



MAPA DE RIESGOS SEGURIDAD DIGITAL

Código: FT-GETI-007

1 de enero de 2023

Revisión: 00

ID Riesgo	Activo de Información	Tipo de activo	Descripción del Riesgo	Tipo de Riesgo	Causa Principal	Consecuencias	RIESGO INHERENTE					Descripción del Control	ATRIBUTOS DE CONTROL					RIESGO RESIDUAL				PLAN DE ACCIÓN									
							Probabilidad inherente	%	Impacto	%	Zona de Riesgo inherente		ID Control	Atributos de Eficiencia		Atributos Informativos			Peso calificación residual	Probabilidad residual final	Impacto residual final	Riesgo residual final	Zona de riesgo final	Tratamiento	ID Acción	Acción	Responsable	Fecha de Inicio	Fecha de Finalización	Acción de Contingencia	
														Tipo	Implementación	Documentación	Frecuencia	Evidencia													
1	SERVIDOR RECEIVE DIRECTORY SERVIDOR MANTECIDA (M) SERVIDOR DISMISO (dfiles) SERVIDOR FILESERVER SERVIDOR FORTISSIM SERVIDOR HERCULES (Repentino de desarrollo) SERVIDOR SERVIDORES DE GESTION DOCUMENTAL SERVIDOR SERVIDOR DE IMPRESION SERVIDOR INTANET SERVIDOR ISOLACION SERVIDOR DISOLUWARE SERVIDOR ANTIWARE (INCAFFE) SERVIDOR GESTION DE SERVICIOS DE TI (JARDANA) SERVIDOR MONTIPED (MADRID) SERVIDOR MODULA SERVIDOR SERVIDOR PAGINA WEB SERVIDOR SERVIDOR PASSWORD SERVIDOR PC-SECURE SERVIDOR PREGADO (DIFECO) SERVIDOR SHSD SERVIDOR SRV802 (Plataforma de Backup) SERVIDOR SRV802 (Agente de Backup) SERVIDOR SVXVCENTER SERVIDOR AVAYA (TELEFONIA) LIBRERIA MSL 2024	Físico y Digital	Pérdida de la disponibilidad en los servicios de asesoramiento de la plataforma tecnológica.	Tecnológico	Daño del directorio activo de la entidad.	1. Fallos en la autenticación de los usuarios. 2. Inconformidad de los usuarios. 3. Crecimiento exponencial de solicitudes de soporte técnico. 4. Dificultades en la ejecución de los procesos de la entidad. 5. Incumplimiento legal/es. 6. Reprocesos.	Muy Bajo	20%	Mayor	80%	Alta	C-153	Detectivo	Manual	PO-GETI-003 Política de seguridad y privacidad de la información.	Continua	Con registro	6%	14%	80%	80%	Muy Bajo	Mayor	Alta	Reducir	151.1	El funcionario designado por el jefe de la DAPS monitorea frecuentemente los servicios dispuestos por la plataforma tecnológica. Como evidencia se deberá dejar registro de esta actividad a través de informes.	Leonarda Peña	1/2/2023	31/12/2023	
																										151.2	El Oficial de Seguridad designado por la Alta Dirección verifica el monitoreo realizado a los sistemas de información administrados por la DAPS de acuerdo a los informes presentados por el profesional designado. Como evidencia quedará a informe de monitoreo e informe de verificación.	Luis Osorio	1/2/2023	31/12/2023	*Realizar una revisión de cumplimiento con el jefe de la DAPS para que se tomen las medidas pertinentes.
																										154.1	El líder de infraestructura tecnológica define procedimiento interno para realizar la actualización de los sistemas de información de la entidad. Como evidencia de esta actividad se dejará el registro del procedimiento en ISOLUION.	Leonarda Peña	1/2/2023	31/12/2023	
																										154.2	El Oficial de Seguridad designado por la Alta Dirección a partir del procedimiento definido, valida las actualizaciones realizadas previamente a las actualizaciones de los sistemas de información. Como evidencia de esta actividad quedarán actas de reunión y/o memorias de apoyo.	Luis Osorio	1/2/2023	31/12/2023	
