Plan de tratamiento de riesgos de seguridad digital/información

Fecha de aprobación por el CIGD - 20 de diciembre de 2024

Proceso: Luis Alberto Conde C. Oficial de Seguridad de la Información – Gerencia de Tecnología

Revisor: Francisco Andrés Rodríguez Ecco – Gerente de Tecnología / Comité Institucional de Gestión y Desempeño UAECD

Aprobó: Comité Institucional de Gestión y Desempeño UAECD

Fecha actualización: 2024-12-20

IDENTIFICACIÓN DEL RIESGO																														
PROCESO	OBJETIVO ESTRATÉGICO	OBJETIVO DEL PROCESO	CÓDIGO DEL RIESGO (Mi riesgo inicia con "RI" seguido del consecutivo de 01, 02, 03, 04, 05, 06, 07, 08 y 09)			Pregunta asociada / dato de información	Tipo de activo (Marcar solo activos de información)	Tipo de riesgo (Marcar solo activos de información)	DESCRIPCIÓN DEL RIESGO - RI si es FISICA, DIGITAL Riesgo de Gestión Posibilidad de ocurrencia (qué) - por (causa) - debido a (por qué) Riesgo de Seguridad de la Información Posibilidad de ocurrencia (qué) Pérdida de la Integridad/Disponibilidad/Confidencialidad (daño/consecuencia) debido a (causa/debilidad) Riesgo Fiscal Posibilidad de efecto dañoso sobre (Bienes/Dineros/Recursos Económicos) debido a ...	Factores de riesgo	Vulnerabilidades (Obligatorio activos de información)	Amenazas (Obligatorio activos de información)	No.	DESCRIPCIÓN DEL CONTROL Responsable + Acción + Complemento	Fecha de implementación del control	Actividades en caso de materialización (indicativas)	Zona de Riesgo Inherente	ZONA DE RIESGO FINAL	TRATAMIENTO	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD - PTRS Programación Cantidad de avance/ejecución por trimestre							
																									ACTIVIDADES	INDICADOR (Numerador / Denominador)	Meta Cantidad / Porcentaje	I TRIM	II TRIM	III TRIM	IV TRIM	RECURSOS	RESPONSABLES
Transversal	Implementar y consolidar un sistema de gestión de seguridad digital que permita el desarrollo de las competencias y conocimientos de un capital humano altamente calificado y los procesos optimizados y el uso de las TIC para la información para mejorar la satisfacción de las necesidades y expectativas de los grupos de valor.	No aplica	RI	TRAN	1	1. Ciberlitos de GGC 2. Ciberlitos de Dirección	Sensitivos	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de 1. Ciberlitos de GGC** **2. Ciberlitos de Dirección por a. Abuso de derechos** **b. Remoto o Corrupción de la información** **c. Fallas Humanas debido a a. Ausencia o inhabilidad segregación de derechos de acceso** **b. Desconocimiento de Políticas de seguridad de la información**	Tecnología	a. Ausencia o inhabilidad segregación de derechos de acceso b. Desconocimiento de Políticas de seguridad de la información	a. Abuso de derechos b. Remoto o Corrupción de la información c. Fallas Humanas	1	El Profesional de Informática y Sistemas revisa la inhabilidad de accesos, mediante una matriz de segregación de funciones, y genera un informe con los hallazgos encontrados y sugerencias para mejora de seleccionar 5. Control Preventivo y seguimiento permanente por parte del Oficial de Seguridad de la Información y Ciberseguridad, que se ejecuta cada vez que se requiera y/o cada vez que se presente un cambio en el rol de un funcionario, con el propósito de asegurar que la información a la entidad pueda ser consultada, modificada o eliminada por los usuarios que se encuentran autorizados.	5-1	Solicitar permiso de consulta de Archivos Digitales a la Dirección, enviar un informe de las posibles acciones de autoridades, a Administración del Oficial de GGC	Bajo	Bajo	Bajo	Aceptar	No	No								
				RI	TRAN	2	1. Ciberlitos de GGC 2. Ciberlitos Dirección	Sensitivos	Pérdida de disponibilidad	**Pérdida de Disponibilidad 1. Ciberlitos de GGC** **2. Ciberlitos Dirección por a. Remoto de información debido a a. Desconocimiento de las políticas de seguridad de la información** **b. Ausencia de controles de respaldo de información**	Tecnología	a. Desconocimiento de las políticas de seguridad de la información b. Ausencia de controles de respaldo de información	a. Remoto de información	2	El jefe de dependencia verifica mediante reportes de seguimiento (ejemplo: Tiempo de respuesta, Capacidad de almacenamiento, etc) que los servidores y/o equipos de cómputo de su área, cuenta con la capacidad requerida para el adecuado funcionamiento de los aplicativos, aplicando el formato establecido en la matriz de segregación de funciones y/o cada vez que se necesite solicitar acceso a los recursos tecnológicos, y/o cuando se presente cambio de rol de un funcionario, con el propósito de asegurar que el personal a la entidad pueda ser consultada, modificada o eliminada por los usuarios que se encuentran autorizados.	5-1	Solicitar la revisión mensual del reporte/log	Moderado	Moderado	Reducir (Mitigar)	Realizar trimestralmente revisiones mensuales de servicios de TI al respaldo que se realiza al Oficial de seguridad de la información y/o cada vez que se necesite solicitar acceso a los recursos tecnológicos	Seguimientos realizados / seguimientos programados SEGUIMIENTO	4	1	1	1	1	Recursos Humanos , Tecnologías	Gerente de Gestión Corporativa
																									Realizar trimestralmente revisiones mensuales de servicios de TI al respaldo que se realiza al Oficial de seguimiento de la información de la SG	Seguimientos realizados / seguimientos programados	4	1	1	1	1	Recursos Humanos , Tecnologías	Directores
				RI	TRAN	3	SharePoint Dirección	Sensitivos	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de SharePoint Dirección por a. Pérdida o hurto de información** **b. Espionaje remoto** **c. Corrupción de la información** **d. Desconocimiento de las políticas de seguridad de la información** **e. Ausencia de copias de respaldo** **f. Asignación errada de los derechos de acceso**	Tecnología	a. Desconocimiento de las políticas de seguridad de la información b. Ausencia de copias de respaldo c. Asignación errada de los derechos de acceso	a. Pérdida o hurto de información b. Espionaje remoto c. Corrupción de los datos	3	El administrador de plataforma de herramientas colaborativas cuando se requiera realizar configuración de herramientas, envía Pirola asignaturas la verificación/validación/segregación de información/herramientas colaborativas, mediante el correo de Microsoft Outlook, con el propósito de asegurar que la información a la entidad pueda ser consultada, modificada o eliminada por los usuarios que se encuentran autorizados.	5-1	Revisar/actualizar las herramientas colaborativas y información de acuerdo con la decisión que se pueda tomar en el comité Pirola con la Unidad	Moderado	Bajo	Aceptar	No	No								

