	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL NIT: 891.180.026-5 GARZÓN - HUILA ANEXO 1: FORMATO DE IDENTIFICACIÓN DE RIESGOS PROCESOS DE APOYO					Código: D Versión: 07 Vigencia: 30/04/2017
PROCESOS DE APOYO	**OBJETIVO**	**SUBPROCESO**	**PROCEDIMIENTO**	**RIESGO**	**DESCRIPCION DEL RIESGO**	**EFECTOS O CONSECUENCIAS**
GESTIÓN SISTEMA DE INFORMACIÓN	Garantizar la administración y uso racional de los recursos asignados a tecnologías de información y operación del área de informática, sistemas en operación y en desarrollo, software, internet, redes, telecomunicaciones y seguridad física, lógica y de datos.	Seguridad Informatica	Administración del Servidor de Datos y Dominio	Daños en las fuentes redundantes del servidor por sobresaltos o pérdida de energía.	Los equipos electrónicos son vulnerablea a los cambios de voltaje de manera drástica.	Servidor fuera de servicio, la institución quedaría temporalmente sin sistema de información hasta que las fuentes sean reemplazadas o reparadas
				Perdida de información	Los discos duros tienen una vida util, la cual hace que de un momento para otro este presente fallas en el acceso de la información.	El sistemas de información perdería en el peor de los casos los datos almacenados desde el último backup realizado, siempre y cuando se dañen tres discos duros al tiempo
			Administración del firewall (Servidor ISA)	Descarga de programas no licenciados	Este procedimiento generalmente realiza instalaciones adicionales de	El equipo de computo puede quedar expuesto a software malicioso, causando
				Acceso a paginas no autorizadas	El acceso a este tipo de páginas puede ocacionar la descarga de software malicioso.	El equipo de computo puede quedar expuesto a software malicioso, causando problemas locales y en la red de computo.
				Virus informáticos	La red del Sistema de Información es altamente vulnerable a los ataques de virus informático, por el inadecuado uso de los elementos del sistema y por la falta de controles al mismo.	Colapso informático Perdida de información por ataque de virus informático, daños de software, perdida económica y de tiempo.
				Ataques de hackers	Bloqueo en el sistemas de información y/o comportamiento inusual de la red, bloqueo de servicios, cuentas de red.	Sistema de información fuera de servicio, no acceso a la red de datos.
			Copia de Respaldo de Datos de Usuarios	Perdida de información	Copias de seguridad mal elaboradas	No se va a tener las copias de respaldo para poder restaurar la base de datos con la información mas reciente, perdida de tiempo para actualizar la información a partir del último backup existente
		Gestión de Redes y Comunicaciones	Administración de Recursos de Red y Soporte en Informática	Daño en el cableado	Cable no da continuidad para la conectividad de los datos	Equipo o equipos de la institución quedarían sin servicio de red.
				Daño en equipos por usuario o por factores externos	Equipo fuera de servicio por mal manejo o maltrato.	Retrazo en los procesos institucionales que realiza el usuario final
		Gestión de Software y Hardware	Mantenimiento y Copia de respaldo de Base de Datos y Administración de Dinámica Gerencial	Indebida captura de información por parte de los usuarios del sistema.	Error de digitación al cargar la información.	Información de mala calidad en la base de datos, generando posibles datos errados en otros módulos del sistema y en reportes estadisticos.
				Errores de digitación.	Error de digitación al cargar la información.	Información de mala calidad en la base de datos, generando posibles datos errados en otros módulos del sistema y reportes estadisticos
				Falla o bloqueo del sistema	El servidor no tiene activo el servicio de SQL Server o este no se deja iniciar. El sistema genera interbloqueos en la actualización de la información.	Bloqueo en el sistema en general y/o bloqueo en los usuario que han generado el interbloqueo en la base de datos.
			Mantenimiento Preventivo y Correctivo de Hardware	Pérdida de tiempo laboral.	El mantenimiento preventivo/correctivo se demora mas de lo estimado.	Retrazo en los procesos institucionales que realiza el usuario final
				Daño definitivo del bien	Parte del equipo o equipo en total no es posible ponerlo en modo operativo.	Retrazo en los procesos institucionales que realiza el usuario final
				Demora en la ejecución de soporte.	El soporte al mantenimiento preventivo se demora demasiado.	Retrazo en los procesos institucionales que realiza el usuario final
				Reincidencia de falla en un bien	Las partes reparadas o el mantenimiento correctivo no dio el resultado esperado.	Retrazo en los procesos institucionales que realiza el usuario final