2	SERVIDOR ACTIVE DIRECTORY SERVIDOR MANTECIDA (M) SERVIDOR DISMISO (dfiles) SERVIDOR FILESERVER SERVIDOR HERCULES (Repentino de desarrollo) SERVIDOR SERVIDORES DE GESTION DOCUMENTAL SERVIDOR INTANET SERVIDOR ISOLACION SERVIDOR DISOLUWARE SERVIDOR GESTION DE SERVICIOS DE TI (JARDANA) SERVIDOR MODULA SERVIDOR SERVIDOR PAGINA WEB SERVIDOR SERVIDOR PASSWORD SERVIDOR PREGADO (DIFECO) SERVIDOR SHSD SERVIDOR SRV802 (Plataforma de Backup) SERVIDOR SRV802 (Agente de Backup) SERVIDOR SVXVCENTER SERVIDOR AVAYA (TELEFONIA) LIBRERIA MSL 2024 SERVIDOR SIMPLIFYV 380 010 SERVIDOR HIPERCONVERGENCIA 380 09 SERVIDOR STORE ONCE 5200 SERVIDOR ONACLE CIDA X7 SERVIDOR ONACLE CIDA X1	Físico y Digital	Pérdida de la confidencialidad de la información de la SES.	Tecnológico	Falta de monitoreo por parte de los administradores de los sistemas de información de la SES frente los permisos de acceso	1. Fallos en los aplicativos. 2. Inconformidad de los usuarios. 3. Crecimiento exponencial de solicitudes de soporte técnico. 4. Dificultades en la ejecución de los procesos de la entidad, generando reprocesos. 5. Incumplimiento legal/es.	Muy Bajo	20%	Mayor	80%	Alta	C-154	Detectivo	Manual	Documentado	Continua	Con registro	6%	14%	Muy Bajo	80%	80%	Mayor	Alta	Reducir	151.1	El Oficial de seguridad de la información, bimestralmente realiza monitoreo de los logs de acceso de los sistemas de información. Como evidencia quedará el informe de monitoreo.	Oficial de Seguridad	1/2/2023	31/12/2023	*Al no encontrarse personal de planta capacitado, realizar una contingencia de respaldo.
3	SERVIDOR ACTIVE DIRECTORY SERVIDOR MANTECIDA (M) SERVIDOR DISMISO (dfiles) SERVIDOR FILESERVER SERVIDOR HERCULES (Repentino de desarrollo) SERVIDOR SERVIDORES DE GESTION DOCUMENTAL SERVIDOR INTANET SERVIDOR ISOLACION SERVIDOR DISOLUWARE SERVIDOR GESTION DE SERVICIOS DE TI (JARDANA) SERVIDOR MODULA SERVIDOR SERVIDOR PAGINA WEB SERVIDOR SERVIDOR PASSWORD SERVIDOR PREGADO (DIFECO) SERVIDOR SHSD SERVIDOR SRV802 (Plataforma de Backup) SERVIDOR SRV802 (Agente de Backup) SERVIDOR SVXVCENTER SERVIDOR AVAYA (TELEFONIA) LIBRERIA MSL 2024 SERVIDOR STORE EASY 1660 SERVIDOR SIMPLIFYV 380 010 SERVIDOR HIPERCONVERGENCIA 380 09 SERVIDOR STORE ONCE 5200 SERVIDOR ONACLE CIDA X7	Físico y Digital	Pérdida de la integridad de la información registrada en los sistemas de información de la SES.	Tecnológico	Cambios no aprobados en la información registrada en los sistemas de información por parte de los administradores.	1. Sanciones legales 2. Daño en el sistema 3. Daños en los aplicativos 4. Dificultades en la ejecución de los procesos de la entidad, generando reprocesos. 5. Inconformidad de los usuarios. 6. Pérdida de confianza por parte del sector público vigilado	Muy Bajo	20%	Catastrófico	100%	Extrema	C-156	Detectivo	Automático	Documentado	Continua	Con registro	6%	14%	Muy Bajo	100%	100%	Catastrófico	Extremo	Reducir	156-1	El Oficial de seguridad de la información bimestralmente realiza una verificación del cumplimiento de los requisitos dispuestos en la declaración de aplicabilidad del anexo A de la ISO 27001:2013. Como evidencia quedará informe de verificación.	Oficial de Seguridad	1/8/2023	31/12/2023	*Al no encontrarse personal de planta capacitado, no existe una contingencia de respaldo.

Proceso (s) relacionado (s):
 Gestión de TI
 Elaboró: Luis Edwin Osorio - Oficial de Seguridad
 Revisó: Luis María Gabriela Gómez - Jefe Oficina Asesora de Planeación y Sistema
 Aprobó: