	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. **VALLE DEL CAUCA** **NIT: 891900441-1**	**PÁGINA 1**
		CÓDIGO: TI-F-01
	MATRIZ Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	**VERSIÓN 1**
		FECHA DE APROBACIÓN: 31/07/2019

ID Riesgo	Activo(s) según el tipo	RIESGO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO DE RIESGO	CAUSA/VULNERABILIDAD	CONSECUENCIAS
1	Bases de Datos	Modificación no autorizada de la información	Un atacante logra acceder a los sistemas de información del operador y recolecte, retenga y comparta información de identificación personal de los ciudadanos enrolados	Incumplimiento en el mantenimiento Ataque informático Abuso de derechos Falsificación de derechos Sabotaje de la información Suplantación de identidad	Integridad	Falta de políticas que rigen el uso aceptable de los activos de información Asignación errada de los derechos de acceso Ausencia de mecanismos de identificación y autentificación Ausencia de mecanismos de monitoreo Ausencia de procedimientos para el manejo de información tipificada Ausencia de control de los activos que se encuentran fuera de las instalaciones Mantemiento insuficiente Exposición de datos de respaldo Vulnerabilidades conocidas Gestión deficiente de credenciales de acceso Información legible y en texto plano	Pérdida de la información y posibles sanciones legales por falta de oportunidad y calidad de la informado
2	Información			Escucha encubierta Espionaje remoto Incumplimiento en el mantenimiento Ataque informático Suplantación de identidad		Falta de políticas que rigen el uso aceptable de los activos de información Ausencia de pruebas de envío o recepción de mensajes Líneas de comunicación sin protección Tráfico sensible sin protección Ausencia de mecanismos de monitoreo Ausencia de identificación y auntenticación de emisor y recepto Conexiones de red publicas sin protección Gestion inadecuada de la red (Tolerancia a fallos en el enrutamiento)	
3	front End Usuarios, Front End Operador Front End Entidad			Incumplimiento en el mantenimiento Ataque informático Abuso de derechos Falsificación de derechos Sabotaje de la información Suplantación de identidad		Asignación errada de los derechos de acceso Ausencia de mecanismos de identificación y autentificación Ausencia de mecanismos de monitoreo Ausencia de manuales de uso Mantemiento insuficiente Ausencia o insuficiencia de pruebas Ausencia de terminación de sesión Vulnerabilidades conocidas Gestión deficiente de credenciales de acceso	
4	Información			Terremoto Incendio Robo de Información Terrorismo Falla en equipo de telecomunicaciones Ataque informatico		Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Infraestructuras no preparadas para resistir desastres naturales Falta de capacidades y competencias Medios de comunicación obsoletos o en mal estado. Exposición a humedad o agua Exposición a contaminación Exposición a electromagnetismo Configuración y/o instalación incorrectas Vulnerabilidad conocidades Exposición a temperaturas no toleradas por el HW	

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. **VALLE DEL CAUCA** **NIT: 891900441-1**	**PÁGINA 1** **CÓDIGO: TI-F-01**
	MATRIZ Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	**VERSIÓN 1** **FECHA DE APROBACIÓN: 31/07/2019**

