GESTIÓN TECNOLOGICA

PLAN CONTINUIDAD DEL NEGOCIO

DICIEMBRE 01 DEL 2021

SISTEMA GESTIÓN DE CALIDAD

SANATORIO DE AGUA DE DIOS E.S.E.

TABLA DE CONTENIDO

1. OBJETIVO

Definir los roles y las actividades preventivas y correctivas, ante situaciones de emergencia, desastres o fallos inesperados, con el fin de gestionar adecuadamente los recursos disponibles (Humanos, Tecnológicos e Infraestructura), garantizando la confidencialidad, integridad y disponibilidad de la información para la continuidad en la prestación del servicio en el Sanatorio de Agua de Dios E.S.E.

1.1 OBJETIVOS ESPECIFICOS

- Definir los roles y responsabilidades para afrontar la emergencia, desastre o fallas inesperadas en el Sanatorio de Agua de Dios E.S.E.
- Identificar los procesos críticos del Sanatorio de Agua de Dios E.S.E y a partir de estos elaborar el plan de continuidad de negocio.
- Evaluar que las medidas adoptadas en el plan de Continuidad sean apropiadas para la mitigación o eliminación de los riesgos identificados en los procesos.

2. ALCANCE

El Plan de Continuidad del Negocio establece las actividades que se deben realizar por parte de los servidores públicos ante la materialización de un escenario de emergencia, desastre o falla inesperada en el Sanatorio de Agua de Dios E.S.E, para restablecer en el menor tiempo posible los procesos afectados para garantizar la prestación del servicio.

Tipo de Componente	Descripción	Tiempo de Interrupción Tolerable (RTO)
Aplicaciones	• PANACEA	24 horas ((1 día hábil)
	• Novasoft Web	72 horas (3 día hábil)
	• Orfeo	24 horas (1 día hábil)
	• Intranet (Mesa de Ayuda – Pagina intranet)	24 horas (1 día hábil)
	• Voip (Troncal Telefónica)	24 horas ((1 día hábil)
Mensajería	• Correo Electrónico (.com)	24 horas ((1 día hábil)
	• Correo Electrónico (gov.co)	8 horas (1 día Laboral)
Comunicaciones	• Corta fuegos	24 horas (1 día hábil)
	• Switch	
	• Radio Enlace con Internet	
	• Enlaces con intendencias	
Servicios	• DNS	24 horas (1 día hábil)
Infraestructura	• Sistema Eléctrico (Planta)	120 horas (1 Semana hábil)
	• Sistema Aire Acondicionado	24 horas (1 día hábil)

	• Sistema Regulado UPS	15 minutos sin ningún tipo de suministro Eléctrico

3. TERMINOS Y DEFINICIONES

EMERGENCIA: Una emergencia, en definitiva, es un suceso que exige atención inmediata ya que implica un desastre consumado o potencial. (definicion.de, 2021).

DESASTRE: Se entiende por desastre el daño grave o la alteración de las condiciones normales de vida en un área geográfica determinada, causado por fenómenos naturales y por efectos catastróficos de la acción del hombre en forma accidental, que requiera por ello de la especial atención de los organismos del estado y de otras entidades de carácter humanitario o de servicio social. (es.wikipedia.org, 2021).

ROL: El rol es el papel o función que alguien o algo representa o desempeña, por voluntad propia o por imposición. La palabra, como tal, proviene del inglés role, que significa 'papel de un actor', y este a su vez viene del francés rôle. Los roles son funciones que le son atribuidas a una persona para que, en determinadas situaciones o circunstancias, actúe o se comporte de acuerdo a un conjunto de pautas, en satisfacción de una serie de expectativas.

BCP: Sigla en inglés (Business Continuity Plan) que hace referencia al Plan de Continuidad de Negocio, el cual integra el DRP, planes de contingencia y recuperación de procesos de la entidad, planes de emergencia, y plan de comunicación y administración de crisis.

BIA: Sigla en inglés (Business Impact Analisys), y hace referencia a un documento que identifica la disponibilidad requerida de la plataforma tecnológica para soportar los procesos de la entidad, con el fin de garantizar la continuidad en la prestación del servicio a los usuarios internos y externos.

DRP: Sigla en inglés (Disaster Recovery Plan), que hace referencia al Plan de Recuperación ante Desastres de Tecnología, el cual define los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

RPO: Sigla en inglés (Recovery Point Objetive), que corresponde a la cantidad de datos o información, en términos de tiempo, que tolera perder un proceso o servicio.

RTO: Sigla en inglés (Recovery Time Objetive), que corresponde al tiempo máximo de interrupción tolerable para un proceso, servicio, proveedor, sistema de información o plataforma tecnológica.

4. ROLES Y RESPONSABILIDADES

ROL	ANTES DEL EVENTO DE INTERRUPCIÓN	DURANTE EL EVENTO DE INTERRUPCIÓN	DESPÚES DEL EVENTO DE INTERRUPCIÓN
Responsable TIC´S - DRP	✓ Elaborar y mantener actualizado el **DRP** y los recursos requeridos. ✓ Realizar la asignación y pruebas del **DRP** ✓ Gestionar la adquisición de los recursos necesarios para el **DRP**. ✓ Realizar las comunicaciones correspondientes sobre la situación de contingencia.	✓ Evaluar y activar el **DRP** y las estrategias de recuperación y contingencia. ✓ Comunicar a los coordinadores de Procesos sobre el estado de la operación de Contingencia. ✓ Informar las limitaciones al operar en contingencia en la prestación del Servicio ✓ Liderar la operación en el estado de contingencia. ✓ Comunicar a la dirección el desastre, interrupción o evento contingente. ✓ Liderar el retorno a la normalidad.	✓ Actualizar el **DRP** acorde con los inconvenientes presentados y las oportunidades de mejora identificados durante el evento de interrupción. ✓ Informar a los coordinadores de Procesos sobre el retorno a la normalidad y agradecer la comprensión y el apoyo de todos ante la situación.
Apoyo TIC'S -DRP	✓ Comunicar al responsable TIC'S - DRP las necesidades de ajuste. ✓ Participar en la ejecución de las pruebas al **DRP**.	✓ Evaluar emergencia, desastres o fallos inesperados. ✓ En caso de no contar con un contrato de mantenimiento vigente se debe tener un listado de posibles proveedores de acciones correctivas de solución. ✓ Comunicar el evento al responsable TIC'S - **DRP** ✓ Revisar disponibilidad y notificar al personal requerido para atender el incidente. ✓ Ejecutar las guías de contingencia y recuperación. ✓ Comunicar a los proveedores la activación del **DRP**. ✓ Solicitar la corrección del componente afectado y realizar seguimiento de la solución. ✓ Estar atentos para dar una correcta información a las personas que lo requieran. ✓ Mantener informado al responsable TIC´S - **DRP**	✓ Reportar los inconvenientes y oportunidades de mejora del DRP
	✓ Desarrollar actividades	✓ Proveer soporte a los	✓ Actualizar el **DRP**, de acuerdo

ROL	ANTES DEL EVENTO DE INTERRUPCIÓN	DURANTE EL EVENTO DE INTERRUPCIÓN	DESPÚES DEL EVENTO DE INTERRUPCIÓN
Responsable Seguridad	de entrenamiento, documentación y actualización del **DRP**. ✓ Coordinar las actividades de pruebas del **DRP**. ✓ Identificar los recursos requeridos para la operación del **DRP**.	profesionales especializados. ✓ Mantener informado al responsable TIC'S - DRP	con los inconvenientes y oportunidades de mejora encontrados.
Apoyo Mantenimiento	✓ Participar en la ejecución de las pruebas al **DRP**	✓ Apoyar a los involucrados del DRP, en actividades administrativas y de mantenimiento ante una contingencia. ✓ Suministro de información en contratos. ✓ Contacto de proveedores, si es requerido	✓ Reportar los inconvenientes y oportunidades de mejora del DRP

5. PLAN DE CONTINUIDAD DEL SERVICIO (BCP)

Para el desarrollo del Plan de Continuidad del Servicio en el Sanatorio de Agua de Dios E.S.E se hace necesario garantizar una serie de actividades y procedimientos mínimos con el ánimo de mantener un nivel aceptable en la prestación del servicio en la entidad.