			BS	GEDP	6	ejercicio de todos los servidores públicos de la ciudad. Son las siguientes: - Base de Datos Funcionarios(Excel) - Base de Datos Planta de personal (SIGEP)	Base de datos	Pérdida de Disponibilidad	**- Base de Datos Geodatabase(Arcgis (BDG)** **- Base de Datos Funcionarios(Excel) (BDF) por 1. Pérdida o hurto de información** **2. Acceso autorizado a los datos personales** **3. Pérdida, destrucción, acceso a uso no autorizado dádiva o 1. Los funcionarios de la entidad** **2. Acceso no autorizado a la información** **en la descripción de los cargos** **3. Ubicación en oficina de la información (mapas de los funcionarios)**	Talento humano	1. Responsabilidades en la seguridad de la información en la Descripción de los cargos 2. Ubicación en oficina de la información (mapas de los funcionarios)	1. Pérdida o hurto de datos personales 2. Acceso no autorizado a los datos personales 3. Pérdida, destrucción, acceso a uso no autorizado	6	El grupo de operadores de soft cada vez entra a bases de datos de respaldo y los pide dependencias a grupo de administradores de plataforma para que se tomen ¿¿ó ¿¿ó¿¿¿

E6	GEES	S	Credenciales de acceso a los Redes Sociales (Comunicaciones)	Sensibles	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e Integridad de Credenciales de acceso a las Redes Sociales (Comunicaciones) por 1. Falsificación de derechos** **2. Fallas Humanas debido a 1. Ausencia de mecanismos de identificación y autenticación, entre la autenticidad de usuario** **2. Desconocimiento de las políticas de seguridad y privacidad de la información** **3. Falta de monitoreo**	Talento humano	1. Ausencia de mecanismos de identificación y autenticación entre la autenticidad de usuario 2. Desconocimiento de las políticas de seguridad y privacidad de la información 3. Falta de monitoreo	1. Falsificación de derechos 2. Fallas Humanas	3	0.2	Revisión de la gestión de accesos a los sistemas	Bajo	Bajo	Aceptar	NA	NA								
												4	0.2																
												5	1																
												6	1																
E6	GEES	S	Credenciales de acceso a los Redes Sociales (Comunicaciones)	Sensibles	Pérdida de Disponibilidad	**Pérdida de disponibilidad de credenciales de acceso a las Redes Sociales (Comunicaciones) por 1. Ataques cibernéticos** **1a. Pérdida o borrado de la información.** **1 b. Mal funcionamiento del software** **2. Acceso no autorizado a cuenta de root principal** **3. Caducidad de la cuenta**	Talento humano	1. Ausencia de parámetros de seguridad 1a. Ausencia de copias de respaldo 2. Ausencia de control de accesos a los redes sociales	1. Ataques cibernéticos 1a. Pérdida o borrado de la información. 1b. Mal funcionamiento del software 2. Acceso no autorizado a cuenta de root principal	4	0.5	En caso que se llega a materializar el riesgo de ciberseguridad se debe de comunicar a la alta dirección y realizar la notificación al gobierno para que en escalamiento al colcert	Moderado	Bajo	Aceptar	NA	NA								
												5	0.5																
												6	1																
E6	GEES	X	Filezserver/empresa! (Comunicaciones)	Sensibles	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e Integridad de Filezserver temporal (Comunicaciones) por 1. Acceso autorizado de la información** **2. Fallas Humanas debido a 1. Ausencia de revisiones regulares por parte del jefe de dependencia** **2. Desconocimiento de políticas de seguridad y privacidad de la información**	Tecnología	1. Ausencia de revisiones regulares por parte del jefe de dependencia 2. Desconocimiento de políticas de seguridad y privacidad de la información	1. Uso no autorizado de la información 2. Fallas Humanas	7	0.2	Revisión de la gestión de accesos al Filz server	Alto	Bajo	Aceptar	NA	NA								
												8	0.2																
												9	0.2																
												10	1																
E6	GEES	X	Filezserver/empresa! (Comunicaciones)	Sensibles	Pérdida de Disponibilidad	**Pérdida de Disponibilidad de Filezserver temporal (Comunicaciones) por 1. Pérdida o acceso autorizado a información** **2. Fallas Humanas** **3. Incumplimiento en el mantenimiento del Filezserver debido a 1. Ausencia de parámetros de seguridad** **1a. Ausencia de copias de respaldo** **2. Desconocimiento de políticas de seguridad y privacidad de la información** **3. Ausencia de mantenimiento al Filezserver**	Tecnología	1. Ausencia de parámetros de seguridad 1a. Ausencia de copias de respaldo 2. Desconocimiento de políticas de seguridad y privacidad de la información 3. Ausencia de mantenimiento al Filezserver	1. Pérdida o acceso no autorizado a la información 2. Fallas Humanas 3. Incumplimiento en el mantenimiento del Filezserver	11 No 12	0.5	Restauración del respaldo del file server	Alto	Bajo	Aceptar	NA	NA								
												13	0.5																
												14	1 No 15																
												16	0.5																
												17	0.5																
												18	1 No 19																
												20	1 No 21																
E6	GEES	X	OneNote (Comunicaciones)	Sensibles	Pérdida de confidencialidad e Integridad	**Pérdida de confidencialidad e Integridad de OneNote (Comunicaciones) por 1. Pérdida o borrado de información** **2. Espionaje remoto** **3. Corrupción de los datos** **4. Sabotaje de la red debido a 1. Desconocimiento de las políticas de seguridad de la información** **2. Ausencia de monitoreo** **3. Ausencia de respaldo de la información** **4. Asignación errada de los derechos de acceso**	Tecnología	1. Desconocimiento de las políticas de seguridad de la información 2. Ausencia de monitoreo 3. Ausencia de respaldo de la información 4. Asignación errada de los derechos de acceso	1. Pérdida o borrado de información 2. Espionaje remoto 3. Corrupción de los datos	1	0.2	Restauración de las herramientas colaborativas a información de usuarios Formato que no coincide con el formato de la unidad	Moderado	Bajo	Aceptar	NA	NA								
