EMPRESA SOCIAL DEL ESTADO
PASTO SALUD E.S.E
NIT.900091143-9

MATRIZ DE RIESGOS - SEGURIDAD DE LA INFORMACION (PARTE B)

VERSION	PROCESO / SERVICIO	CODIGO	NUM
6,0	GESTION DE SISTEMAS DE INFORMACION	GSI-RSI	411-B

FECHA DE ACTUALIZACION:	10-AGOSTO DE 2021	MACROPROCESO	PROCESO SISTEMAS DE INFORMACION

PROCESO	RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD	CONSECUENCIA	VALORACION DEL ACTIVO	VALORACIÓN DEL RIESGO SIN CONTROLES			CONTROLES	VALORACIÓN DEL RIESGO DESPUES DE CONTROLES			TRATAMIENTO					
								PROBABILIDAD	IMPACTO	SEVERIDAD		PROBABILIDAD	IMPACTO	SEVERIDAD	OPCIONES DE MANEJO	ACCIONES	RESPONSABLE DE LAS ACCIONES	FECHA DE IMPLEMENTACION		MEDIO DE EVIDENCIA
																		INICIO	FINAL	
GESTION DE SISTEMAS DE INFORMACION	Posibilidad de perder completitud, la exactitud y la coherencia de datos de las bases de datos por modificaciones no autorizadas y vulneración de datos reservados debido a contraseñas no seguras, ausencia de mecanismos de autenticación, ausencia de bloqueos de sesión y ausencia de políticas de control de acceso.	Bases de datos	INFORMACION	. Modificaciones no autorizadas . Vulneración de datos reservados	.Contraseñas no seguras .Ausencia de mecanismos de autenticación de usuarios .Ausencia de bloqueos de sesión .Ausencia de políticas de control de acceso	.Legales .Económicas .Mala toma de decisiones .Error en la recepción y envío de comunicaciones oficiales . Imagen Reputación	ALTO	80% Alta	80% Mayor	ALTA	**Control 1:** El ingeniero de sistemas encargado de realizar la auditoría de seguridad de la información, verifica que los colaboradores estén aplicando las buenas prácticas de seguridad y privacidad de la información, a través de una evaluación de conocimientos y de un cuestionario de verificación en los puestos de trabajo de las sedes auditadas. **Control 2:** El Sistema de gestión de base de datos relacional SQL Server verifica que los roles y derecho de acceso de los usuarios sean los correctos para el acceso a las bases de datos a través del inicio de sesión del usuario y contraseña asignados. **Control 3:** El administrador de directiva de grupos del directorio activo de manera automática bloquea los usuarios que han intentado acceder más de tres veces con la contraseña errónea a través de la política del directorio activo implementada. **Control 4**: El administrador de directiva de grupos del directorio activo de manera automática valida que las contraseñas creada contengan combinación de mínimo 8 caracteres través de la política de contraseñas seguras del directorio activo implementada.	7% Muy baja	80% Mayor	ALTA	**MITIGAR EL RIESGO** (Tomar correctivos en caso de materialización del riesgo, toda vez que la probabilidad de ocurrencia es muy baja de acuerdo a los controles preventivos aplicados en la Entidad)	**1.** Asignación de perfiles a las bases de datos por custodios de la información y seguimiento. **2.** Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	**1.** Profesional Universitario Ingeniero de Sistemas **2.** Líder del proceso Oficina Control Interno	**1.** 1/09/2021 **2.** Segundo semestre de 2021. Semestralmente	**1.** 30/11/2021 **2.** Segundo semestre de 2021. Semestralmente	**1.** Acta de desarrollo de tareas para cambio de perfiles Tabla de acceso y control **2.** Informes