5.1. DESARROLLO DE ESTRATEGIAS PARA LA CONTINUIDAD DEL SERVICIO.

El propósito del desarrollo de las estrategias consiste en identificar las alternativas de Recuperación de las operaciones para la prestación del servicio en Sanatorio de Agua de Dios E.S.E dentro de los tiempos definidos según su criticidad.

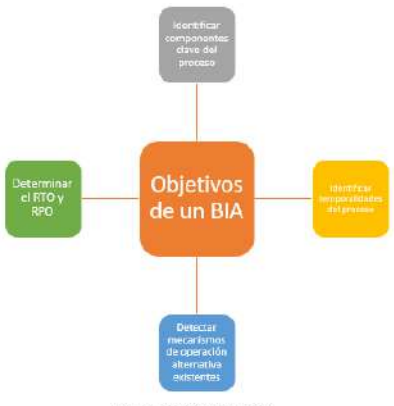


Figura 1. Objetivos de un BIA.

5.1.1. IDENTIFICAR COMPONENTES CLAVE DEL PROCESO

Se involucran todos los procesos que intervienen para la prestación del servicio en el Sanatorio de Agua de Dios E.S.E, con el fin de administrar sus recursos humanos, técnicos o administrativos en caso de presentarse una emergencia, desastre o falla inesperada y así disponer de una serie de actividades que ayuden a mitigar o eliminar el riesgo a través del seguimiento de los indicadores de riesgo, para formular las estrategias y sus responsables para la activación de los procesos de contingencia, como su divulgación en la entidad.

5.1.2. PROCEDIMIENTOS DE CONTROL

Orientado a todas las acciones necesarias para prevención o atención a la materialización de una emergencia, desastre o falla inesperada que podría llegar a poner en riesgo la continuidad en la prestación del servicio en el Sanatorio de Agua de Dios E.S.E y los canales de comunicación ante la emergencia identificada por parte de los responsables del Plan de Recuperación ante Desastres de Tecnología.

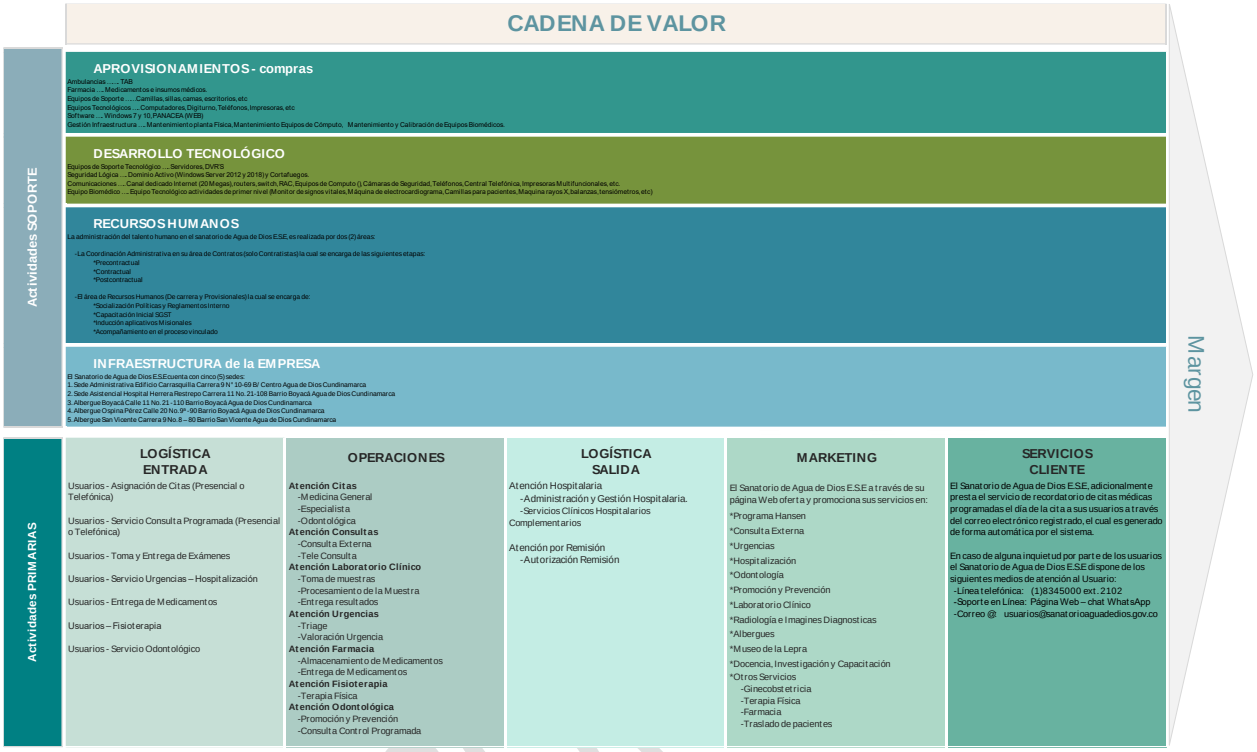
5.1.3. MECANISMOS PARA RESOLVER EMERGENCIAS

Son todas aquellas actividades que se ejecutan para mantener la prestación del servicio en el Sanatorio de Agua de Dios E.S.E, durante la emergencia, desastre o falla inesperada, garantizando niveles aceptables de calidad, es decir, la fase en la cual se activan los planes de contingencia en la entidad para poder resolver las afectaciones que generaron la situación de emergencia.

5.1.4. RESTABLECIMIENTO DEL SERVICIO

Las actividades dispuestas para recuperar la operabilidad de los servicios a su estado normal de funcionamiento una vez se han superado las situaciones que generaron la emergencia, realizando las reparaciones en los sistemas afectados o infraestructura.

6. CADENA DE VALOR



La cadena de valor del Sanatorio de Agua de Dios E.S.E es la siguiente:

Misión

El Sanatorio de Agua de Dios Empresa Social del Estado, brinda servicios integrales en salud a los pacientes con enfermedad de Hansen, además presta servicios de baja y media complejidad a la población en general, contribuyendo al fortalecimiento técnico científico en salud mediante un talento humano comprometido con el mejoramiento continuo en la prestación de servicios, garantizando la calidad de vida de sus pacientes, igualmente aporta a la preservación de la memoria histórica del desarrollo de la enfermedad de Hansen en Colombia, mediante investigaciones y soporte documental.

Visión

Para el 2022 seremos una entidad con estándares superiores de calidad en salud y reconocida a nivel nacional como ente referenciador en el diagnóstico, seguimiento y tratamiento de la enfermedad de Hansen, gestionando el conocimiento científico, comprometidos con la humanización y calidad en la atención de servicios de salud pública con énfasis en los pacientes de los programas de Hansen y Tuberculosis.