ID Riesgo	Activo(s) según el tipo	RIESGO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO DE RIESGO	CAUSA/VULNERABILIDAD	CONSECUENCIAS
5	Información en reposo	Pérdida/Destrucción de información	La información se expone ante amenazas que pueden llevar a su alteración evitando su consecución o destruyéndola	Terremoto Incendio Falla en el suministro de energía Robo de Información Terrorismo Falla en equipos de respaldo Falla en equipos de telecomunicaciones Ataque informatico Error humano	Disponibilidad	Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente No protección contra inundaciones Infraestructuras no preparadas para resistir desastres naturales Protección física insuficiente o incorrecta Abastecimiento de aire (acondicionado) ausente o insuficiente Falta de capacidades y competencias Falta de conciencia seguridad de la información Exposición a temperaturas no toleradas por el HW Exposición a humedad o agua Exposición a electromagnetismo Inexistencia de contingencia Ausencia de políticas para desarrollo seguro Configuración y/o instalación incorrectas Vulnerabilidad conocidas Exposición de los Datos de Respaldo Ausencia de políticas y recursos de backup/respaldo	Sanciones legales a la entidad y al responsable del activo según el decreto 734 de 2002 "custodia y resguardo de la información" artículo 34
6	Información, hardware, software, red	No disponibilidad de la información debido a fallas en sistemas, equipos y servicios	Imposibilidad de acceder a los activos de información (hardaware) por situaciones ajenas al correcto funcionamiento u operación de la entidad	Terremoto Imnundaciones Derrumbe Sabotaje Terrorismo Falla suministro de energía Falla de telecomunicaciones Falla en hardware Falla en software Ataque informatico Incumplimiento en Mantenimiento	Disponibilidad	Políticas ausentes o definidas deficientemente Procedimientos ausentes o definidas deficientemente No protección contra inundaciones Infraestructuras no preparadas para resistir desastres naturales Protección física insuficiente o incorrecta Abastecimiento de aire (acondicionado) ausente o insuficiente Falta de capacidades y competencias Falta de conciencia seguridad de la información Exposición a temperaturas no toleradas por el HW Exposición a humedad o agua Exposición a contaminación Exposición a electromagnetismo Inexistencia de contingencia Ausencia de políticas para desarrollo seguro Configuración y/o instalación incorrectas Vulnerabilidad conocidas Exposición de los Datos de Respaldo Ausencia de políticas y recursos de backup/respaldo Mantenimiento Insuficiente	Posibles silenciios administrativos y sanciones por el cumplimiento al rendir información de ley
7	Información, Sistemas de Enrolamiento	Inconsistencias en la información	Información en los sistemas de información que no corresponden a la realidad o que por motivios de control de usuarios (on/off) puede ser vulnerada.	Error Humano Sabotaje Conflictos Laborales	Integridad	Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Falta de capacitación en el uso de los aplicativos Falta de sensibilización en seguridad de la información Funcionario insatisfecho	Pérdida de la imagen por motivos técnicos, de control y organización demostrando ineficiencia administrativa
8	Hardware e Información	Hurto por parte de propios o terceros	Pérdida del activo de información (hardware) donde se alteran los dispositivos o partes.	Hurto de equipos Hurto de documentos y/o medios Escucha encubierta Recuperación de medios reciclados o desechados Sabotaje	Disponibilidad	Ausencia de controles de seguridad fisica Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Falta de capacitación en el uso de los aplicativos Falta de sensibilización en seguridad de la información Funcionario insatisfecho Equipos de computo desatentidos	Posibles detrimenteos patrimoniales

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. **VALLE DEL CAUCA** **NIT: 891900441-1**	**PÁGINA 1** **CÓDIGO: TI-F-01**
	MATRIZ Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	**VERSIÓN 1** **FECHA DE APROBACIÓN: 31/07/2019**

ID Riesgo	Activo(s) según el tipo	RIESGO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO DE RIESGO	CAUSA/VULNERABILIDAD	CONSECUENCIAS
9	Información Fisica, Digital	Divulgación no autorizada de información confidencial	Pocos controles frente a la administración de los elementos de recolección y publicación de la información	Error Humano Sabotaje Acceso no autorizado a instalaciones Conflictos laborales Tratamiento inadecuado de la información Fuga de información	Confidencialidad	Ausencia de controles de seguridad fisica Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Falta de capacitación en el uso de los aplicativos Falta de sensibilización en seguridad de la información Funcionario insatisfecho Equipos de computo desatentidos Asignación errada de los derechos de acceso	Alteración de los activos de información (Hardware, software, servicios e información) que pueden ocasionar daño a terceros (usuarios que proporcionaron información clasificada o reservada) o la misma entidad
10	Información Fisica, Digital, Sistema de Informacion (Bases de Datos), Front-Ends	Acceso no autorizado a la información	Control de acceso lógicos débiles Controles de acceso fisicos idadecuado o insuficientes Asignación errada de los derechos de acceso	Ingenieria Social Escucha Encubierta Espionaje Remoto Ataque informatico Incumplimiento en Mantenimientos Suplantación de Identidad	Confidencialidad	Falta de políticas que rigen el uso aceptable de los activos de información Falta de capacidades y competencias Falta de conciencia seguridad de la información Procedimientos ausentes o definidas deficientemente Vulnerabilidades conocidas	Alteración de los activos de información (Hardware, software, servicios e información) que ocasionan errores y posibles hechos de corrupción