GESTION DE SISTEMAS DE INFORMACION	Posibilidad de pérdida de la confidencialidad y disponibilidad de la información por falla de los equipos de cómputo, mal funcionamiento de los equipos e infección por virus informático, debido a mantenimiento insuficiente, ausencia de reposición tecnológica, falta de equipos de refrigeración y/o inconvenientes por humedad, polvo o suciedad, descarga y uso no controlado de software y ausencia de virus.	. Servidores . Computadores de escritorio y portátiles . Unidad NAS de almacenamiento	HARDWARE	. Falla de los equipos de computo . Mal funcionamiento de los equipos . Infección por virus informático (Spyware/Malware)	. Mantenimiento insuficiente . Ausencia de reposición tecnológica . Falta de equipos de refrigeración y/o inconvenientes por humedad(o al Polvo y Suciedad) . Descarga y uso no controlado de software . Ausencia de antivirus	.Legales .Económicas .Insatisfacción de usuarios y sus familias por la no atención .No continuidad en el proceso de atención integral en salud y procesos de apoyo a través de la herramienta SIOS . Posible ocurrencia de eventos adversos	ALTO	100% Muy Alta	80% Mayor	ALTA	**Control 1**: El supervisor del contrato de mantenimiento preventivo y correctivo de equipos de comunicaciones y sistemas verifica que se haya ejecutado el mantenimiento por parte del contratista a través del informe que envía el proveedor y la firma del registro a satisfacción de los mantenimientos por parte de los técnicos de sistemas. **Control 2**: El jefe de la Oficina Asesora de Comunicaciones y Sistemas elabora y ejecuta el plan de adquisiciones de nuevas tecnologías con los recursos asignados para compra de equipos asignados en el presupuesto. **Control 3:** El equipo de aire acondicionado mantiene condiciones ambientales precisas para la integridad de los servidores que permite el cuidado y funcionamiento de los equipos que allí se encuentran. **Control 4:** Las políticas de seguridad de la información implementadas administran la infraestructura de hardware y software controlando el acceso y uso a los recursos informáticos y se lo hace a través del directorio activo y del antivirus. **Control 5**: El sistema de antivirus implementado detecta, evita y elimina malware comparando cada archivo del disco duro con un diccionario de virus ya conocidos. Si cualquier pieza de código en un archivo del disco duro coincide con el virus conocido en el diccionario, el software antivirus entra en acción, llevando a cabo una de las acciones posibles.	8% Muy baja	80% Mayor	ALTA	**MITIGAR EL RIESGO** (Tomar correctivos en caso de materialización del riesgo, toda vez que la probabilidad de ocurrencia es muy baja de acuerdo a los controles preventivos aplicados en la Entidad)	**1** Ejecución y Cumplir con la ejecución de el Plan anual de adquisiciones logrando que la reposición tecnológica este al final del año por encima del 90% de lo programado . 2. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	1. Profesional Universitario Ingeniero de Sistemas 2. Líder del proceso Oficina Control Interno	**1.** 1/01/2021 **2.** Segundo semestre de 2021. Semestralmente	**1.** 31/12/2021 **2.** Segundo semestre de 2021. Semestralmente	**1.** Indicador del plan anual de adquisiciones de nuevas tecnologías del poa **2.** Informes