Objetivos Estratégicos

1. Consolidar el Sistema de Gestión en la entidad fortaleciendo el talento humano, el ambiente físico, la tecnología e información con énfasis en el Sistema Obligatorio de Garantía de la Calidad de la Atención en Salud SOGCS, con el fin de garantizar una atención segura, humanizada, centrada en el usuario y su familia.

2. Fortalecer el programa Hansen brindando atención integral al paciente a través de la mejora del sistema de información, la vigilancia epidemiológica y contribuyendo al diagnóstico temprano de la enfermedad.

3. Gestionar los recursos financieros en forma eficiente, mediante una adecuada planificación y ejecución de los mismos, contribuyendo al cumplimiento de las metas y políticas financieras y económicas del gobierno nacional.

4. Fortalecer las actividades técnico científicas para la investigación y capacitación en enfermedades de Hansen y Tuberculosis, teniendo como base la memoria histórica del desarrollo de la enfermedad de Hansen en Colombia.

6.1 ACTIVIDADES PRIMARIAS

- **Logística de Entrada**

  Atención Usuarios: Todo Usuario que es atendido en el Hospital Herrera Restrepo del Sanatorio de Agua de Dios E.S.E debe ser registrado en el sistema PANACEA para la gestión de historias clínicas de las siguientes formas:

  - Usuarios - Asignación de Citas (Presencial o Telefónica)
  - Usuarios - Servicio Consulta Programada (Presencial o Telefónica)
  - Usuarios - Toma y Entrega de Exámenes
  - Usuarios - Servicio Urgencias – Hospitalización
  - Usuarios - Entrega de Medicamentos
  - Usuarios – Fisioterapia
  - Usuarios - Servicio Odontológico

- **Operaciones**

Una vez el usuario ingresa al Hospital Herrera Restrepo del Sanatorio de Agua de Dios E.S.E puede seguir cualquiera de los siguientes procesos:

Atención Citas

- Medicina General
  El usuario deberá solicitar a su cita previamente según disponibilidad de agenda.

- Especialista
  El usuario deberá solicitar a su cita previamente según disponibilidad de agenda.

- Odontológica
  El usuario deberá solicitar a su cita previamente según disponibilidad de agenda.

Atención Consultas

- Consulta Externa
  El usuario deberá asistir a su cita programada previamente con mínimo diez (10) minutos de antelación para confirmar la cita en caja donde el funcionario verificará la información y procederá a facturar e informará el consultorio y nombre del médico.

  Una vez se haya facturado la cita el usuario deberá esperar al llamado del médico para su valoración y diagnóstico, de llegar a requerir exámenes, estos deberán ser solicitados por el medico en el sistema PANACEA para ser facturados.

- Tele Consulta
  Es un servicio que ofrece el Hospital Herrera Restrepo del Sanatorio de Agua de Dios E.S.E para ampliar la cobertura servicios con médicos especialistas.

Atención Laboratorio Clínico

- Toma de muestras
  El usuario deberá presentar la orden expedida por el medico de forma física en caja para facturar y luego acercarse al laboratorio clínico para la toma de muestras Autorizadas.

- Procesamiento de la Muestra
  Las muestras deberán ser marcadas con el nombre y número de cedula del usuario y clasificadas de acuerdo al tipo de examen para su posterior estudio y resultado.

- Entrega resultados
  Una vez se informe que ya están los resultados de los exámenes el usuario deberá acercarse con la cedula de ciudadanía original a reclamar los resultados.

Atención Urgencias

- Triage
  El usuario al llegar al área de urgencias es valorado por un auxiliar de enfermería el cual según los síntomas determina la gravedad de la urgencia y la clasifica de uno (1) a cinco (5) para priorizar el tiempo máximo de atención, donde uno (1) es la prioridad más baja en la cual el usuario puede esperar para ser atendido por consulta externa y cinco (5) la prioridad más alta en la cual el usuario debe ser atendido de manera inmediata. En cualquiera de los casos la información del usuario deberá ser ingresada y/o actualizada en el sistema PANACEA.

- Valoración Urgencia
  Una vez priorizado el usurario con el triage según su necesidad le será asignado un médico el cual validará previamente la información registrada en el sistema PANACEA para su atención (diagnóstico y tratamiento), el cual deberá quedar registrado en el sistema para su facturación en caja.

Atención Farmacia

- Almacenamiento de Medicamentos
  Se reciben los medicamentos y se almacenan según corresponda el medicamento (Temperatura, Humedad, Etc)

- Entrega de Medicamentos
  El usuario deberá acercarse con su respectiva formula médica a caja para realizar el copago y reclamar los medicamentos.

Atención Fisioterapia

- Terapia Física

Atención Odontológica

- Promoción y Prevención

- Consulta Control Programada

7. ANÁLISIS DEL RIESGO

CONTEXTO E IDENTIFICACIÓN DEL RIESGO

VER MATRIZ RIESGOS DE SEGURIDAD DE INFORMACION 2021

No. de Riesgo (Mismo consecutivo para toda la entidad)	Tipo de Riesgo	Clasificación del Riesgo	NOMBRE DEL RIESGO	FACTOR DEL RIESGO		VALIDACIÓN FUENTE GENERADORA DEL EVENTO PARA TIPO	RESULTADO FUENTE GENERADORA DEL EVENTO
				TIPO	SELECCIONE FUENTE GENERADORA DEL EVENTO PARA TIPO E,F,G		
R1	Perdidad de la Integridad	Seguridad de Informacion	Accesos no autorizados a aplicativos de Gestión y sistemas de información.	D_Fallas_Tecnológicas		Tecnologías	Tecnologías
R2	Perdida de la Confidenciabilidad	Seguridad de Informacion	Accesos no autorizados a infraestructura tecnológica	D_Fallas_Tecnológicas		Tecnologías	Tecnologías
R3	pérdida de la disponibilidad de los activos.	Seguridad de Informacion	Pérdida total o parcial de información	D_Fallas_Tecnológicas		Tecnologías	Tecnologías
R4	Perdidad de la Integridad	Seguridad de Informacion	Fuga o robo de Información.	C_Fraude_Interno		Talento_Humano	Talento_Humano
R5	Perdida de la Confidenciabilidad	Seguridad de Informacion	Pérdida de confidencialidad, disponibilidad y integridad de la información física.	D_Fallas_Tecnológicas		Tecnologías	Tecnologías
R6	pérdida de la disponibilidad de los activos.	Seguridad de Informacion	Destrucción de Activos de información	C_Fraude_Interno		Talento_Humano	Talento_Humano
R7	Perdidad de la Integridad	Seguridad de Informacion	Fallas técnicas de los sistemas de información y infraestructura tecnológica	C_Fraude_Interno		Talento_Humano	Talento_Humano
R8	Perdida de la Confidenciabilidad	Seguridad Digital	Ataques a la plataforma Tecnológica.	D_Fallas_Tecnológicas		Tecnologías	Tecnologías
R9	Perdida de la Confidenciabilidad	Seguridad de Informacion	Pérdida la confidencialidad,disponibilidad y integridad de la información debido a la ocurrencia de fenomenos naturales	G_Daños_Activos_Físicos	Evento_Externo		Evento_Externo
R10	pérdida de la disponibilidad de los activos.	Seguridad de Informacion	Destrucción, alterarcion de los datos, sistemas de información y documentos dentro de la Arquitectua informatica.	C_Fraude_Interno		Talento_Humano	Talento_Humano
R11	pérdida de la disponibilidad de los activos.	Seguridad Digital	Robo de Información por malware	C_Fraude_Interno		Talento_Humano	Talento_Humano
R12	Perdida de la Confidenciabilidad	Seguridad de Informacion	Pérdida de confidencialidad de la información por eliminacion	B_Fraude_Externo		Evento_Externo	Evento_Externo

