya la realización del Backups en el tiempo establecido y de manera obligatoria.

Estamos iniciando con un nuevo sistema de filtro de seguridad por el microtik llamado DNS-PROXY, lo cual ya está operativo.

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedePauldelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 13 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
			 MODELO INTEGRADO DE PLANEACION Y GESTION
	SISTEMAS DE INFORMACION	CODIGO:	SIS-INF
		PAGINA	Página 14 de 17

2.3.2.Prevencción de Contingencias

En este ítem se tendrá un análisis más específico de las tareas que se tienen que realizar para poder prevenir el impacto de los riesgos en caso de que alguno de estos suceda. Adicionalmente, permitirá llevar un mayor control sobre el desarrollo de las tareas de respaldo tanto de Hardware y Software en caso tal de que no se estén llevando a cabo, a fin de estar preparados cuando surja alguna eventualidad.

Tipo de Riesgo	Medida a Tomar
Robo de hardware e información	Control del personal y personas visitantes en la entidad por medio de las cámaras de seguridad. Implementar el sistema de Backups por medio de una aplicación informática.
Vandalismo	Capacitación y Evaluación al personal contratante.
Fallas en los equipos	Realizar mantenimiento preventivo, se debe realizar reposición por tiempo de vida útil, y mantenimiento preventivo en la red eléctrica. Adquirir antivirus y Firewall
Virus Informáticos	Adquirir antivirus y firewall corporativos, y actualizados.
Equivocaciones	Capacitación y Evaluación al personal, tanto como contratista como de planta.
Accesos no autorizados	En el caso de los accesos Físicos No Autorizados se deben tener letreros de advertencia, orientación al personal de visita y de planta. En el caso de accesos Lógicos No Autorizados se deben de realizar cambios de Claves de acceso periódicamente.

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedePauldelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 14 de 17	

 ESE HOSPITAL SAN VICENTE DE PAUL HTD: 580264102-7 Cra 26 No 17-124 Tel: 604-7732980 - FAX: 604-7732980 Barrio San Pedro	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014  MODELO INTEGRADO DE PLANEACION Y GESTION	
	SISTEMAS DE INFORMACION		CODIGO:	SIS-INF
			PAGINA	Página 15 de 17

Fraude	Control y Evaluación del personal a cargo de la jefatura de cada proceso.
Fuego	Se eliminaran todo tipo de material inflamable dentro de las oficinas, se debe tener una ventilación adecuada, capacitación al personal y mantenimiento preventivo a la red eléctrica para evitar cortos eléctricos.
Fenómenos Naturales	Capacitación al personal a cargo de los entes especializados en dichos casos (Bomberos, Defensa Civil, etc.) con el fin de disminuir pérdidas humanas en el momento de ocurrir estos tipos de casos.

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentededepaudelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 15 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
	SISTEMAS DE INFORMACION		mipg MODELO INTEGRADO DE PLANEACION Y GESTION
			CODIGO: SIS-INF
		PAGINA	Página 16 de 17

CAPITULO III: PLAN DE RESPALDO DE LA INFORMACIÓN

3.1. Actividades Previas a la seguridad

Vamos a definir todas las actividades de planeación, preparación, entrenamiento y ejecución de las acciones de resguardo de la información.

3.2. PLAN DE ACCION

Sistemas de Información en la entidad:

A continuación, se determinan los sistemas de información utilizados en la ESE Hospital San Vicente de Paul de Lorica, los cuales son primordiales para el correcto desarrollo de las operaciones diarias.

Actividades a Realizar para recuperar la información:

Esta es la principal razón para que la implementación de un sistema de Backups sea una realidad, porque la primera herramienta que se utiliza recuperar información es mediante la copia de seguridad que se hace en su debido tiempo periódico.

Por lo regular el Backups es almacenado en la oficina de sistemas, Estas copias de seguridad deben estar debidamente clasificadas para poder tener una rápida identificación de la información que se necesita.

Almacenamiento y Respaldos de la Información:

Se deben crear unas Políticas de Seguridad, que incluyan la forma de almacenar la información en el equipo de informática, la manera de realizar una copia de seguridad, etc.

Se debe implementar de manera urgente un sistema de Backups el cual permita de manera organizada y bien estructurada identificar la información requerida.

Prácticas Habituales:

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentedePauldelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 16 de 17	

	FORTALECIMIENTO INSTITUCIONAL		MECI 1000:2014
	SISTEMAS DE INFORMACION		mipg MODELO INTEGRADO DE PLANEACION Y GESTION
			CODIGO: SIS-INF
		PAGINA	Página 17 de 17

Dentro de las Políticas de Seguridad se tienen que incorporar recomendaciones sobre el cuidado y el aseo de los equipos de cómputo.

Y se debe poner en práctica la reposición de equipos, básicamente este proceso se lleva a cabo en tres situaciones muy particulares:

- Cuando cumple su Ciclo de Vida.
- Cuando falla el Hardware.
- Cuando exista una perdida.

Elaborado por:	CALLE 26 No 17-124 Barrio San Pedro LORICA -CORDOBA TEL: (604) 7732980 email:secretaria@esesanvicentededepaudelorica.gov.co	VERSION	001
IVAN BENEDETTI		DCTO	CONTROLADO
		Página 17 de 17	