												2	0.2																
												3	1																
												4	1																
												5	1																
												6	1																
												7	1																
												8	1																
E6	GEES	X	OneNote (Comunicaciones)	Sensibles	Pérdida de Disponibilidad	**Pérdida de Disponibilidad de OneNote (Comunicaciones) por 1. Pérdida o borrado de información** **2. Espionaje remoto** **3. Corrupción de los datos** **4. Sabotaje de la red debido a 1. Desconocimiento de las políticas de seguridad de la información** **2. Ausencia de monitoreo** **3. Ausencia de respaldo de la información** **4. Asignación errada de los derechos de acceso**	Tecnología	1. Desconocimiento de las políticas de seguridad de la información 2. Ausencia de monitoreo 3. Ausencia de respaldo de la información 4. Asignación errada de los derechos de acceso	1. Pérdida o borrado de información 2. Espionaje remoto 3. Corrupción de los datos 4. Sabotaje de la red	9	0.2	Restauración de las herramientas colaborativas a información de usuarios Formato que no coincide con el formato de la unidad	Moderado	Bajo	Aceptar	NA	NA								
												10	1																
												11	1																
												12	1																
												13	1																
E6	GEES	X	Fotografía - Realizador Audiovisual Comunicaciones Sociales	Recurso Humano	Pérdida de confidencialidad	**Pérdida de Confidencialidad de Fotografía - Realizador Audiovisual Comunicaciones Sociales por 1. Ataque de ingeniería social debido a 1. Desconocimiento de las políticas de seguridad de la información**	Talento humano	1. Desconocimiento de las políticas de seguridad de la información	1. Ataque de ingeniería social	14	1	Aplicar charlas de verificación ocular	Moderado	Bajo	Aceptar	NA	NA								
												15	1																
												16	1																
E6	GEES	M	Fotografía - Realizador Audiovisual Comunicaciones Sociales	Recurso Humano	Pérdida de Disponibilidad	**Pérdida de Disponibilidad de Fotografía - Realizador Audiovisual Comunicaciones Sociales por 1. Fuga de conocimiento debido a 1. Alta rotación del personal** **2. Desconocimiento de las políticas de seguridad y presentidad de la información**	Talento humano	1. Alta rotación del personal 2. Desconocimiento de las políticas de seguridad y presentidad de la información	1. Fuga de conocimiento	1	0.5	Contar mínimo dos personas capacitadas en una misma actividad	Bajo	Bajo	Aceptar	NA	NA								
												2	0.5																
												3	1																
E6	GEES	M	Gsapiad - Módulo de Facturación (GSAC) (Opción de elaboración de facturas conforme al procedimiento)	Software	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e Integridad de Gsapiad - Módulo de Facturación (GSAC)** **(Opción de elaboración de facturas conforme al procedimiento) por 1.Quejas y reclamos por prestación de servicios** **2. Pérdida de oportunidades de negocio** **3. Investigaciones por entes de control** **debido a** **1. Fallas en la asignación y control de privilegios y permisos en la plataforma** **2. Desconocimiento de políticas de seguridad de la información** **3. Fallas en la administración de la herramienta tecnológica**	Tecnología	1. Fallas en la asignación y control de privilegios y permisos en la plataforma 2. Desconocimiento de políticas de seguridad de la información 3. Fallas en la administración de la herramienta tecnológica	1.Quejas y reclamos por prestación de servicios 2. Pérdida de oportunidades de negocio 3. Investigaciones por entes de control	4	0.2	Revisión del reporte de errores generados desde la Subgerencia de Operaciones y Tecnología	Alto	Moderado	Reducir (mitigar)	1. Realizar capacitación en las funcionarios y periteos de seguridad de información. 1 por semestre	Cantidad de capacitaciones realizadas al equipo GSAC /2 capacitaciones al año	2		1		1	Recurso Humano Mesa de servicio tecnológica	Funcionario enterado de seguridad
												5	0.2																
												6	1										2. Realizar verificación comercial de proveedores. 1 por semestre. con el de licitador	Cantidad de verificaciones realizadas al equipo GSAC /2 proveedores al año	2		1		1	Recurso Humano Mesa de servicio tecnológica	Funcionario delegado por el responsable del proceso Funcionario delegado en equipo gestion de nuestras de TI
E6	GEES	M	Gsapiad - Módulo de Facturación (GSAC) (Opción de elaboración de facturas conforme al procedimiento)	Software	Pérdida de Disponibilidad	**Pérdida de Disponibilidad de Gsapiad - Módulo de Facturación (GSAC)** **(Opción de elaboración de facturas conforme al procedimiento) por 1. Quejas y reclamos sin clientes e intermedio** **2. Pérdida de oportunidad de negocio. debido a** **1. Falta de mantenimiento preventivo y correctivo.** **2. Falta de complitencia del modelamiento permanente de la plataforma** **3. Recurso tecnológico para atender incidentes excesos** **4. Falta de conexión con el proveedor**	Tecnología	1. Falta de mantenimiento preventivo y correctivo. 2. Falta de complitencia del modelamiento permanente de la plataforma 3. Recurso tecnológico para atender incidentes excesos 4.Falta de conexión con el proveedor	1. Quejas y reclamos sin clientes e intermedio 2. Pérdida de oportunidad de negocio.	7	0.2	El propietario del activo en caso de presentarse un incidente de seguridad informática. Tecnológica	Alto	Moderado	Reducir (mitigar)	Realizar mantenimiento preventivo de la plataforma	Cantidad de mantenimientos realizados /2 mantenimientos al año	2		1		1	Recurso Humano Mesa de servicio tecnológica	Funcionario liderar funcional de la GSAC
												8	0.2																
												9	1																