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1	PÁGINA 1 CÓDIGO: TI-F-01
	MATRIZ Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN 1 FECHA DE APROBACIÓN:

PROBABILIDAD

ID Riesgo	Activo(s) según el tipo	RIESGO	P1	P2	P3	P4	P5	P6	TOTAL	PROM	APROXIMACIÓN
1	Bases de Datos Información front End Usuarios, Front End Operador Front End Entidad	Modificación no autorizada de la información	3	4	3	3	5	2	20	3.33333333	3
2	Información Información en reposo	Pérdida/Destrucción de información	3	2	3	4	2	3	17	2.83333333	3
3	Información, hardware, software, red	No disponibilidad de la información debido a fallas en sistemas, equipos y servicios	2	3	1	2	3	2	13	2.16666667	2
4	Información, Sistemas de Enrolamiento	Inconsistencias en la información	3	4	2	3	4	4	20	3.33333333	3
5	Hardware e Información	Hurto por parte de propios o terceros	1	1	2	2	1	1	8	1.33333333	1
6	Información Fisica, Digital	Divulgación no autorizada de información confidencial	1	1	1	1	1	2	7	1.16666667	1
7	Información Fisica, Digital, Sistema de Informacion (Bases de Datos), Front-Ends	Acceso no autorizado a la información	3	3	4	4	3	4	21	3.5	4

¡o - P1: Participante 1 P… - Tot: Total puntaje - Prom.: Promedio

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1	PÁGINA 1 CÓDIGO: TI-F-01
	MATRIZ Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN 1 FECHA DE APROBACIÓN: 31/07/2019

RIESGO	AMENAZA	CAUSA/VULNERABILIDAD	PROBABILIDAD	IMPACTOS						PROM	IMPACTO	ZONA DE RIESGO
				SOCIAL	ECONÓMICO	AMBIENTAL	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD			
Modificación no autorizada de la información	Incumplimiento en el mantenimiento Ataque informático Abuso de derechos Falsificación de derechos Sabotaje de la información Suplantación de identidad	Falta de políticas que rigen el uso aceptable de los activos de información Asignación errada de los derechos de acceso Ausencia de mecanismos de identificación y autentificación Ausencia de mecanismos de monitoreo Ausencia de procedimientos para el manejo de información tipificada Ausencia de control de los activos que se encuentran fuera de las instalaciones Mantemiento insuficiente Exposición de datos de respaldo Vulnerabilidades conocidas Gestión deficiente de credenciales de acceso Información legible y en texto plano	**3**	4	2	N/A	4	5	3	3.6	**4**	**Zona de riesgo Extremo**
	Escucha encubierta Espionaje remoto Incumplimiento en el mantenimiento Ataque informático Suplantación de identidad	Falta de políticas que rigen el uso aceptable de los activos de información Ausencia de pruebas de envío o recepción de mensajes Líneas de comunicación sin protección Tráfico sensible sin protección Ausencia de mecanismos de monitoreo Ausencia de identificación y auntenticación de emisor y recepto Conexiones de red publicas sin protección Gestion inadecuada de la red (Tolerancia a fallos en el enrutamiento)										
	Incumplimiento en el mantenimiento Ataque informático Abuso de derechos Falsificación de derechos Sabotaje de la información Suplantación de identidad	Asignación errada de los derechos de acceso Ausencia de mecanismos de identificación y autentificación Ausencia de mecanismos de monitoreo Ausencia de manuales de uso Mantemiento insuficiente Ausencia o insuficiencia de pruebas Ausencia de terminación de sesión Vulnerabilidades conocidas Gestión deficiente de credenciales de acceso										
	Terremoto Incendio Robo de Información Terrorismo Falla en equipo de telecomunicaciones Ataque informatico	Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Infraestructuras no preparadas para resistir desastres naturales Falta de capacidades y competencias Medios de comunicación obsoletos o en mal estado. Exposición a humedad o agua Exposición a contaminación Exposición a electromagnetismo Configuración y/o instalación incorrectas Vulnerabilidad conocidades Exposición a temperaturas no toleradas por el HW										

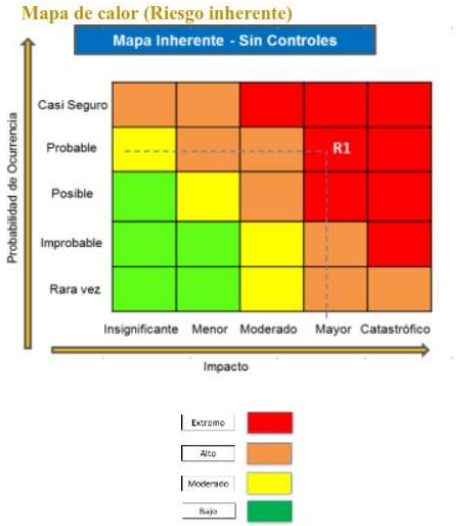
	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1	PÁGINA 1 CÓDIGO: TI-F-01
	MATRIZ Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN 1 FECHA DE APROBACIÓN: 31/07/2019

RIESGO	AMENAZA	CAUSA/VULNERABILIDAD	PROBABILIDAD	IMPACTOS						PROM	IMPACTO	ZONA DE RIESGO
				SOCIAL	ECONÓMICO	AMBIENTAL	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD			
Pérdida/Destrucción de información	Terremoto Incendio Falla en el suministro de energía Robo de Información Terrorismo Falla en equipos de respaldo Falla en equipos de telecomunicaciones Ataque informatico Error humano	Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente No protección contra inundaciones Infraestructuras no preparadas para resistir desastres naturales Protección física insuficiente o incorrecta Abastecimiento de aire (acondicionado) ausente o insuficiente Falta de capacidades y competencias Falta de conciencia seguridad de la información Exposición a temperaturas no toleradas por el HW Exposición a humedad o agua Exposición a electromagnetismo Inexistencia de contingencia Ausencia de políticas para desarrollo seguro Configuración y/o instalación incorrectas Vulnerabilidad conocidas Exposición de los Datos de Respaldo Ausencia de políticas y recursos de backup/respaldo	**3**	2	3	N/A	4	5	5	3.8	**4**	**Zona de riesgo Alto**
No disponibilidad de la información debido a fallas en sistemas, equipos y servicios	Terremoto Imnundaciones Derrumbe Sabotaje Terrorismo Falla suministro de energía Falla de telecomunicaciones Falla en hardware Falla en software Ataque informatico Incumplimiento en Mantenimiento	Políticas ausentes o definidas deficientemente Procedimientos ausentes o definidas deficientemente No protección contra inundaciones Infraestructuras no preparadas para resistir desastres naturales Protección física insuficiente o incorrecta Abastecimiento de aire (acondicionado) ausente o insuficiente Falta de capacidades y competencias Falta de conciencia seguridad de la información Exposición a temperaturas no toleradas por el HW Exposición a humedad o agua Exposición a contaminación Exposición a electromagnetismo Inexistencia de contingencia Ausencia de políticas para desarrollo seguro Configuración y/o instalación incorrectas Vulnerabilidad conocidas Exposición de los Datos de Respaldo Ausencia de políticas y recursos de backup/respaldo Mantenimiento Insuficiente	**2**	2	4	N/A	1	4	5	3.2	**3**	**Zona de riesgo Moderado**
Inconsistencias en la información	Error Humano Sabotaje Conflictos Laborales	Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Falta de capacitación en el uso de los aplicativos Falta de sensibilización en seguridad de la información Funcionario insatisfecho	**3**	5	4	N/A	2	4	1	3.2	**3**	**Zona de riesgo Alto**
Hurto por parte de propios o terceros	Hurto de equipos Hurto de documentos y/o medios Escucha encubierta Recuperación de medios reciclados o desechados Sabotaje	Ausencia de controles de seguridad fisica Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Falta de capacitación en el uso de los aplicativos Falta de sensibilización en seguridad de la información Funcionario insatisfecho Equipos de computo desatentidos	**1**	3	5	N/A	4	4	5	4.2	**4**	**Zona de riesgo Alto**

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1	PÁGINA 1 CÓDIGO: TI-F-01
	MATRIZ Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN 1 FECHA DE APROBACIÓN: 31/07/2019