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9	MATRIZ DE RIESGOS - SEGURIDAD DE LA INFORMACION (PARTE B)		
VERSION	PROCESO / SERVICIO	CODIGO	NUM
6,0	GESTION DE SISTEMAS DE INFORMACION	GSI-RSI	411-B

FECHA DE ACTUALIZACION:	10-AGOSTO DE 2021	MACROPROCESO	PROCESO SISTEMAS DE INFORMACION

PROCESO	RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD	CONSECUENCIA	VALORACION DEL ACTIVO	VALORACIÓN DEL RIESGO SIN CONTROLES			CONTROLES	VALORACIÓN DEL RIESGO DESPUES DE CONTROLES			TRATAMIENTO					
								PROBABILIDAD	IMPACTO	SEVERIDAD		PROBABILIDAD	IMPACTO	SEVERIDAD	OPCIONES DE MANEJO	ACCIONES	RESPONSABLE DE LAS ACCIONES	FECHA DE IMPLEMENTACION		MEDIO DE EVIDENCIA
																		INICIO	FINAL	
GESTION DE SISTEMAS DE INFORMACION	Posibilidad de pérdida de confidencialidad y disponibilidad de la información por falla de la conectividad, falla de las telecomunicaciones y espionaje remoto. Debido a la ausencia de cumplimiento de los niveles de servicio por parte del proveedor, ausencia de equipos para la protección externa y conexiones de red sin protección.	. Switches . Acces Point . Cableado Fibra Óptica . Cableado Estructurado . Foirtigate	REEDES	. Falla de la conectividad . Falla de las telecomunicaciones . Espionaje Remoto (Hackers)	.Ausencia de cumplimiento de los niveles de servicio por parte de proveedor. . Ausencia de equipos para la protección externa . Conexiones de red sin protección	.Pérdida de la información durante la contingencia (Historia Clínica). . Perdida de tiempo operacional . Perdida de datos al momento de la caída del servicio	ALTA	100% Muy Alta	80% Mayor	ALTO	**Control 1**: El jefe la Oficina Asesora de Comunicaciones y Sistema verifica el cumplimiento del servicio de conectividad e internet a través del acuerdo de nivel de servicios establecido en el contrato con el proveedor. **Control 2:** La herramienta PRTG monitorea los niveles de servicios de conectividad e internet a través del indicador del informe mensual suministrado por el software donde se establecen las caídas de los servicios. **Control 3:** El equipo FORTINET es un dispositivo de seguridad perimetral que controla amenazas emergentes detectando prevención de intrusos, bloqueo a sitos web maliciosos, amenazas de malware a través del firewall.	22% Baja	80% Mayor	ALTO	**MITIGAR EL RIESGO** (Tomar correctivos en caso de materialización del riesgo, toda vez que la probabilidad de ocurrencia es baja de acuerdo a los controles preventivos aplicados en la Entidad)	**1.**Consultar periódicamente los boletines de amenazas informáticas, caídas de conectividad y realizar los ajustes necesarios a los controles cuando aplique. 2. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	**1.** Profesional Universitario Sistemas/Ingeniero de Sistemas **2.** Líder del proceso Oficina Control Interno	**1.** 1/09/2021 **2.** Segundo semestre de 2021. Semestralmente	**1.** 31/12/2021 **2.** Segundo semestre de 2021. Semestralmente	**1.** Informe mensual de monitoreo y seguimiento a eventos que pueden afectar la seguridad de la información. **2.** Informes
GESTION DE SISTEMAS DE INFORMACION	Posibilidad de pérdida de confidencialidad y disponibilidad de la información por error en el uso de equipos y software, abuso de derechos, entrega equivocada de información, divulgación de contraseñas, revelación de información y fuga de información. Debido a entrenamiento insuficiente, desconocimiento y falta de apropiación de la política de seguridad de la información, desconocimiento en los tiempos de entrega y recepción de documentos.	. Personal Técnico Interno . Personal Técnico Externo . Colaboradores	TALENTO HUMANO	. Error en el uso de equipos y software . Abuso de derechos . Entrega equivocada de correspondencia . Divulgación de contraseñas. . Revelación de información. . Fuga de información.	. Entrenamiento insuficiente . Desconocimiento y Falta de apropiación de la política de seguridad de la información . Desconocimiento en los tiempos de entrega y recepción de documentos	.Sanciones disciplinarias .Legales .Económicas . Imagen Reputación	ALTA	80% Alta	80% Mayor	ALTO	**Control 1:** El ingeniero de sistemas elabora la capacitación virtual para el conocimiento y aplicabilidad de la política de seguridad de la información para personal interno, a través de un cuestionario de evaluación en la plataforma Moodle. **Control 2:** La contratista de Gestión Documental brindará capacitación a todos los colaboradores para el manejo de la conservación documental y tablas de retención documental a través de las temáticas de las jornadas de capacitación programadas por Talento Humano.	29% Baja	80% Mayor	ALTO	**MITIGAR EL RIESGO** (Tomar correctivos en caso de materialización del riesgo, toda vez que la probabilidad de ocurrencia es baja de acuerdo a los controles preventivos aplicados en la Entidad)	**1.** Sensibilizar a los a colaboradores de la entidad en la apropiación de la política de seguridad de información, manual de política de seguridad de la información. **2.** Realizar capacitaciones cortas y concretas al respecto, en el manejo sensible de la información y comunicaciones evitando que los colaboradores incurra en errores de tipo procedimental por desconocimiento. **3.** Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	**1. y 2.** Ingeniero de Sistemas Técnicos de Sistemas Técnico Archivo **3.** Líder del proceso Oficina Control Interno	**1. y 2.** 1/09/2021 **3.** Segundo semestre de 2021. Semestralmente	**1. y 2.** 31/12/2021 **3.** Segundo semestre de 2021. Semestralmente	**1. y 2.** Registro de asistencia y evaluación **3.** Informes

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9	MATRIZ DE RIESGOS - SEGURIDAD DE LA INFORMACION (PARTE B)		
VERSION	PROCESO / SERVICIO	CODIGO	NUM
6,0	GESTION DE SISTEMAS DE INFORMACION	GSI-RSI	411-B