EQUIPO : OPERATIVO

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL NIT: 891.180.026-5 GARZÓN - HUILA	Código: D Versión: 07
	ANEXO 2: FORMATO ANÁLISIS Y VALORACIÓN DE RIESGOS PROCESOS DE APOYO	Vigencia: 30/04/2017

PROCESOS	RIESGO	CALIFICACIÓN		EVOLUCIÓN DEL RIESGO		MEDIDAS DE RESPUESTA
		Probabilidad ALTA = 3 MEDIA = 2 BAJA = 1	Impacto ALTO = 20 MEDIO = 10 BAJO = 5	Valoración	Zona de Riesgo	
GESTIÓN SISTEMA DE INFORMACIÓN	Daños en las fuentes redundantes del servidor por sobresaltos o pérdida de energía.	1	20	20	Moderado	Prevenir, reducir o dispersar el riesgo
	Perdida de información	1	20	20	Moderado	Prevenir, reducir o dispersar el riesgo
	Descarga de programas no licenciados	2	10	20	Moderado	Prevenir, reducir o dispersar el riesgo
	Acceso a paginas no autorizadas	1	5	5	Bajo	Asumir el riesgo
	Virus informáticos	1	20	20	Moderado	Prevenir, reducir o dispersar el riesgo
	Ataques de hackers	1	20	20	Moderado	Prevenir, reducir o dispersar el riesgo
	Perdida de información	1	20	20	Moderado	Prevenir, reducir o dispersar el riesgo
	Daño en el cableado	1	10	10	Bajo	Asumir el riesgo
	Daño en equipos por usuario o por factores externos	1	5	5	Bajo	Asumir el riesgo
	Indebida captura de información por parte de los usuarios del sistema.	1	5	5	Bajo	Asumir el riesgo
	Errores de digitación.	1	5	5	Bajo	
	Falla o bloqueo del sistema	1	20	20	Moderado	Prevenir, reducir o dispersar el riesgo
	Pérdida de tiempo laboral.	1	10	10	Bajo	Asumir el riesgo
	Daño definitivo del bien	1	10	10	Bajo	Asumir el riesgo
	Demora en la ejecución de soporte.	1	10	10	Bajo	Asumir el riesgo
	Reincidencia de falla en un bien	1	10	10	Bajo	Asumir el riesgo

Zona de Riesgo	Medidas de Respuestas
ALTO	Eliminar, reducir, compartir o transferir el riesgo
MODERADO	Prevenir, reducir o dispersar el riesgo
BAJO	Asumir el riesgo

EQUIPO: OPERATIVO

ANÁLISIS DE RIESGOS

PROBABILIDAD

ALTA	3	15	30	60	Probable o casi seguro
MEDIA	2	10	20	40	Probable o posible
BAJA	1	5	10	20	Raro o improbable
		5	10	20	
IMPACTO		BAJO	MODERADO	ALTO	
		Daño mínimo	Daño manejable	Daño catastrófico	

	EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL NIT: 891.180.026-5 GARZÓN - HUILA	Código: D
		Versión: 07
	ANEXO 3: MAPA DE RIESGOS PROCESOS DE APOYO	Vigencia: 30/04/2017

PROCESO	RIESGO	CALIFICACIÓN PROB.	CALIFICACIÓN IMPAC	EVALUACIÓN	CONTROL AL RIESGO	NUEVA CALIFICACIÓN PROB.	NUEVA CALIFICACIÓN IMPAC	NUEVA EVALUACIÓN	OPCIONES DE MANEJO	ACCIONES	RESPONSABLE	INDICADOR
GESTIÓN SISTEMA DE INFORMACIÓN	Daños en las fuentes redundantes del servidor por sobresaltos o pérdida de energía.	1	20	20	1. Instalación de UPS para el servidor y rack 2. Conexión a corriente regulada.	1	5	5	Bajo	Mantener el Control	Soporte Redes	Número Daños Suministro de Energía / Número de Días del Período a Evaluar
	Perdida de información	1	20	20	1. Actualización de licencias y parches	1	5	5	Bajo	Mantener el Control	Soporte Redes	Número de Evento de Pérdida de Información / Número de Días del Período a Evaluar
	Descarga de programas no licenciados	2	10	20	1. Restricción y monitoreo a usuario final. 2. Administración de políticas en el Firewall	1	10	10	Bajo	Mantener el Control	Soporte Redes	Número de Equipos con Software No Licenciado / Número Total de Equipos
	Acceso a paginas no autorizadas	1	5	5	1. Implementación de listas negras en el Firewall 2. Monitoreo a consultas de páginas - usuarios finales	1	5	5	Bajo	Mantener el Control	Soporte Redes	Cantidad de Equipos que acceden a Páginas No Autorizadas / Número Tota de Equipos con Acceso a Internet
	Virus informáticos	1	20	20	1. Actualización permanente del antivirus institucional 2. Actualización de los parches seguridad de Windows	1	5	5	Bajo	Mantener el Control	Soporte Redes	Cantidad de Equipos Infectados por Virus / Número total de Equipos
	Ataques de hackers	1	20	20	1. Restricción de páginas de contenido no permitido en las políticas de la ESE por medio de listas negras en el Firewall. 2. Actualización de los parches seguridad de Windows	1	10	10	Bajo	Mantener el Control	Soporte Redes	Cantidad de Ataques Hackers / Número total de equipos
	Perdida de información	1	20	20	Copia de respaldo diaria	1	5	5	Bajo	Mantener el Control	Soporte Redes	Número de Evento de Pérdida de Información / Número de Días del Período a Evaluar
	Daño en el cableado	1	10	10	Revisión periódica del cableado	1	5	5	Bajo	Mantener el Control	Soporte Redes	Cantidad de Puntos de Datos Dañados / Cantidad de Puntos de Datos Habilitados
	Daño en equipos por usuario o por factores externos	1	5	5	Solicitud de revisión por parte del usuario	1	5	5	Bajo	Mantener el Control	Soporte HelpDesk	Número de Equipos Dañados / Número Total de Equipos
	Indebida captura de información por parte de los usuarios del sistema.	1	5	5	Capacitación y/o explicación a los usuarios del modulo en el momento de detectar una inconsistencia.	1	5	5	Bajo	Mantener el Control	Soporte DGH / Soporte HelpDesk	Cantidad de Eventos de Capturas Indebidas / Número de Equipos con DGH
	Errores de digitación.	1	5	5	Solución inmediata a la solicitud de soporte del usuario.	1	5	5	Bajo	Mantener el Control	Soporte DGH / Soporte HelpDesk	Cantidad de Errores de Digitación / Cantidad de Registros del Módulo
	Falla o bloqueo del sistema	1	20	20	1. Revisión constante de los procesos del servido para prevenir bloqueos. 2. Proceso de Tunning a la base de datos.	1	5	5	Bajo	Mantener el Control	Soporte DGH / Soporte Redes	Cantidad de Fallas o Bloqueos / Número de Días del Período a Evaluar
	Pérdida de tiempo laboral.	1	10	10	Elaboración de cronograma de actividades	1	5	5	Bajo	Mantener el Control	Soporte DGH/Soporte HelpDesk/Soporte Redes	Horas perdidas en Tiempo Laboral / Cantidad de Horas Laborales en Período de Tiempo
	Daño definitivo del bien	1	10	10	Consulta a manuales técnicos de usuario	1	5	5	Bajo	Mantener el Control	Soporte HelpDesk	Cantidad de Daños Definitivos del Bien / Cantidad total de Bienes
	Demora en la ejecución de soporte.	1	10	10	Reemplazo temporal de equipos (stock de sistemas)	1	5	5	Bajo	Mantener el Control	Soporte HelpDesk	Cantidad de Soportes Demorados / Numero total de soportes registrados en Periodo de Tiempo
	Reincidencia de falla en un bien	1	10	10	Efectuar diagnostico para cambio definitivo	1	5	5	Bajo	Mantener el Control	Soporte HelpDesk	Numero de Reincidencias en Fallas en Bienes / Cantidad de Fallas en Bienes

ALTO	Eliminar, reducir, compartir o transferir el riesgo
MODERADO	Prevenir, reducir o dispersar el riesgo
BAJO	Asumir el riesgo

EQUIPO : OPERATIVO