RIESGO	AMENAZA	CAUSA/VULNERABILIDAD	PROBABILIDAD	IMPACTOS						PROM	IMPACTO	ZONA DE RIESGO
				SOCIAL	ECONÓMICO	AMBIENTAL	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD			
Divulgación no autorizada de información confidencial	Error Humano Sabotaje Acceso no autorizado a instalaciones Conflictos laborales Tratamiento inadecuado de la información Fuga de información	Ausencia de controles de seguridad fisica Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Falta de capacitación en el uso de los aplicativos Falta de sensibilización en seguridad de la información Funcionario insatisfecho Equipos de computo desatentidos Asignación errada de los derechos de acceso	**1**	5	4	N/A	5	2	2	3.6	**4**	**Zona de riesgo Alto**
Acceso no autorizado a la información	Ingenieria Social Escucha Encubierta Espionaje Remoto Ataque informatico Incumplimiento en Mantenimientos Suplantación de Identidad	Falta de políticas que rigen el uso aceptable de los activos de información Falta de capacidades y competencias Falta de conciencia seguridad de la información Procedimientos ausentes o definidas deficientemente Vulnerabilidades conocidas	**4**	5	4	N/A	5	5	5	4.8	**5**	**Zona de riesgo Extremo**

Convenciones: - Prom.: Promedio



	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1	PÁGINA 1
		CÓDIGO: TI-F-01
	MATRIZ Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN 1
		FECHA DE APROBACIÓN: 31/07/2019

Nro	Activo	Riesgo	Tipo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo Residual	Opción Tratamiento	Actividad de Control	Soporte	Responsable	Tiempo	Indicador
	Bases de Datos	Modificación no autorizada de la información	Integridad	Incumplimiento en el mantenimiento Ataque informático Abuso de derechos Falsificación de derechos Sabotaje de la información Suplantación de identidad	Falta de políticas que rigen el uso aceptable de los activos de información Asignación errada de los derechos de acceso Ausencia de mecanismos de identificación y autentificación Ausencia de mecanismos de monitoreo Ausencia de procedimientos para el manejo de información tipificada Ausencia de control de los activos que se encuentran fuera de las instalaciones Mantemiento insuficiente Exposición de datos de respaldo Vulnerabilidades conocidas Gestión deficiente de credenciales de acceso Información legible y en texto plano	3	4	Zona de riesgo Extremo	Reducir	1. Detallar adecuadamente los procedimientos que se realizan en las bases de datos. 2. Evitar emplear aplicaciones/códigos/componentes, que tengan vulnerabilidades conocidas en fuentes como (CVE, NVD) entre otras fuentes. 3. Definir una política de contraseñas seguras, que rijan todos los accesos a las bases de datos, si se considera necesario, se deberá implementar 2 o más factores de autenticación. 4. Definir planes de mantenimiento/depuración/actualización/afinamiento de las bases de datos de manera periódica. 5. Todas las bases de datos deberán ser tenidas en cuenta para la generación de las políticas y planes de respaldos de información.	Procedimientos, políticas e informes documentados	Gerencia / Oficina sistemas / Comité Institucional de Gestión y Desempeño / Comité de riesgos	2020	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
	Información			Escucha encubierta Espionaje remoto Incumplimiento en el mantenimiento Ataque informático Suplantación de identidad	Falta de políticas que rigen el uso aceptable de los activos de información Ausencia de pruebas de envío o recepción de mensajes Líneas de comunicación sin protección Tráfico sensible sin protección Ausencia de mecanismos de monitoreo Ausencia de identificación y auntenticación de emisor y recepto Conexiones de red publicas sin protección Gestion inadecuada de la red (Tolerancia a fallos en el enrutamiento)					Teniendo en cuenta las conexiones de red que se definan y que así lo requieran, se deberán implementar las siguientes medidas: Para las conexiones entre entidades es importante tener en cuenta las siguientes recomendaciones: 1. Deberán monitorearse los canales y las conexiones, para verificar posibles pérdidas en el canal que puedan afectar los datos transmitidos. 2. Los accesos a las plataformas deberán tener diferentes factores de autenticación si así se consideran, teniendo una política de contraseñas previamente definida en los sistemas de información.				
	front End Usuarios, Front End Operador Front End Entidad			Incumplimiento en el mantenimiento Ataque informático Abuso de derechos Falsificación de derechos Sabotaje de la información Suplantación de identidad	Asignación errada de los derechos de acceso Ausencia de mecanismos de identificación y autentificación Ausencia de mecanismos de monitoreo Ausencia de manuales de uso Mantemiento insuficiente Ausencia o insuficiencia de pruebas Ausencia de terminación de sesión Vulnerabilidades conocidas Gestión deficiente de credenciales de acceso					1. Implementación Web Application Firewall. 2. Desarrollar el código de las aplicaciones web teniendo en cuenta las recomendaciones dadas en OWASP.				
	Información			Terremoto Incendio Robo de Información Terrorismo Falla en equipo de telecomunicaciones Ataque informatico	Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Infraestructuras no preparadas para resistir desastres naturales Falta de capacidades y competencias Medios de comunicación obsoletos o en mal estado. Exposición a humedad o agua Exposición a contaminación Exposición a electromagnetismo Configuración y/o instalación incorrectas Vulnerabilidad conocidades Exposición a temperaturas no toleradas por el HW					1. Verificación de canales de contingencia entre los operadores, para evitar perdida de solicitudes de transacciones o transmisión de información entre los mismos. 2. Elaborar un plan de continuidad de negocio, con roles, responsabilidades, recursos tecnológicos y personal necesario para asegurar la continuidad del servicio en los escenarios más críticos. 3. Todos los procedimientos de contingencia deberán estar debidamente documentados, para garantizar una respuesta adecuada ante posibles incidentes y a su vez la mayor disponibilidad posible de los servicios y de la información. 4. Control de acceso físico a datacenters, con registros (preferiblemente bajo sistemas de información) 5. Capacitación del personal de seguridad física, en temas de seguridad de la información.				**EFICACIA:** Índice de cumplimiento actividades= (# de actividades

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1	PÁGINA 1
		CÓDIGO: TI-F-01
	MATRIZ Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN 1
		FECHA DE APROBACIÓN: 31/07/2019

Nro	Activo	Riesgo	Tipo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo Residual	Opción Tratamiento	Actividad de Control	Soporte	Responsable	Tiempo	Indicador
	Información en reposo	Pérdida/Destrucción de información	Disponibilidad	Terremoto Incendio Falla en el suministro de energía Robo de Información Terrorismo Falla en equipos de respaldo Falla en equipos de telecomunicaciones Ataque informatico Error humano	Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente No protección contra inundaciones Infraestructuras no preparadas para resistir desastres naturales Protección física insuficiente o incorrecta Abastecimiento de aire (acondicionado) ausente o insuficiente Falta de capacidades y competencias Falta de conciencia seguridad de la información Exposición a temperaturas no toleradas por el HW Exposición a humedad o agua Exposición a electromagnetismo Inexistencia de contingencia Ausencia de políticas para desarrollo seguro Configuración y/o instalación incorrectas Vulnerabilidad conocidas Exposición de los Datos de Respaldo Ausencia de políticas y recursos de backup/respaldo	**3**	**4**	**Zona de riesgo Alto**	Reducir	1. Elaborar un plan de continuidad de negocio, con roles, responsabilidades, recursos tecnológicos y personal necesario para asegurar la continuidad del servicio en los escenarios más críticos. 2. Mantenimientos periódicos a los sistemas eléctricos, con el diseño de su respectiva contingencia. 3. Mantener mantenimiento y monitoreo constante en los sistemas de refrigeración y de control de humedad. 4.Control de acceso físico a datacenters, con registros (preferiblemente bajo sistemas de información) 5. Capacitación del personal de seguridad física, en temas de seguridad de la información. 6. Definición de políticas de respaldo de información.	Procedimientos, políticas e informes documentado	Gerencia / Oficina sistemas / Comité Institucional de Gestión y Desempeño / Comité de riesgos	2020	cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
	Información, hardware, software, red	No disponibilidad de la información debido a fallas en sistemas, equipos y servicios	Disponibilidad	Terremoto Imnundaciones Derrumbe Sabotaje Terrorismo Falla suministro de energía Falla de telecomunicaciones Falla en hardware Falla en software Ataque informatico Incumplimiento en Mantenimiento	Políticas ausentes o definidas deficientemente Procedimientos ausentes o definidas deficientemente No protección contra inundaciones Infraestructuras no preparadas para resistir desastres naturales Protección física insuficiente o incorrecta Abastecimiento de aire (acondicionado) ausente o insuficiente Falta de capacidades y competencias Falta de conciencia seguridad de la información Exposición a temperaturas no toleradas por el HW Exposición a humedad o agua Exposición a contaminación Exposición a electromagnetismo Inexistencia de contingencia Ausencia de políticas para desarrollo seguro Configuración y/o instalación incorrectas Vulnerabilidad conocidas Exposición de los Datos de Respaldo Ausencia de políticas y recursos de backup/respaldo Mantenimiento Insuficiente	**2**	**3**	**Zona de riesgo Moderado**	Reducir	1. Definir una política de continuidad de negocio y los respectivos planes derivados para los servicios más críticos. 2. Deberán documentarse todos los procedimientos definidos para la recuperación de los servicios y para el desarrollo de las actividades más críticas para el servicio. 3. Realizar controles de cambios para verificar consecuencias en actualizaciones o configuraciones nuevas, empleando los respectivos ambientes de desarrollo, pruebas y producción. 4. Garantizar pruebas periódicas en contingencia de energía eléctrica, con el uso de UPS, plantas alternas etc.... 5. Garantizar la seguridad física donde se encuentren ubicados los sistemas de información, así mismo asegurar las conexiones electricas para evitar sabotajes como desconexión de los servidores o de los dispositivos de red. 6. Implementación de aplicaciones de seguridad (Antimalware, antiphishing, antispyware, etc.)	Procedimientos, políticas e informes documentado	Gerencia / Oficina sistemas / Comité Institucional de Gestión y Desempeño / Comité de riesgos	2020	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1	PÁGINA 1 CÓDIGO: TI-F-01
	MATRIZ Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN 1 FECHA DE APROBACIÓN: 31/07/2019

Nro	Activo	Riesgo	Tipo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo Residual	Opción Tratamiento	Actividad de Control	Soporte	Responsable	Tiempo	Indicador
	Información, Sistemas de Enrolamiento	Inconsistencias en la información	Integridad	Error Humano Sabotaje Conflictos Laborales	Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Falta de capacitación en el uso de los aplicativos Falta de sensibilización en seguridad de la información Funcionario insatisfecho	**3**	**3**	**Zona de riesgo Alto**	Reducir	1. En los posibles puntos de enrolamiento se recomienda verificar que el personal tenga los procedimientos de enrolamientos bien documentados y definidos. 2. En caso de despido o de bajas de personal, efectuar las bajas en los sistemas de información a la mayor brevedad (esto implica el desarrollo de procedimientos de creación y gestión de usuarios según cada rol). 3. Verificar adecuadamente que los usuarios registren información verídica, todo esto en el marco del procedimiento de enrolamiento que deberá generarse. 4. Capacitación adecuada en los diferentes procesos, para evitar el mal uso de las aplicaciones o la carga de información errada en las mismas.	Procedimientos, políticas e informes documentado	Gerencia / Oficina sistemas / Comité Institucional de Gestión y Desempeño / Comité de riesgos	2020	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
	Hardware e Información	Hurto por parte de propios o terceros	Disponibilidad	Hurto de equipos Hurto de documentos y/o medios Escucha encubierta Recuperación de medios reciclados o desechados Sabotaje	Ausencia de controles de seguridad fisica Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Falta de capacitación en el uso de los aplicativos Falta de sensibilización en seguridad de la información Funcionario insatisfecho Equipos de computo desatentidos	**1**	**4**	**Zona de riesgo Alto**	Reducir	1. En el caso de información física sensible, deberá disponerse de un área de archivo con la custodia correspondiente (Puertas, Cámaras de seguridad y Controles de Acceso Físico) 2. Garantizar la seguridad física donde se encuentren ubicados los sistemas de información, así mismo asegurar las conexiones electricas para evitar sabotajes como desconexión de los servidores o de los dispositivos de red. 3. Tener plenamente preparados planes de continuidad de negocio en caso de robo de algún componente específico, teniendo en cuenta los tiempos de respuesta definidos. 4. Políticas para disposición de información de medios físicos. 5. Sensibilización a todo el personal en temas de ingeniería social, para evitar posibles robos de información a través de estos métodos. 6. Implementación de herramientas como antivirus o IPS a nivel de Host, que protejan a los servidores y/o sistemas de información de amenazas como ransomware y otro tipo de malware.	Procedimientos, políticas e informes documentado	Gerencia / Oficina sistemas / Comité Institucional de Gestión y Desempeño / Comité de riesgos	2020	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1	PÁGINA 1 CÓDIGO: TI-F-01
	MATRIZ Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN 1 FECHA DE APROBACIÓN: 31/07/2019