FACTORES DE RIESGO	DESCRIPCIÓN

1. Tecnológicos	1.1. Accesos no autorizados a aplicativos de Gestión y sistemas de información. 1.2. Destrucción de Activos de información. 1.3. Ataques a la plataforma Tecnológica. 1.4. Fallas técnicas de los sistemas de información y/o infraestructura tecnológica. 1.5. Destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas de información 1.6. Robo de Información ocasionada por malware. 1.7. Pérdida total o parcial de información 1.8. Accesos no autorizados a infraestructura tecnológica (servidores, bases de datos, estaciones de trabajo, redes y servicios de red). 1.9. Fuga o robo de Información. 1.10. Pérdida de confidencialidad de la información por borrado o destrucción. 1.11. Pérdida de confidencialidad y/o disponibilidad y/o integridad de la información física. 1.12. Fallo en el suministro eléctrico del Sanatorio de Agua de Dios E.S.E
2. Talento Humano	2.1. Incumplimiento de los procedimientos establecidos por parte del Sanatorio de Agua de Dios E.S.E. 2.2. Comportamientos inadecuados por parte de los servidores públicos en sus áreas de trabajo.
3. Administrativos (Procedimientos)	3.1. Inexistencia de políticas de seguridad, manuales y procedimientos del servicio por parte del Sanatorio de Agua de Dios E.S.E

7.2. RIESGO EXTERNO

FACTORES DE RIESGO	DESCRIPCIÓN
1. Tecnológicos	1.13. Falla de comunicación con el proveedor del servicio de Internet para el Sanatorio de Agua de Dios E.S.E 1.14. Ataques informáticos a las plataformas del Sanatorio de Agua de Dios E.S.E por parte de expertos en informática "Hackers" (Robo, secuestro de Información y denegación del Servicio)
2. Talento Humano	2.3. Interrupción del servicio por manifestaciones o protestas por personal ajeno a la entidad. 2.4. Atentados terroristas que afecten la infraestructura ya sea física o lógica del Sanatorio de Agua de Dios E.S.E
3. Administrativos (Procedimientos)	N/A
4. Infraestructura	4.1. Pérdida de la confidencialidad y/o disponibilidad y/o integridad de la información debido a la ocurrencia de desastres naturales.

8. PROBABILIDAD DE OCURRENCIA

CÓDIGO RIESGO	PROBABILIDAD	ACCIONES	IMPACTO
1.1.	RARA VEZ	✓ El responsable de Tics establece los criterios de acceso a los usuarios del sistema de información en el sistema de información institucional de acuerdo al	MAYOR

		perfil y rol. ✓ El Coordinador y/o responsable de área revisa, verifica y ajusta los perfiles de usuario y roles en el sistema de información, de acuerdo a los accesos solicitados y autorizados. ✓ El responsable de Tics mantiene un Inventario para Control de Accesos, en el que se identifiquen los usuarios y los privilegios autorizados y denegados. el cual se revisa mensualmente, mediante verificación de log de usuarios. ✓ Los coordinadores y/o Responsables de Área implementan mecanismos para la definición de las contraseñas de acuerdo a los lineamientos establecidos por la oficina de Tics	
1.2.	POSIBLE	✓ El responsable de Tics implementa herramientas para el ingreso a las áreas restringidas mediante la utilización de control de acceso biométrico. ✓ El responsable de Tics realiza copias de respaldo de los sistemas de información mediante los planes de mantenimiento. ✓ El Profesional de Apoyo del área de Tics realiza seguimiento a los ingresos de los sistemas interno y externo mensualmente revisando posibles accesos no autorizados.	MAYOR
1.3.	POSIBLE	✓ El responsable de Tics garantiza el mantenimiento preventivo y correctivo a los contrafuegos. ✓ El Profesional de Apoyo del área de Tics realizar revisión de accesos a sitios no autorizados periódicamente y se establecen restricciones. ✓ El Profesional de Apoyo del área de Tics mantiene la plataforma antivirus actualizada periódicamente y activados los elementos de protección	CATASTROFICO
1.4.	POSIBLE	✓ El responsable de Tics garantiza la comunicación de la infraestructura mediante planes de contingencia. ✓ El Profesional de Apoyo del área de Tics realiza mantenimiento preventivo y correctivo de acuerdo al cronograma de equipos de cómputo. ✓ El Profesional de Apoyo del área de Tics	MAYOR

		realiza revisión a los equipos de comunicaciones y sistema de información periódicamente y de acuerdo a lo registrado en la mesa de ayuda.	
1.5.	IMPROBABLE	✓ El responsable de Tics realiza actualización de usuarios en el directorio activo. ✓ El responsable de Tics gestiona los usuarios de acceso a los sistemas mediante la gestión en el módulo de parametrización de perfiles y roles. ✓ El responsable de Tics implementa restricciones en el proxy de los sitios web mediante la configuración de las listas de control de acceso. ✓ El responsable de Tics implementa políticas de grupo en el Servidor para la restricción de instalación de aplicativos.	MAYOR
1.6.	POSIBLE	✓ El responsable de Tics garantiza el mantenimiento preventivo y correctivo a los contrafuegos semestralmente. ✓ El Profesional de Apoyo del área de Tics realizar revisión de accesos a sitios no autorizados periódicamente y se establecen restricciones. ✓ El Profesional de Apoyo del área de Tics mantiene la plataforma antivirus actualizada periódicamente y activados los elementos de protección.	CATASTROFICO
1.7.	POSIBLE	✓ El responsable de Tics realiza copias de seguridad mediante los planes de mantenimiento del Servicio de Base de Datos. ✓ Los Coordinadores y/o Responsables de Área realizan copias de seguridad acorde al manual establecido por el Sanatorio de Agua de Dios ESE. ✓ Los Coordinadores y/o Responsables de Área adoptan los lineamientos establecidos en la política se seguridad de la información. ✓ El responsable de Tics realiza copias de los sistemas institucionales periódicamente de acuerdo al plan de mantenimiento.	MAYOR
1.8.	IMPROBABLE	✓ El responsable de Tics gestiona los accesos a los dispositivos activos de Hardware mediante gestión de contraseñas	MAYOR

		seguras. ✓ El responsable de Tics administra los accesos a las áreas de servicios informáticos mediante los perfiles de usuarios y control automatizado. ✓ El responsable de Tics verifica mensualmente los accesos y perfiles de los usuarios.	
1.9.	IMPROBABLE	✓ El responsable de Tics realiza actualización de usuarios en el directorio activo. ✓ El responsable de Tics gestiona los usuarios de acceso a los sistemas mediante la gestión en el módulo de parametrización de perfiles y roles. ✓ El responsable de Tics implementa restricciones en el proxy de los sitios web mediante la configuración de las listas de control de acceso. ✓ El responsable de Tics implementa política de grupo en el Servidor para la restricción de instalación de aplicativos.	MAYOR
1.10.	POSIBLE	✓ El responsable de Tics realiza actualización de usuarios en el directorio activo. ✓ El responsable de Tics gestiona los usuarios de acceso a los sistemas mediante la gestión en el módulo de parametrización de perfiles y roles. ✓ El responsable de Tics implementa restricciones en el proxy de los sitios web mediante la configuración de las listas de control de acceso.	CATASTROFICO
1.11.	IMPROBABLE	✓ El responsable de Tics implementa políticas de acceso a los sistemas para salva guardar la información mediante los perfiles de usuarios y control automatizado. ✓ El responsable de Tics implementa control acceso biométrico para el acceso a áreas restringida mediante los perfiles de usuarios y control automatizado. ✓ El responsable de Tics realiza copias de los Sistemas de Información mediante planes de mantenimiento en los sistemas de Información	MAYOR
1.12.	POSIBLE	✓ Implementar sistemas de alimentación ininterrumpida (UPS), para evitar daños por	BAJA