E6	GEES	M	Gsapiad - Módulo de Facturación (GSAC) (Opción de elaboración de facturas conforme al procedimiento)	Software	Pérdida de Disponibilidad	**Pérdida de Disponibilidad de Gsapiad - Módulo de Facturación (GSAC)** **(Opción de elaboración de facturas conforme al procedimiento) por 1. Ataques cibernéticos** **2. Quejas y reclamos sin clientes e intermedio** **3. Pérdida de oportunidad de negocio.** **1. Falta de mantenimiento preventivo y correctivo.** **2. Falta de complitencia del modelamiento permanente de la plataforma** **3. Recurso tecnológico para atender incidentes excesos** **4. Falta de conexión con el proveedor**	Tecnología	1. Falta de mantenimiento preventivo y correctivo. 2. Falta de complitencia del modelamiento permanente de la plataforma 3. Recurso tecnológico para atender incidentes excesos 4.Falta de conexión con el proveedor	1. Ataques cibernéticos 2. Quejas y reclamos sin clientes e intermedio 3. Pérdida de oportunidad de negocio.	10	0.2	Restauración del respaldo de la información (Modelo de facturación)	Moderado	Bajo	Aceptar	NA	NA								
												11	0.2																
												12	1																
												13	1																
E6	GEES	M	(Canales en línea GSAC-SINA)	Sensibles	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e Integridad de (Canales en línea GSAC-SINA) por** **1. Pérdida de la información.** **2. Suplantación de usuarios autorizados. 3. Ingresos no autorizados (usuarios clonados)** **5. Ataques cibernéticos internacionales** **debido a 1. Ausencia de controles de cuentas.** **2. Fallas en la asignación de privilegios y permisos en la plataforma.** **3. Disposición para ventiladas y ciudadanos por la misma opción** **4.Falta o debilidad de auditorías en el software**	Tecnología	1. Ausencia de controles de cuentas. 2. Fallas en la asignación de privilegios y permisos en la plataforma. 3. Disposición para ventiladas y ciudadanos por la misma opción 4.Falta o debilidad de auditorías en el software	1. Pérdida o modificación de la información 2. Suplantación de usuarios autorizados. 3. Ingresos no autorizados (usuarios clonados) 5. Ataques cibernéticos por parte internacionales	1		El propietario del activo en caso de presentarse un incidente de seguridad informática. Tecnología	Alto	Moderado	Reducir (mitigar)	Realizar mantenimiento preventivo de la plataforma	Cantidad de mantenimientos realizados /2 mantenimientos al año	2		1		1	Recurso Humano Mesa de servicio tecnológica	Funcionario liderar funcional de la GSAC
												2	1																
												3	1																
												4	1																
												5	1																
												6	1																
E6	GEES	M	(Canales en línea GSAC-SINA)	Sensibles	Pérdida de Disponibilidad	**Pérdida de Disponibilidad de (Canales en línea GSAC-SINA) por** **1. Quejas - reclamos por parte internacion** **2. Impacto en imagen institucional** **3. Fallas en conectividad por procedimiento debido a** **1. Falta de mantenimiento preventivo y correctivo y adaptativo.** **2. Falta de monitoreo permanente de la plataforma. que demanden internetnacia** **3.Falta de mecanismos que permitan restablecer el servicio en forma prioritaria**	Tecnología	1. Falta de mantenimiento preventivo y correctivo y adaptativo. 2. Falta de monitoreo permanente de la plataforma. que demanden internetnacia 3.Falta de mecanismos que permitan restablecer el servicio en forma prioritaria	1. Quejas - reclamos por parte internacion 2. Impacto en imagen institucional 3. Fallas en conectividad por procedimiento	7		Mantenimiento de la plataforma. Tecnología	Alto	Moderado	Reducir (mitigar)	Implementar mesa de ayuda especializada diagnostico mesa si se presenta cualquier operación o daño en tecnología a es por monitoreo	Informe de ejecución	1		1		1	Recurso Humano Mesa de servicio tecnológica	Funcionario liderar funcional de la GSAC
												8	1																
												9	1																
												10	1																
												11	1																
												12	1																
												13	1																

			R6	GEDI	J6	(Plataforma Tienda Virtual GCAE)	Servicios	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de (Plataforma Tienda Virtual GCAE) por :** **1.- Pérdida o modificación de la información.** **2.Suplantación de usuarios autenticados ingresos no autorizados** **3. Ataques y robos por partes interesadas debido a 1. Debilidad en parámetros de seguridad** **2.Debilidad en el control de autenticación de usuarios** **3.Falta de actualización de la plataforma** **4. Fallas en la conexión de las aplicaciones o sistemas que presten el producto**	Tecnología	1. Debilidad en parámetros de seguridad 2.Debilidad en el control de autenticación de usuarios 3.Falta de actualización de la plataforma 4.Fallas en la conexión de las aplicaciones o sistemas que presten el producto	1. 1. Pérdida o modificación de la información 2.Suplantación de usuarios autenticados ingresos no autorizados 3. Ataques y robos por partes interesadas	6	Desconectividad a la plataforma de tienda virtual	1	Revisión de avances de la plataforma como Reporte a seguridad digital según procedimiento	Alto	Bajo	Aceptar	No	No							
																		7	El sistema realiza la validación de la matrícula usuario, en ciertos periodos ,requiere haber logueado las cuentas. El usuario tiene su responsabilidad ,y ,ellimitarse directamente a cuentas	0,5												
																		8	El ciberatacante antes de entrar a la plataforma ,requiere haber logueado las cuentas. El usuario tiene su responsabilidad ,y ,ellimitarse directamente a cuentas	0,5												
																		9	El usuario ingresa con su tarjeta crédito , con ,ataques ,ingresos y ,vulnerabilidades ,en ,el sistema ,y ,el sistema ,y ,el ,usuario ,no ,tiene ,seguridad ,y ,vulnerabilidad ,en ,el ,sistema ,y ,el ,sistema ,y ,el ,usuario ,no ,tiene ,seguridad ,y ,vulnerabilidad	2,5												
																		10	Desprotección a la plataforma de tienda virtual	1												
																		11	Desprotección a la plataforma de tienda virtual	1												
																		12	Desconectividad a la plataforma de tienda virtual	1												