FECHA DE ACTUALIZACION:	10-AGOSTO DE 2021	MACROPROCESO	PROCESO SISTEMAS DE INFORMACION

PROCESO	RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD	CONSECUENCIA	VALORACION DEL ACTIVO	VALORACIÓN DEL RIESGO SIN CONTROLES			CONTROLES	VALORACIÓN DEL RIESGO DESPUES DE CONTROLES			TRATAMIENTO					
								PROBABILIDAD	IMPACTO	SEVERIDAD		PROBABILIDAD	IMPACTO	SEVERIDAD	OPCIONES DE MANEJO	ACCIONES	RESPONSABLE DE LAS ACCIONES	FECHA DE IMPLEMENTACION		MEDIO DE EVIDENCIA
																		INICIO	FINAL	
GESTION DE SISTEMAS DE INFORMACION	Posibilidad de pérdida de confidencialidad y disponibilidad de la información por copia fraudulenta de software, infección por virus informático, falla de los sistemas de información, errores de software, instalaciones y uso no autorizado de software. Debido a descarga y uso no controlado de software, ausencia de copias de respaldo, ausencia de antivirus, ausencia de validación de licenciamiento, mantenimiento insuficiente y ausencia de políticas de restricción de software.	. Sistema de Información SIOS . Sistema SICA . Sistema de Costos . Antivirus . MilPS . Infomedic . Spark . Ostickets . Sistemas Operativos Windows . Office Bussines	SOFTWARE	. Copia Fraudulenta de Software . Infección por virus informático (Spyware/Malware) . Falla de los sistemas de información . Infracción legal . Errores de software. . Instalación no autorizada de software. . Uso no autorizado de software.	.Descarga y uso no controlado de software . Ausencia de copias de respaldo . Ausencia de antivirus . Ausencia de validación de licenciamiento . Mantenimiento insuficiente . Ausencia de políticas de restricción de software	.Legales .Económicas .No continuidad en el proceso de atención integral en salud y procesos de apoyo a través de la herramienta SIOS . Subfacturación por no disponibilidad del sistema SIOS	**MEDIA**	**100%** **Muy Alta**	**100%** **Catastrófico**	**EXTREMO**	**Control 1:** EL directorio activo de Windows server tiene configuradas las políticas de seguridad de la información a nivel de software que controlan las descargas e instalación de software no autorizados a los recursos informáticos a través de alertas como acciones preventivas. **Control 2:** Microsoft SQL Server y COBIAN son sistemas que ejecuta las copias de respaldo de las bases de datos y archivos de los servidores y equipos a través de la programación de copias de respaldo full y diferenciales programadas. **Control 3:** El sistema de antivirus implementado detecta, evita y elimina malware comparando cada archivo del disco duro con un diccionario de virus ya conocidos. Si cualquier pieza de código en un archivo del disco duro coincide con el virus conocido en el diccionario, el software antivirus entra en acción, llevando a cabo una de las acciones posibles. **Control 4:** El supervisor del contrato de mantenimiento preventivo y correctivo de equipos de comunicaciones y sistemas verifica que se haya ejecutado el mantenimiento por parte del contratista a través del informe que envía el proveedor y la firma del registro a satisfacción de los mantenimientos por parte de los técnicos de sistemas. **Control 5:** EL directorio activo de Windows server tiene configuradas las políticas de seguridad de la información a nivel de software que controlan los accesos a la red de datos y validan usuarios y contraseñas a través de los perfiles asignados a los colaboradores	**13%** **Muy Baja**	**65%** **Mayor**	**MODERADO**	**ACEPTAR EL RIESGO** (El riesgo se encuentra en un nivel que puede asumir el mismo, conociendo los efectos de su posible materialización sin necesidad de tomar otras medidas de control diferentes a las que se poseen)	**1.** Monitorear y hacer seguimiento a los eventos o incidentes que pueden afectar la seguridad de la información **2.** Consultar periódicamente los boletines de amenazas informáticas y realizar ajustes a los controles recomendados sobre la plataforma de seguridad. **3.** Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	**1. y 2.** Profesional Universitario Sistemas **3.** Líder del proceso Oficina Control Interno	**1. y 2.** 1/08/2021 **3.** Segundo semestre de 2021. Semestralmente	**1. y 2.** 31/12/2021 **3.** Segundo semestre de 2021. Semestralmente	**1. y 2.** Informe mensual de incidentes o eventos que afectan la seguridad de la información **3.** Informes