		perdida de potencia y fluctuaciones eléctricas. ✓ Implementar un sistema de respaldo de energía eléctrica (Planta Eléctrica), que permita garantizar el suministro sin interrupciones.	
1.13.	POSIBLE	✓ Implementar servicio de conectividad de respaldo a Internet.	MODERADO
1.14.	POSIBLE	✓ El responsable de Tics garantiza el mantenimiento preventivo y correctivo a los contrafuegos. ✓ El Profesional de Apoyo del área de Tics realizar revisión de accesos a sitios no autorizados periódicamente y se establecen restricciones. ✓ El Profesional de Apoyo del área de Tics mantiene la plataforma antivirus actualizada periódicamente y activados los elementos de protección	CATASTROFICO
2.1.	POSIBLE	✓ Implementar Plan de capacitación Anual y reinducción puesto de trabajo y procedimientos.	BAJA
2.2.	POSIBLE	✓ Implementar Manual uso de Equipos	MODERADO
2.3.	POSIBLE	✓ El responsable de Tics realiza copias de seguridad mediante los planes de mantenimiento del Servicio de Base de Datos ✓ Los Coordinadores y/o Responsables de Área realizan copias de seguridad acorde al manual establecido por el Sanatorio de Agua de Dios ESE	BAJA
2.4.	POSIBLE	✓ El responsable de Tics realiza copias de seguridad mediante los planes de mantenimiento del Servicio de Base de Datos ✓ Los Coordinadores y/o Responsables de Área realizan copias de seguridad acorde al manual establecido por el Sanatorio de Agua de Dios ESE	MAYOR
3.1.	IMPROBABLE	✓ Crear Políticas y Manuales que permitan de acuerdo a la planificación de los riesgos.	MODERADO
4.1.	RARA VEZ	✓ El responsable de Tics realiza copias de seguridad mediante los planes de mantenimiento del Servicio de Base de Datos.	MAYOR

		✓ Los Coordinadores y/o Responsables de Área realizan copias de seguridad acorde al manual establecido por el Sanatorio de Agua de Dios ESE.	

9. PROBABILIDAD DE IMPACTO

VER MATRIZ RIESGOS DE SEGURIDAD DE INFORMACION 2021

MAPA DE RIESGOS SEGURIDAD DE INFORMACION

ENTIDAD:	SANATORIO DE AGUA DE DIOS ESE
PROCESO:	OFICINA TICS

				CALIFICACIÓN RIESGO RESIDUAL		
No. Riesgo	**RIESGO**	**Probabilidad Residual**	**Probabilidad Residual**	**Probabilidad**	**Impacto**	**Severidad (Nivel de Riesgo)**
R1	Accesos no autorizados a aplicativos de Gestión y sistemas de información.	4%	52%	Muy Baja	Moderado	Moderado
R2	Accesos no autorizados a infraestructura tecnológica	10%	52%	Muy Baja	Moderado	Moderado
R3	Pérdida total o parcial de información	8%	52%	Muy Baja	Moderado	Moderado
R4	Fuga o robo de Información.	5%	52%	Muy Baja	Moderado	Moderado
R5	Pérdida de confidencialidad, disponibilidad y integridad de la información física.	10%	52%	Muy Baja	Moderado	Moderado
R6	Destrucción de Activos de información	15%	52%	Muy Baja	Moderado	Moderado
R7	Fallas técnicas de los sistemas de información y infraestructura tecnológica.	25%	52%	Baja	Moderado	Moderado
R8	Ataques a la plataforma Tecnológica.	18%	65%	Muy Baja	Mayor	Alto
R9	Pérdida la confidencialidad,disponibilidad y integridad de la información debido a la ocurrencia de fenomenos naturales	10%	52%	Muy Baja	Moderado	Moderado
R10	Destrucción, alterarcion de los datos, sistemas de información y documentos dentro de la Arquitectua informatica.	5%	52%	Muy Baja	Moderado	Moderado
R11	Robo de Información por malware	11%	65%	Muy Baja	Mayor	Alto
R12	Pérdida de confidencialidad de la información por eliminacion	21%	65%	Baja	Mayor	Alto

10. MAPA DE CALOR DEL RIESGO

VER MATRIZ RIESGOS DE SEGURIDAD DE INFORMACION 2021

MAPA DE RIESGOS SEGURIDAD DE INFORMACION

ENTIDAD:	SANATORIO DE AGUA DE DIOS ESE
PROCESO:	OFICINA TICS

MAPA DE CALOR RIESGO INHERENTE

Probabilidad \ Impacto	Leve	Menor	Moderado	Mayor	Catastrófico
Muy Alta					
Alta				R3 R6 R7	R8 R11 R12
Media					
Baja				R2 R4 R5 R10	
Muy Baja				R1 R9	

MAPA DE CALOR RIESGO RESIDUAL

Probabilidad \ Impacto	Leve	Menor	Moderado	Mayor	Catastrófico
Muy Alta					
Alta					
Media					
Baja			R7	R12	
Muy Baja			R1 R2 R3 R4 R5 R6 R9 R10	R8 R11	

MAPA DE RIESGOS SEGURIDAD DE INFORMACION

ENTIDAD:	SANATORIO DE AGUA DE DIOS ESE
PROCESO:	OFICINA TICS

RIESGO INHERENTE Y RESIDUAL DEL PROCESO

Explicaciones Para realizar la ponderación de Riesgos.

1. Si en la sumatoria de los riesgos los Extremos representan mas o igual al 20% de los Riesgos, la calificación del Proceso será EXTREMO.
2. Si en la sumatoria de los riesgos Extermos y altos representan mas o igual al 30% de los Riesgos Calificados, y menos del 20% de los Riesgos Extremos la calificación del Proceso será ALTO.
3. Si en la sumatoria de los riesgos Extremos, altos y moderados representan mas o igual al 40% de los Riesgos Calificados, y menos del 30% de los Riesgos Extremos y Altos, y Menos del 20% de los Riesgos Extremos, la calificación del Proceso será MODERADO.
4. Si en la sumatoria de los riesgos Extremos, altos, moderados y bajos representan mas o igual al 50% de los Riesgos Calificados, y menos del 40% de los riesgos Extremos, altos y moderados, y menos del 30% de los riesgos calificados en Extremos y Altos, y menos del 20% de los riesgos Extremos, la calificación del proceso sera BAJO.

Nota: Adapatado de Instituto de Auditores Internos **COSO ERM** Agosto 2014

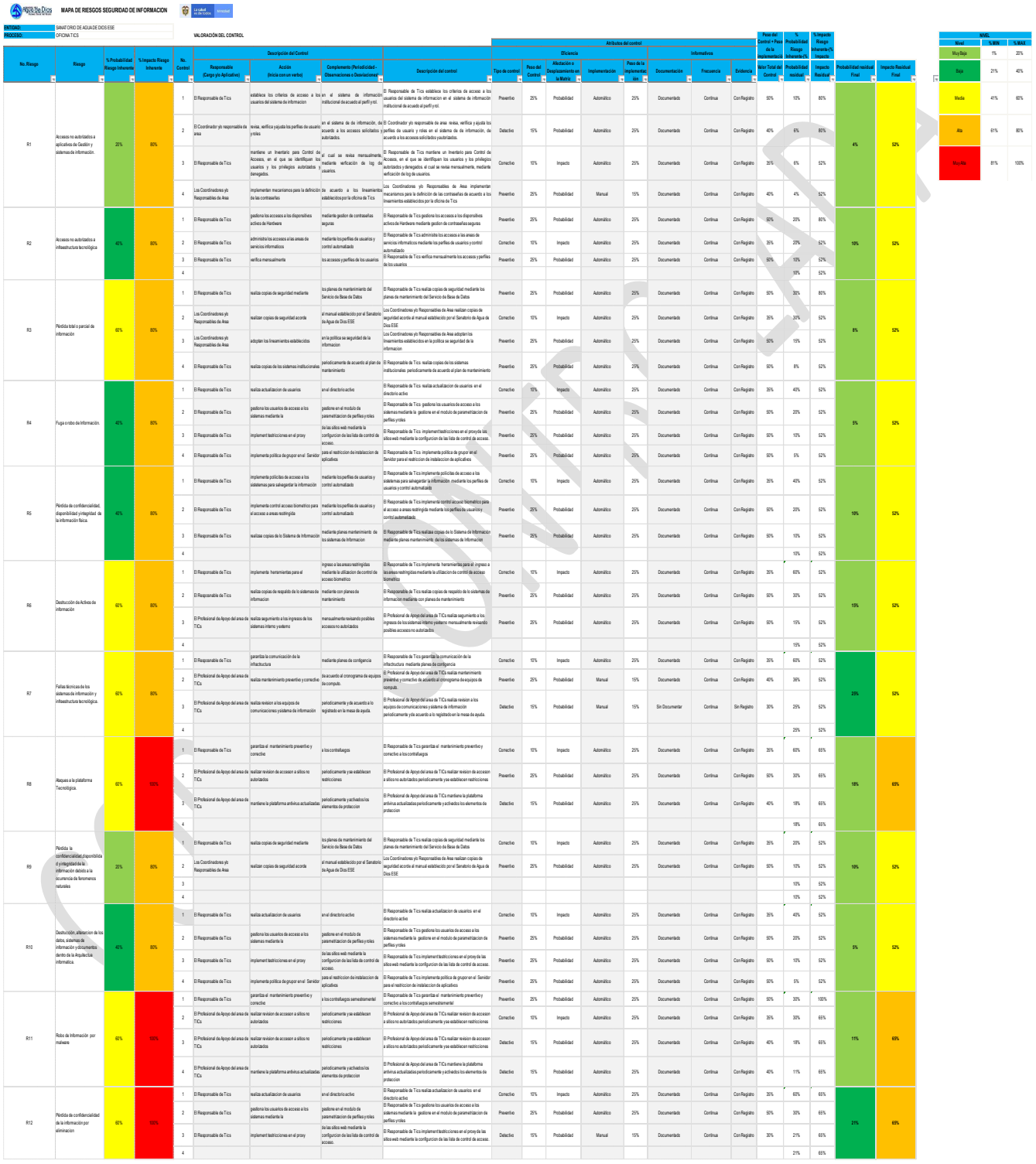
	RIESGO INHERENTE DEL PROCESO		RIESGO RESIDUAL DEL PROCESO	
Sumatoria de riesgos Extremos	3	25%	0	0%
Sumatoria de riesgos altos	9	75%	3	25%
Sumatoria de riesgos moderados	0	0%	9	75%
Sumatoria de Riesgos bajos	0	0%	0	0%
Total	12	100%	12	100%