			R6	GEDI	J6	(Plataforma Tienda Virtual GCAE)	Servicios	Pérdida de Disponibilidad	**Pérdida de Disponibilidad de (Plataforma Tienda Virtual GCAE) por 1.- Ejecuta - ecriptores por interesados** **2. Adulteración de documentos** **3. Fallas en los proveedores de internet** **débiles.** **4. Falta de mantenimiento preventivo y correctivo monitoreo permanente de plataforma** **5. Fallas en la conexión con los sistemas o aplicaciones requeridas para disponer el producto (passarela de pagos, s/c, contragolpe) .** **6. Falta de recurso humano en tecnología para atender en TBG escalonada**	Tecnología	1. Falta de mantenimiento preventivo y correctivo monitoreo permanente de plataforma 2. Fallas en la conexión con los sistemas o aplicaciones requeridas para disponer el producto (passarela de pagos, s/c, contragolpe) . 3. Falta de recurso humano en tecnología para atender en TBG escalonada	1. Ejecuta - ecriptores por interesados 2. Adulteración de documentos 3. Fallas en los proveedores de internet	1	El ciberatacante logra de responsa a servicio tienda virtual, verificar, solicitudes de información ,también ,en ,el ,debido ,a ,falla ,en ,la ,plataforma, ,y ,no ,se ,registra ,tiene ,de ,servicio ,en ,5	1	Reporte por mesa de servicio para revisación de plataforma virtual	Alto	Moderado	Reducir (mitigar)	Ingeniero de iniciativa a TI para viabilidad de acuerdo de disposición de productos , con Compra determinada	1 mes a de servicio	1	1			Recurso Humano Mesa de servicio tecnológico	Funcionario Líder funcional de la GCAE
																		2	El ,ciberatacante ,logra ,de ,responsa ,a ,servicio ,tienda ,virtual, ,verificar, ,solicitudes ,de ,información ,también ,en ,el ,debido ,a ,falla ,en ,la ,plataforma, ,y ,no ,se ,registra ,tiene ,de ,servicio ,en ,5	1												
																		3	El ,ciberatacante ,logra ,de ,responsa ,a ,servicio ,tienda ,virtual, ,verificar, ,solicitudes ,de ,información ,también ,en ,el ,debido ,a ,falla ,en ,la ,plataforma, ,y ,no ,se ,registra ,tiene ,de ,servicio ,en ,5	1												
																		4	El ,ciberatacante ,logra ,de ,responsa ,a ,servicio ,tienda ,virtual, ,verificar, ,solicitudes ,de ,información ,también ,en ,el ,debido ,a ,falla ,en ,la ,plataforma, ,y ,no ,se ,registra ,tiene ,de ,servicio ,en ,5	1												
																		5	El ,ciberatacante ,logra ,de ,responsa ,a ,servicio ,tienda ,virtual, ,verificar, ,solicitudes ,de ,información ,también ,en ,el ,debido ,a ,falla ,en ,la ,plataforma, ,y ,no ,se ,registra ,tiene ,de ,servicio ,en ,5	1												
																		6	Desprotección a la plataforma de tienda virtual	1												
																		7	Desconectividad a la plataforma de tienda virtual	1												
Gestión estratégica de tecnología	Implementar y controlar un Modelo de gestión institucional que permita el desarrollo de las competencias y habilidades del recurso humano y la adopción de nuevas tecnologías y aplicaciones así como de las tecnologías de la información para mejorar la satisfacción de los requerimientos, expectativas de los grupos de valor.	Establecer proyectos estratégicos de Tecnologías de la información y las comunicaciones, fortalecimiento e implementación de nuevas tecnologías que permitan la adopción de nuevas aplicaciones así como el acceso, uso y apropiación de los sistemas, para el cumplimiento de los objetivos institucionales, bajo criterios de calidad, seguridad y pertinencia de la información y la continuidad de los servicios tecnológicos.	R6	GEDI	A	MESA DE SERVICIOS - CA	Software	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de MESA DE SERVICIOS - CA por 1. 2.Modificación, Borrado o Acceso no autorizado a la información desde el rol de administrador 3.Desconocimiento de políticas de seguridad relacionadas con el control de acceso a información clasificada o reservada. 5. Asignación errada de derechos o privilegios**	Tecnología	1. Defensas bien conocidas en el software 2.Desconocimiento de políticas de seguridad relacionadas con el control de acceso a información clasificada o reservada. 5. asignación errada de derechos o privilegios	1 y 5.Abuso de los derechos 2.Modificación, Borrado o Acceso no autorizado a la información desde el rol de admi ninistrador.	5	El ,ciberatacante ,ha ,logrado ,ingresar ,a ,la ,plataforma ,de ,mesa ,de ,servicios ,con ,el ,rol ,de ,administrador, ,ya ,que ,no ,se ,ha ,logrado ,identificar ,los ,servicios ,en ,las ,diferentes ,herramientas ,de ,seguridad ,informática ,y ,vulnerabilidades ,que ,se ,encuentran ,en ,la ,plataforma ,de ,mesa ,de ,servicios ,y

					Sector, Mapa de Automatizados, (Servicio)		Ciudadanía		Tecnología	1. Acceso de terceros 2. Daño físico 3. Ataques internos intencionales 4. Abuso de derechos 5. Fallas Humanas 6. Mal funcionamiento de IT 7. Ataques externos intencionales 8. Fallas Proveedores 9. Ataques internos intencionales 10. Fallas Proveedores 11. Fallas Humanas 12. Mal funcionamiento de IT	1. Acceso de terceros 2. Daño físico 3. Ataques internos intencionales 4. Abuso de derechos 5. Fallas Proveedores 6. Ataques internos intencionales 7. Fallas Proveedores 8. Fallas Humanas 9. Mal funcionamiento de IT	8	Hacer revisiones periódicas (diarias, semanal, quincenal)de que todos los servicios estan disponibles.	1	Evaluaciones periódicas realizadas que no presentan											
																9	Update disponibilidad de la plataforma tecnológica	1										
																6	Ejecutar actividades de mantenimiento de la infraestructura tecnológica	1										