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9	MATRIZ DE RIESGOS - SEGURIDAD DE LA INFORMACION (PARTE B)		
VERSION	PROCESO / SERVICIO	CODIGO	NUM
6,0	GESTION DE SISTEMAS DE INFORMACION	GSI-RSI	411-B

FECHA DE ACTUALIZACION:	10-AGOSTO DE 2021	MACROPROCESO	PROCESO SISTEMAS DE INFORMACION

PROCESO	RIESGO	TIPO DE ACTIVO	ACTIVO	AMENAZA	VULNERABILIDAD	CONSECUENCIA	VALORACION DEL ACTIVO	VALORACIÓN DEL RIESGO SIN CONTROLES			CONTROLES	VALORACIÓN DEL RIESGO DESPUES DE CONTROLES			TRATAMIENTO					
								PROBABILIDAD	IMPACTO	SEVERIDAD		PROBABILIDAD	IMPACTO	SEVERIDAD	OPCIONES DE MANEJO	ACCIONES	RESPONSABLE DE LAS ACCIONES	FECHA DE IMPLEMENTACION		MEDIO DE EVIDENCIA
																		INICIO	FINAL	
GESTION DE SISTEMAS DE INFORMACION	Posibilidad de pérdida de confidencialidad y disponibilidad de la información por fuga de información, inundaciones y perdida de información. Debido a la ausencia de controles de acceso físico, susceptibilidad a la humedad, el polvo y la suciedad y falta de copias de respaldo.	. Archivos electrónicos y digitales . Documentos físicos y comunicaciones oficiales	INFORMACION	. Fuga de información . Inundaciones . Perdida de información	.Ausencia de Controles de acceso físico . Susceptibilidad a la humedad el polvo y la suciedad . Falta de copias de respaldo	.Legales .Económicas . Imagen Reputación	**ALTA**	**80% Alta**	**80% Mayor**	**ALTO**	**Control 1:**El dispositivo termo higrómetro mide la temperatura y humedad de los archivos de historia clínica, a través del formato de registro definido para tal fin se llevan los datos históricos de la medición. **Control 2**: El personal de aseo realiza limpieza y desinfección de las áreas de archivo y registra en el formato de limpieza y desinfección estandarizado por la empresa **Control 3:** El profesional Universitarios de Salud y Seguridad en el trabajo implementó la señalización a los espacios físicos de los archivos, data center y oficinas de la empresa mediante avisos preventivos de acceso al personal interno y externo. **Control 4:** El jefe de la oficina Asesora de comunicaciones y Sistemas gestionó la instalación de una puerta electrónica con clave de acceso al datacenter de la empresa, la clave de acceso es manejada solo por el personal de ingenieros de la oficina. **Control 5**: La cámara de video vigilancia instalada en el datacenter permite controlar el acceso del personal técnico a través de las grabaciones realizadas en el DVR. **Control 6:** COBIAN backup es una herramienta que ejecuta las copias de respaldo de los documentos de los equipos priorizados a través de la programación de copias de respaldo full y diferenciales programadas para ser almacenadas en la unidad de almacenamiento del datacenter.	**4% Muy Baja**	**52% Moderado**	**MODERADO**	**ACEPTAR EL RIESGO** (El riesgo se encuentra en un nivel que puede asumir el mismo, conociendo los efectos de su posible materialización sin necesidad de tomar otras medidas de control diferentes a las que se poseen)	**1.** Revisar de manera sistemática la realización de copias de seguridad en medios magnéticos **2**. Verificación semestral del cumplimiento de las actividades propuestas en el documento sistema integrado de conservación SIC **3**. Realizar monitoreo y seguimiento a los controles para que se apliquen continuamente, presentando informe al comité coordinador de control interno	**1. y 2.** Profesional Universitario Sistemas **3.** Líder del proceso Oficina Control Interno	**1. y 2** 1/01/2021 **3.** Segundo semestre de 2021. Semestralmente	**1. y 2.**31/12/2021 **3.** Segundo semestre de 2021. Semestralmente	**1. y 2.** Indicador de copias de seguridad MiIPS **3.** Informe al cumplimiento de las actividades del SIC

ELABORO	REVISO	APROBO (Líder de Proceso)
WILLIAM MONTENEGRO	JAIME SANTACRUZ S.	ARVEY VALLEJO