NIVELES DE RIESGO
Extremo
Alto
Moderado
Bajo

RIESGO INHERENTE DEL PROCESO	RIESGO RESIDUAL DEL PROCESO
Extremo	Moderado

11. VALORACION Y CONTROLES

VER MATRIZ RIESGOS DE SEGURIDAD DE INFORMACION 2021



MAPA DE RIESGOS SEGURIDAD DE INFORMACION

ENTIDAD: SANATORIO DE AGUA DE DIOS ESE
PROCESO: OFICINA TICS

VALORACIÓN DEL CONTROL

No. Riesgo	Riesgo	% Probabilidad Riesgo Inherente	% Impacto Riesgo Inherente	No. Control	Descripción del Control: Responsable (Cargo y/o Aplicativo)	Descripción del Control: Acción (inicia con un verbo)	Descripción del Control: Complemento (Periodicidad - Observaciones o Desviaciones)	Descripción del control	Atributos del control: Eficiencia: Tipo de control	Eficiencia: Peso del Control	Eficiencia: Afectación o Desplazamiento en la Matriz	Eficiencia: Implementación	Eficiencia: Peso de la implementación	Informativos: Documentación	Informativos: Frecuencia	Informativos: Evidencia	Peso del Control + Peso de la implementación: Valor Total del Control	% Probabilidad Riesgo Inherente: % Probabilidad residual	% Impacto Riesgo Inherente: % Impacto Residual	Probabilidad residual Final	Impacto Residual Final
R1	Accesos no autorizados a aplicativos de Gestion y sistemas de información.	20%	80%	1	El Responsable de Tics	establece los criterios de acceso a los usuarios del sistema de informacion	en el sistema de información institucional de acuerdo al perfil y rol.	El Responsable de Tics establece los criterios de acceso a los usuarios del sistema de informacion en el sistema de información institucional de acuerdo al perfil y rol.	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	10%	80%	4%	52%
				2	El Coordinador yo responsable de area	revisa, verifica y ajusta los perfiles de usuario y roles	en el sistema de de información, de acuerdo a los accesos solicitados autorizados.	El Coordinador yo responsable de area revisa, verifica y ajusta los perfiles de usuario y roles en el sistema de de información, de acuerdo a los accesos solicitados yautorizados.	Detective	15%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	40%	6%	80%		
				3	El Responsable de Tics	mantiene un Inventario para Control de Accesos, en el que se identifiquen los usuarios y los privilegios autorizados y denegados.	el cual se revisa mensualmente, mediante verficación de log de usuarios.	El Responsable de Tics mantiene un Inventario para Control de Accesos, en el que se identifiquen los usuarios y los privilegios autorizados y denegados, el cual se revisa mensualmente, mediante verficación de log de usuarios.	Corrective	10%	Impacto	Automático	25%	Documentado	Continua	Con Registro	35%	6%	52%		
				4	Los Coordinadores yo Responsables de Area	implementan mecanismos para la definición de las contraseñas	de acuerdo a los lineamientos establecidos por la oficina de Tics	Los Coordinadores yo Responsables de Area implementan mecanismos para la definición de las contraseñas de acuerdo a los lineamientos establecidos por la oficina de Tics	Preventivo	25%	Probabilidad	Manual	15%	Documentado	Continua	Con Registro	40%	4%	52%		
R2	Accesos no autorizados a infraestructura tecnológica	40%	80%	1	El Responsable de Tics	gestiona los accesos a los dispositivos activos de Hardware	mediante gestion de contraseñas seguras	El Responsable de Tics gestiona los accesos a los dispositivos activos de Hardware mediante gestion de contraseñas seguras	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	20%	80%	10%	52%
				2	El Responsable de Tics	administra los accesos a las areas de servicios informaticos	mediante los perfiles de usuarios y control automatizado	El Responsable de Tics administra los accesos a las areas de servicios informaticos mediante los perfiles de usuarios y control automatizado	Corrective	10%	Impacto	Automático	25%	Documentado	Continua	Con Registro	35%	22%	52%		
				3	El Responsable de Tics	verifica mensualmente	los accesos y perfiles de los usuarios	El Responsable de Tics verifica mensualmente los accesos y perfiles de los usuarios	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	10%	52%		
				4														10%	52%		
R3	Perdida total o parcial de información	60%	80%	1	El Responsable de Tics	realiza copias de seguridad mediante	los planes de mantenimiento del Servicio de Base de Datos	El Responsable de Tics realiza copias de seguridad mediante los planes de mantenimiento del Servicio de Base de Datos	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	30%	80%	8%	52%
				2	Los Coordinadores yo Responsables de Area	realizan copias de seguridad acorde	al manual establecido por el Sanatorio de Agua de Dios ESE	Los Coordinadores yo Responsables de Area realizan copias de seguridad acorde al manual establecido por el Sanatorio de Agua de Dios ESE	Corrective	10%	Impacto	Automático	25%	Documentado	Continua	Con Registro	35%	32%	52%		
				3	Los Coordinadores yo Responsables de Area	adoptan los lineamientos establecidos	en la política se seguridad de la informacion	Los Coordinadores yo Responsables de Area adoptan los lineamientos establecidos en la política se seguridad de la informacion	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	15%	52%		
				4	El Responsable de Tics	realiza copias de los sistemas institucionales	periodicamente de acuerdo al plan de mantenimiento	El Responsable de Tics realiza copias de los sistemas institucionales periodicamente de acuerdo al plan de mantenimiento	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	8%	52%		
R4	Fuga o robo de Información.	40%	80%	1	El Responsable de Tics	realiza actualizacion de usuarios	en el directorio activo	El Responsable de Tics realiza actualizacion de usuarios en el directorio activo	Corrective	10%	Impacto	Automático	25%	Documentado	Continua	Con Registro	35%	40%	52%	5%	52%
				2	El Responsable de Tics	gestiona los usuarios de acceso a los sistemas mediante la	gestione en el modulo de parametrizacion de perfiles y roles	El Responsable de Tics gestiona los usuarios de acceso a los sistemas mediante la gestione en el modulo de parametrizacion de perfiles y roles	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	20%	52%		
				3	El Responsable de Tics	implement restricciones en el proxy	de las sitios web mediante la configurcion de las lista de control de acceso.	El Responsable de Tics implement lasrestricciones en el proxy de las sitios web mediante la configurcion de las lista de control de acceso.	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	10%	52%		
				4	El Responsable de Tics	implementa politica de grupor en el Servidor	para el restriccion de instalaccion de aplicativos	El Responsable de Tics implementa politica de grupor en el Servidor para el restriccion de instalaccion de aplicativos	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	5%	52%		
R5	Perdida de confidencialidad, disponibilidad yintegridad de la información física.	40%	80%	1	El Responsable de Tics	implementa policitas de acceso a los sistemas para salvegartar la información	mediante los perfiles de usuarios y control automatizado	El Responsable de Tics implementa policitas de acceso a los sistemas para salvegartar la información mediante los perfiles de usuarios y control automatizado	Corrective	10%	Impacto	Automático	25%	Documentado	Continua	Con Registro	35%	40%	52%	10%	52%
				2	El Responsable de Tics	implementa control acceso biometrico para el acceso a areas restringida	mediante los perfiles de usuarios y control automatizado	El Responsable de Tics implementa control acceso biometrico para el acceso a areas restringida mediante los perfiles de usuarios y control automatizado	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	20%	52%		
				3	El Responsable de Tics	realiza copias de lo Sistema de Informacion	mediante planes mantenimiento de los sistemas de Informacion	El Responsable de Tics realiza copias de lo Sistema de Informacion mediante planes mantenimiento de los sistemas de Informacion	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	10%	52%		
				4														10%	52%		
R6	Destrucción de Achivos de información	60%	80%	1	El Responsable de Tics	implementa herramientas para el	ingreso a las areas restringidas mediante la utilizacion de control de acceso biometrico	El Responsable de Tics implementa herramientas para el ingreso a las areas restringidas mediante la utilizacion de control de acceso biometrico	Corrective	10%	Impacto	Automático	25%	Documentado	Continua	Con Registro	35%	60%	52%	15%	52%
				2	El Responsable de Tics	realiza copias de respaldo de lo sistemas de informacion	mediante con planes de mantenimiento	El Responsable de Tics realiza copias de respaldo de lo sistemas de informacion mediante con planes de mantenimiento	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	30%	52%		
				3	El Profesional de Apoyo del area de TICs	realiza seguimiento a los ingresos de los sistemas interno y externo	mensualmente revisando posibles accesos no autorizados	El Profesional de Apoyo del area de TICs realiza seguimiento a los ingresos de los sistemas interno y externo mensualmente revisando posibles accesos no autorizados	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	15%	52%		
				4														15%	52%		
R7	Fallas técnicas de los sistemas de información y infraestructura tecnológica.	60%	80%	1	El Responsable de Tics	garantiza la comunicación de la infractructura	mediante planes de contigencia	El Responsable de Tics garantiza la comunicación de la infractructura mediante planes de contigencia	Corrective	10%	Impacto	Automático	25%	Documentado	Continua	Con Registro	35%	60%	52%	20%	52%
				2	El Profesional de Apoyo del area de TICs	realiza mantenimiento preventivo y correctivo	de acuerdo al cronograma de equipos de computo.	El Profesional de Apoyo del area de TICs realiza mantenimiento preventivo y correctivo de acuerdo al cronograma de equipos de computo.	Preventivo	25%	Probabilidad	Manual	15%	Documentado	Continua	Con Registro	40%	36%	52%		
				3	El Profesional de Apoyo del area de TICs	realiza revision a los equipos de comunicaciones y sistema de información	periodicamente y de acuerdo a lo registrado en la mesa de ayuda.	El Profesional de Apoyo del area de TICs realiza revision a los equipos de comunicaciones y sistema de información periodicamente y de acuerdo a lo registrado en la mesa de ayuda.	Detective	15%	Probabilidad	Manual	15%	Sin Documentar	Continua	Sin Registro	30%	25%	52%		
				4														25%	52%		
R8	Ataques a la plataforma Tecnológica.	60%	100%	1	El Responsable de Tics	garantiza el mantenimiento preventivo y correctivo	a los contratlagos	El Responsable de Tics garantiza el mantenimiento preventivo y correctivo a los contratlagos	Corrective	10%	Impacto	Automático	25%	Documentado	Continua	Con Registro	35%	60%	65%	18%	65%
				2	El Profesional de Apoyo del area de TICs	realiza revision de accesos a sitios no autorizados	periodicamente y se establecen restricciones	El Profesional de Apoyo del area de TICs realiza revision de accesos a sitios no autorizados periodicamente y se establecen restricciones	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	30%	65%		
				3	El Profesional de Apoyo del area de TICs	mantiene la plataforma antivirus actualizada	periodicamente y achivados los elementos de protecion	El Profesional de Apoyo del area de TICs mantiene la plataforma antivirus actualizadas periodicamente y achivados los elementos de protecion	Detective	15%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	40%	18%	65%		
				4														18%	65%		
R9	Perdida la confidencialidad,disponibilidad y integridad de la información debido a la ocurrencia de fenomenos naturales	20%	80%	1	El Responsable de Tics	realiza copias de seguridad mediante	los planes de mantenimiento del Servicio de Base de Datos	El Responsable de Tics realiza copias de seguridad mediante los planes de mantenimiento del Servicio de Base de Datos	Corrective	10%	Impacto	Automático	25%	Documentado	Continua	Con Registro	35%	20%	52%	10%	52%
				2	Los Coordinadores yo Responsables de Area	realizan copias de seguridad acorde	al manual establecido por el Sanatorio de Agua de Dios ESE	Los Coordinadores yo Responsables de Area realizan copias de seguridad acorde al manual establecido por el Sanatorio de Agua de Dios ESE	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	10%	52%		
				3														10%	52%		
				4														10%	52%		
R10	Destrucción, alteracion de los datos, sistemas de información y elmumento dentro de la Arquitectura informatica.	40%	80%	1	El Responsable de Tics	realiza actualizacion de usuarios	en el directorio activo	El Responsable de Tics realiza actualizacion de usuarios en el directorio activo	Corrective	10%	Impacto	Automático	25%	Documentado	Continua	Con Registro	35%	40%	52%	5%	52%
				2	El Responsable de Tics	gestiona los usuarios de acceso a los sistemas mediante la	gestione en el modulo de parametrizacion de perfiles y roles	El Responsable de Tics gestiona los usuarios de acceso a los sistemas mediante la gestione en el modulo de parametrizacion de perfiles y roles	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	20%	52%		
				3	El Responsable de Tics	implement restricciones en el proxy	de las sitios web mediante la configurcion de las lista de control de acceso.	El Responsable de Tics implement lasrestricciones en el proxy de las sitios web mediante la configurcion de las lista de control de acceso.	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	10%	52%		
				4	El Responsable de Tics	implementa politica de grupor en el Servidor	para el restriccion de instalaccion de aplicativos	El Responsable de Tics implementa politica de grupor en el Servidor para el restriccion de instalaccion de aplicativos	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	5%	52%		
R11	Robo de Información por malware	60%	100%	1	El Responsable de Tics	garantiza el mantenimiento preventivo y correctivo	a los contratlagos semestralmental	El Responsable de Tics garantiza el mantenimiento preventivo y correctivo a los contratlagos semestralmental	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	30%	100%	11%	65%
				2	El Profesional de Apoyo del area de TICs	realiza revision de accesos a sitios no autorizados	periodicamente y se establecen restricciones	El Profesional de Apoyo del area de TICs realiza revision de accesos a sitios no autorizados periodicamente y se establecen restricciones	Corrective	10%	Impacto	Automático	25%	Documentado	Continua	Con Registro	35%	30%	65%		
				3	El Profesional de Apoyo del area de TICs	realiza revision de accesos a sitios no autorizados	periodicamente y se establecen restricciones	El Profesional de Apoyo del area de TICs realiza revision de accesos a sitios no autorizados periodicamente y se establecen restricciones	Detective	15%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	40%	18%	65%		
				4	El Profesional de Apoyo del area de TICs	mantiene la plataforma antivirus actualizada	periodicamente y achivados los elementos de protecion	El Profesional de Apoyo del area de TICs mantiene la plataforma antivirus actualizadas periodicamente y achivados los elementos de protecion	Detective	15%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	40%	11%	65%		
R12	Perdida de confidencialidad de la información por eliminacion	60%	100%	1	El Responsable de Tics	realiza actualizacion de usuarios	en el directorio activo	El Responsable de Tics realiza actualizacion de usuarios en el directorio activo	Corrective	10%	Impacto	Automático	25%	Documentado	Continua	Con Registro	35%	60%	65%	21%	65%
				2	El Responsable de Tics	gestiona los usuarios de acceso a los sistemas mediante la	gestione en el modulo de parametrizacion de perfiles y roles	El Responsable de Tics gestiona los usuarios de acceso a los sistemas mediante la gestione en el modulo de parametrizacion de perfiles y roles	Preventivo	25%	Probabilidad	Automático	25%	Documentado	Continua	Con Registro	50%	30%	65%		
				3	El Responsable de Tics	implement restricciones en el proxy	de las sitios web mediante la configurcion de las lista de control de acceso.	El Responsable de Tics implement lasrestricciones en el proxy de las sitios web mediante la configurcion de las lista de control de acceso.	Detective	15%	Probabilidad	Manual	15%	Documentado	Continua	Con Registro	30%	21%	65%		
				4														21%	65%		