Nro	Activo	Riesgo	Tipo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo Residual	Opción Tratamiento	Actividad de Control	Soporte	Responsable	Tiempo	Indicador
	Información Fisica, Digital	Divulgación no autorizada de información confidencial	Confidencialidad	Error Humano Sabotaje Acceso no autorizado a instalaciones Conflictos laborales Tratamiento inadecuado de la información Fuga de información	Ausencia de controles de seguridad fisica Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Falta de capacitación en el uso de los aplicativos Falta de sensibilización en seguridad de la información Funcionario insatisfecho Equipos de computo desatentidos Asignación errada de los derechos de acceso	1	4	Zona de riesgo Alto	Reducir	1. Verificación minuciosa sobre el personal contratado (Pasado judicial y pruebas de seguridad), dependiendo del tipo de privilegios que pueda tener en cuanto al acceso a los datos o la información. 2. Firma de acuerdos de confidencialidad para cada uno de los empleados que tengan o no acceso a la información y las instalaciones (incluyendo al personal de mantenimiento y aseo) 3. En los acuerdos o documentos definidos para la confidencialidad, deberá enfatizarse las consecuencias legales y disciplinarias correspondientes en caso de faltar a los compromisos que en este se enuncien. 4. Políticas que regulen el ingreso de dispositivos de almacenamiento extraíbles como discos duros, memorias USB etc... las cuales no deberían emplearse por parte del operador. 5. Limitar el uso de herramientas personales (correo electrónico, soluciones en la nube etc...) Ajenas a las asignadas por el operador, incluyendo los computadores, NO debe haber acceso a la administración de las plataformas desde máquinas particulares o personales. 6. Preparar al personal de técnicas como la ingeniería social para evitar fugas de información por este método. 7. Garantizar la seguridad física donde se encuentren ubicados los sistemas de información, así mismo asegurar las conexiones electricas para evitar sabotajes como desconexión de los servidores o de los dispositivos de red.	Procedimientos, políticas e informes documentado	Gerencia / Oficina sistemas / Comité Institucional de Gestión y Desempeño / Comité de riesgos	2020	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
	Información Fisica, Digital, Sistema de Informacion (Bases de Datos), Front-Ends	Acceso no autorizado a la información	Confidencialidad	Ingenieria Social Escucha Encubierta Espionaje Remoto Ataque informatico Incumplimiento en Mantenimientos Suplantación de Identidad	Falta de políticas que rigen el uso aceptable de los activos de información Falta de capacidades y competencias Falta de conciencia seguridad de la información Procedimientos ausentes o definidas deficientemente Vulnerabilidades conocidas	4	5	Zona de riesgo Extremo	Reducir	1. Definir las políticas de uso aceptable de los recursos tecnológicos asignados, entre ellos la cuentas de usuario de las plataformas de administración. 2. Generación de campañas para la ciudadanía, reforzando los temas principalmente de ingeniería social y phishing, para el robo de datos de acceso. 3. Definir factores adicionales de autenticación que incrementen los niveles de seguridad, teniendo en cuenta los principios: *Algo que el usuario sabe. (Ej. Contraseña, PIN) *Algo que el usuario posee. (Ej. Token, Apps, Tarjetas) *Algo que el usuario es. (Ej .Biometría) *Algo que el usuario sabe hacer. (Ej. Firma) 4. Garantizar la seguridad física donde se encuentren ubicados los sistemas de información, así mismo asegurar las conexiones electricas para evitar sabotajes como desconexión de los servidores o de los dispositivos de red. 5. En el caso de información física sensible, deberá disponerse de un área de archivo con la custodia correspondiente (Puertas, Cámaras de seguridad y Controles de Acceso Físico)	Procedimientos, políticas e informes documentado	Gerencia / Oficina sistemas / Comité Institucional de Gestión y Desempeño / Comité de riesgos	2020	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)