			RS	CASE	3	Bases de Datos Automatizados 1. Bases de datos geográfica 2. Bases de datos geográfica de servicios públicos (Bases de Datos)	Bases de datos	Pérdida de confidencialidad	**Pérdida de confidencialidad e integridad de Bases de Datos Automatizados** **1. Bases de datos geográfica** **2. Bases de datos geográfica de servicios públicos** **(Bases de Datos) por 1. Abuso de derechos** **2. Perdida, Hurto o modificación de la información** **3. Falsificación de derechos.**	Tecnología	1. Asignación errada de permisos de acceso a través del administrador de la base de datos 2. Información Servicios Ciudadanos en Bases de datos 3. Gestión deficiente de las mantenciones de administración en la base de datos	1. Abuso de derechos 2. Perdida, Hurto o modificación de la información 3. Falsificación de derechos. 4. Fallas Humanas	1. El Director de Bases de Datos asigna de responsable de la base de datos a un funcionario de la Dirección de Bases de Datos, quien es el encargado de la administración de la base de datos y es el responsable de la información. La actividad se realiza por correo electrónico. El acceso que se otorga a los usuarios es de consulta y modificación de información, dependiendo de la información a consultar, se solicitan las modificaciones correspondientes. La evidencia del control quedará registrada en el formato de solicitud de cambios. 2. El encargado de la base de datos realiza copias de seguridad de la información, con el fin de que las dependencias accedan al proceso programado. Verifica las personas que acceden y los que no acceden a las actividades realizadas por dependencias y que no pertenezcan a funcionarios y contratistas. De igual manera programa y los funcionarios y contratistas, en cualquier actividad que se realice, se informan de la seguridad de la información. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios.	1	Mantener revisiones de actualización de la Dirección de Tecnología e Datos para mantenerse al tanto de las posibles vulnerabilidades que se presentan	Moderado	Bajo	Aceptar	No	No						
			RS	CASE	3	Bases de Datos Automatizados 1. Bases de datos geográfica 2. Bases de datos geográfica de servicios públicos (Bases de Datos)	Bases de datos	Pérdida de disponibilidad	**Pérdida de Disponibilidad de Bases de Datos Automatizados** **1. Bases de datos geográfica** **2. Bases de datos geográfica de servicios públicos** **(Bases de Datos) por 1. Mal funcionamiento del equipo y/o software** **2. Perdida de información** **3. Error en el Uso** **4. Ausencia de copias de respaldo** **5. Ausencia de mecanismos de monitoreo** **2. Ausencia de documentación** **2a Configuración incorrecta de parámetros** **3. Desconocimiento de políticas de seguridad de la información**	Tecnología	1. Ausencia de copias de respaldo 2. Ausencia de mecanismos de monitoreo 3. Ausencia de documentación 4. Configuración incorrecta de parámetros 5. Desconocimiento de políticas de seguridad de la información	1. Mal funcionamiento del equipo y/o software 2. Perdida de información 3. Error en el Uso	1. El jefe de dependencia revisa cada día el reporte de copias de respaldo y verifica que se hayan realizado las copias de seguridad de la información de acuerdo a las correspondencias, y la información está completa. El jefe de dependencia revisa la matriz y en caso de un siniestro informa a quien se modificaron, permanente, su evidencia queda registrada en la matriz de copias de respaldo. 2. El oficial de seguridad de la información revisa las diferentes programadas de actividades frente de seguridad de la información, con el fin de que las dependencias accedan al proceso programado. Verifica las personas que acceden y los que no acceden a las actividades realizadas por dependencias y que no pertenezcan a funcionarios y contratistas. De igual manera programa y los funcionarios y contratistas, en cualquier actividad que se realice, se informan de la seguridad de la información. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. 3. Los administradores de plataforma documentan cada uno su plataforma y que administración se debe realizar que son mantenimientos diariamente, semanal, quincenal, mensual, trimestral, semestral y anual. Los administradores de plataforma actualizan la información de la plataforma, con el fin de que la información sea la más reciente. Los administradores de plataforma documentan cada uno su plataforma y que administración se debe realizar que son mantenimientos diariamente, semanal, quincenal, mensual, trimestral, semestral y anual. Los administradores de plataforma actualizan la información de la plataforma, con el fin de que la información sea la más reciente. La evidencia del control quedará registrada en la herramienta Sibila y mantenimiento actualizado por el personal de TI. 4. Los administradores de plataforma documentan cada uno su plataforma que administración se debe realizar que son mantenimientos diariamente, semanal, quincenal, mensual, trimestral, semestral y anual. Los administradores de plataforma actualizan la información de la plataforma, con el fin de que la información sea la más reciente y cuentan con diferentes herramientas de administración. Son herramientas manejadas por personas de TI. Los administradores de plataforma documentan cada uno su plataforma que administración se debe realizar que son mantenimientos diariamente, semanal, quincenal, mensual, trimestral, semestral y anual. Los administradores de plataforma actualizan la información de la plataforma, con el fin de que la información sea la más reciente y cuentan con diferentes herramientas de administración. Son herramientas manejadas por personas de TI. La evidencia del control quedará registrada en la herramienta Sibila y mantenimiento actualizado por el personal de TI. 5. Los administradores de plataforma documentan cada uno su plataforma que administración se debe realizar que son mantenimientos diariamente, semanal, quincenal, mensual, trimestral, semestral y anual. Los administradores de plataforma actualizan la información de la plataforma, con el fin de que la información sea la más reciente y cuentan con diferentes herramientas de administración. Son herramientas manejadas por personas de TI. La evidencia del control quedará registrada en la herramienta Sibila y mantenimiento actualizado por el personal de TI.	1	Mantener revisiones de actualización de la Dirección de Tecnología e Datos para mantenerse al tanto de las posibles vulnerabilidades que se presentan	Moderado	Bajo	Aceptar	No	No						