NIVEL	% MIN	% MAX
Muy Baja	1%	20%
Baja	21%	40%
Media	41%	60%
Alta	61%	80%
Muy Alta	81%	100%

12. ESTRATEGIA DE CONTINUIDAD

ESCENARIO DE INTERRUPCION	AMENAZAS	CONTINGENCIA
 NO DISPONIBILIDAD DE LOS SERVICIOS TECNOLÓGICOS	1) Fallas en el sistema de Información. 2) Fallas de conectividad: • Hardware • Base de Datos • Software 3) Falla Eléctrica. 4) Falla conexión Internet	1) Implementación estrategia DRP y los procesos se llevarán de manera manual hasta restablecer el sistema. 2) Implementación estrategia DRP Canal de Backup del canal principal 3) Implementación estrategia DRP suministro eléctrico a través de la planta Eléctrica hasta por una semana. 4) Implementación estrategia DRP Cambio del canal Principal a canal de Respaldo.
 NO DISPONIBILIDAD DE LA INFRAESTRUCTURA FÍSICA	1) Incendio 2) Desastres Naturales: • Inundaciones • Terremotos 3) Actos vandálicos	1) Restablecimiento de servicios en las diferentes sedes con que cuenta la entidad. 2) Convenios con otras entidades de Salud. 3) Trabajo en Casa
 NO DISPONIBILIDAD DE INFORMACIÓN	1) Falla Eléctrica 2) Desastres Naturales 3) Fallas de conectividad: • Hardware • Base de Datos • Software	1) Restablecimiento de las copias de seguridad (Backup) de los sistemas de información. 2) Herramientas alternas de comunicación (WhatsApp, Usb; etc)
 NO DISPONIBILIDAD DE COLABORADORES DEL PROCESO	1) Incapacidades Medicas 2) Huelgas de Trabajadores 3) Retiro o Muerte de Trabajadores 4) Pandemias	1) Arboles de llamadas 2) Rotación de los Trabajadores 3) Capacitación de Trabajadores 4) Contratación

13. APROBACIÓN

ELABORO	REVISO	APROBO	Vo. Bo. SGC
LUIS DANIEL RODRIGUEZ Auxiliar Administrativo TICS	EDGAR ANGELICO GAMBOA MUR Coordinador GIT Planeación y sistemas de información	FERNANDO ARTURO TORRES JIMENEZ Gerente	JULIO CESAR SALGADO GUERRERO Profesional de Apoyo Oficina de Planeación
FECHA DE CAMBIO (DD/MM/AAA)	**FECHA DE CAMBIO (DD/MM/AAA)**	**FECHA DE CAMBIO (DD/MM/AAA)**	**FECHA DE CAMBIO (DD/MM/AAA)**
01/12/2021	01/12/2021	01/12/2021	01/12/2021

14. CONTROL DE CAMBIOS

ASPECTO DE MODIFICACION	DETALLE DE LOS CAMBIOS	RESPONSABLE	FECHA DE CAMBIO (DD/MM/AAA)	VERSION
VERSION INICICAL	VERSION INICICAL	EDGAR ANGELICO GAMBOA MUR Coordinador GIT Planeacion y sistemas de información	01/12/2021	UNO