			RS	CASE	3	1. Bases de Datos con información Personal entregada por Entidades públicas y privadas (Bases de Datos)	Bases de datos	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de 1. Bases de Datos con información Personal entregada por Entidades públicas y privadas** **(Bases de Datos) por 1. Pérdida, borrado o uso no autorizado de la información** **2. Fallas Humanas / error en el Uso debido a 1. Ausencia de control de acceso** **2. Desconocimiento de políticas de seguridad de la información**	Tecnología	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida, borrado o uso no autorizado de la información 2. Fallas Humanas / error en el Uso	1. El jefe de dependencia revisa cada día el reporte de copias de respaldo y verifica que se hayan realizado las copias de seguridad de la información de acuerdo a las correspondencias, y la información está completa. El jefe de dependencia revisa la matriz y en caso de un siniestro informa a quien se modificaron, permanente, su evidencia queda registrada en la matriz de copias de respaldo. 2. El oficial de seguridad de la información revisa las diferentes programadas de actividades frente de seguridad de la información, con el fin de que las dependencias accedan al proceso programado. Verifica las personas que acceden y los que no acceden a las actividades realizadas por dependencias y que no pertenezcan a funcionarios y contratistas. De igual manera programa y los funcionarios y contratistas, en cualquier actividad que se realice, se informan de la seguridad de la información. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. 3. El encargado de dominio cada uno que son usuarios identifica un grupo de contratistas que son los contratistas ya office que son usuarios autenticados en la red. El usuario accede con su contraseña a la red y a los recursos de la red. La evidencia del control quedará registrada en el dominio.	1	Mantener revisiones de actualización de la Dirección de Tecnología e Datos para mantenerse al tanto de las posibles vulnerabilidades que se presentan	Bajo	Bajo	Aceptar	No	No						
			RS	CASE	3	1. Bases de Datos con información Personal entregada por Entidades públicas y privadas (Bases de Datos)	Bases de datos	Pérdida de disponibilidad	**Pérdida de Disponibilidad de 1. Bases de Datos con información Personal entregada por Entidades públicas y privadas** **(Bases de Datos) por 1. Pérdida, borrado o uso no autorizado de la información** **2. Fallas Humanas / error en el Uso debido a 1. Ausencia de copias de respaldo en bases de datos**	Tecnología	1. Ausencia de copias de respaldo en bases de datos	1. Pérdida, borrado o uso no autorizado de la información	1. El jefe de dependencia revisa cada día el reporte de copias de respaldo y verifica que se hayan realizado las copias de seguridad de la información de acuerdo a las correspondencias, y la información está completa. El jefe de dependencia revisa la matriz y en caso de un siniestro informa a quien se modificaron, permanente, su evidencia queda registrada en la matriz de copias de respaldo. 2. El oficial de seguridad de la información revisa las diferentes programadas de actividades frente de seguridad de la información, con el fin de que las dependencias accedan al proceso programado. Verifica las personas que acceden y los que no acceden a las actividades realizadas por dependencias y que no pertenezcan a funcionarios y contratistas. De igual manera programa y los funcionarios y contratistas, en cualquier actividad que se realice, se informan de la seguridad de la información. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. 3. El profesional encargado de la base de datos realiza una actualización cada cierto tiempo de la información de la base de datos, con el fin de que la información sea la más reciente. La evidencia del control queda en el repositorio designado.	1	Mantener revisiones de actualización de la Dirección de Tecnología e Datos para mantenerse al tanto de las posibles vulnerabilidades que se presentan	Bajo	Bajo	Aceptar	No	No						
Gestión Administrativa y Financiera	Implementar y consolidar un modelo de gestión institucional que permita el fortalecimiento de competencias y conocimientos de los servidores públicos, la adopción de procesos optimizados y el uso de las tecnologías de información para mejorar la eficiencia, la productividad y expectativas de los grupos de valor.	Administrar los recursos financieros, mediante información presupuestal, contable y tesorería para apoyar el cumplimiento de la misión de la UAESP.	RS	GFPI	1	Expediente de Contratos	Información digital	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e Integridad de Expediente de Contratos por 1. Hurto, perdida o modificación de documentos.** **2. Fallas Humanas. Abdicta 1. Ausencia en el control de acceso al filesserver.** **2. Alojamiento errónea de permisos de acceso.** **3. Desconocimiento de políticas de seguridad de la información.**	Tecnología	1. Ausencia en el control de acceso al Filesserver. 2. Alojamiento errónea de permisos de acceso. 3. Desconocimiento de políticas de seguridad de la información.	1. Hurto, perdida o modificación de documentos. 2. Abuso de derechos. 3. Fallas Humanas.	1. Se debe mantener revisiones de actualización de la información y actividades. El control operativo que se mantiene entre el oficial de seguridad de la información y los funcionarios y contratistas. Los gestores deben programar y los funcionarios y contratistas, en cualquier actividad que se realice, se informan de la seguridad de la información. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. 2. El oficial de seguridad de la información revisa las diferentes programadas de actividades frente de seguridad de la información, con el fin de que las dependencias accedan al proceso programado. Verifica las personas que acceden y los que no acceden a las actividades realizadas por dependencias y que no pertenezcan a funcionarios y contratistas. Los gestores deben programar y los funcionarios y contratistas, en cualquier actividad que se realice, se informan de la seguridad de la información. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. Adicionalmente se genera reconocimiento.	1	El jefe de dependencia registra la solicitudes en la mesa de servicios de TI, para restablecer el servicio	Moderado	Moderado	Reducir (mitigar)	Continuar refiriendo los sombreros mentirosos y alegre evidencia de la información que los funcionarios y contratistas deben de mantener en secuencia y proporcionar de acuerdo con como sucia establecido en el instructivo de información digital.	Informes trimestrales sobre el seguimiento de la información que los funcionarios y contratistas deben de mantener en secuencia y proporcionar de acuerdo con el instructivo de información digital.	4 reportes enviados, 24 reportes programados "100	4	1	1	1	1	Personas Humanas, Técnicas y Tecnológicas	Subgerencia Administrativa y Financiera
																2	Planillas programadas / Planillas Elaboradas.	1										
			RS	GFPI	2	Expediente de Contratos	Información digital	Pérdida de disponibilidad	**Pérdida de Disponibilidad de Expediente de Contratos por 1. Fallas Humanas.** **2. Ataques Internos.** **3. Pérdida de información.** **4. Fallas Humanas. Abdicta 1. Errores de información (Indiga datos personales) por error humano.** **2. Ataque Internos de información.** **3. Ausencia de copias de respaldo.** **4. Desconocimiento de políticas de seguridad de la información.**	Tecnología	1. Errores de información (Indiga datos personales) por error humano. 2. Ataque Internos de información. 3. Ausencia de copias de respaldo o backups de la información. 4. Desconocimiento de políticas de seguridad de la información.	1. Fallas Humanas. 2. Gestiones de Intereses. 3. Pérdida de información. 4. Fallas Humanas.	1. El jefe de dependencia revisa cada día el reporte de copias de respaldo y verifica que se hayan realizado las copias de seguridad de la información de acuerdo a las correspondencias, y la información está completa. El jefe de dependencia revisa la matriz y en caso de un siniestro informa a quien se modificaron, permanente, su evidencia queda registrada en la matriz de copias de respaldo. 2. El oficial de seguridad de la información revisa las diferentes programadas de actividades frente de seguridad de la información, con el fin de que las dependencias accedan al proceso programado. Verifica las personas que acceden y los que no acceden a las actividades realizadas por dependencias y que no pertenezcan a funcionarios y contratistas. De igual manera programa y los funcionarios y contratistas, en cualquier actividad que se realice, se informan de la seguridad de la información. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. La evidencia del control quedará registrada en el correo enviado y en el formato de solicitud de cambios. 3. El encargado de dominio cada uno que son usuarios identifica un grupo de contratistas que son los contratistas ya office que son usuarios autenticados en la red. El usuario accede con su contraseña a la red y a los recursos de la red. La evidencia del control quedará registrada en el dominio.	1 1 1

								1. Ausencia de control de acceso a la información digital. 2. Deficiencia en la adquisición de permisos. 3. Desconocimiento de políticas de seguridad de la información.	políticas de seguridad de la información	1. Ausencia de información digital Abuso de derechos. 3. Fallas Humanas.	1 2 3	1.2	Gestión Documental	Moderado	Bajo	Aceptar										
			EG	GIRI	A	Filoscanner de SAF - Financiero	Servicios	Pérdida de Disponibilidad	Pérdida de Disponibilidad de Filoscanner de SAF - Financiero por 1. Pérdida o alteración de la información. 2. Fallas Humanas. debido a 1. Ausencia de copias de respaldo. 2. Desconocimiento de políticas de seguridad de la información. 3. Ausencia de planes de contingencia.	1. Ausencia de copias de respaldo. 2. Desconocimiento de políticas de seguridad. 3. Ausencia de planes de contingencia.	Tecnología	1. Pérdida o borrado de la información. 2. Fallas Humanas.	1 2 3	1.2	Restauración de la información del - Filoscanner	Moderado	Bajo	Aceptar	No.	No.								
			EG	GIRI	B	Equipos de Financiera	Hardware	Pérdida de Disponibilidad	Pérdida de confidencialidad e integridad de Equipos de Financiera por 1. Pérdida o modificación de información. 2. Fallas Humanas. debido a 1. Ausencia de control de acceso. 2. Desconocimiento de políticas de seguridad de la información.	1. Ausencia de control de acceso. 2. Desconocimiento de políticas de seguridad de la información.	Tecnología	1. Pérdida o modificación de información. 2. Fallas Humanas.	1 2 3	1	Registrar la solicitud en la mesa de servicios de TI, para restablecer un Equipo PC	Moderado	Bajo	Aceptar	No.	No.								
			EG	GIRI	M	Equipos de Financiera	Hardware	Pérdida de Disponibilidad	Pérdida de Disponibilidad de Equipos de Financiera por 1. Pérdida o borrado de información. 2. Fallas Humanas. debido a 1. Ausencia de copias de respaldo. 2. Desconocimiento de políticas de seguridad de la información. 3. Ausencia de planes de contingencia. 4. Mantenimiento insuficiente / Instalación fallida de hardware o software. 5. Desconocimiento	1. Ausencia de copias de respaldo. 2. Desconocimiento de políticas de seguridad de la información. 3. Ausencia de planes de contingencia. 4. Mantenimiento insuficiente / Instalación fallida de hardware o software. 5. Desconocimiento	Tecnología	1. Pérdida o borrado de información. 2. Fallas Humanas. 3. Incumplimiento en el mantenimiento de los equipos de cómputo.	1 2 3 4 5	1	Registrar la solicitud en la mesa de servicios de TI, para restablecer un Equipo PC	Moderado	Bajo	Aceptar	No.	No.								
			EG	GIRI	M	Funcionarios de Financiera	Recurso Humano	Pérdida de Disponibilidad	Pérdida de confidencialidad e integridad	1. Incumplimiento en la disciplina del personal. 2. Error en uso. debido a 1. Ausencia del personal. 2. Desconocimiento de la seguridad. 3. Falta de conciencia acerca de la seguridad.	Talento humano	1. Incumplimiento en la disciplina del personal. 2. Error en uso.	1 2 3	1.2	Contar mínimo dos personas que realicen una misma actividad	Moderado	Bajo	Aceptar	No.	No.								
			EG	GIRI	M	Funcionarios de Financiera	Recurso Humano	Pérdida de Disponibilidad	Pérdida de Disponibilidad de Funcionarios de Financiera por 1. Pérdida, fuga de información. 2. Desuso de información. debido a 1. Afectación de personal especializado. 2. Falta de conciencia acerca de la seguridad.	1. Afectación de personal especializado. 2. Falta de conciencia acerca de la seguridad.	Talento humano	1. Pérdida, fuga de información. 2. Desuso de información a terceros.	1 2 3	1.2	Contar mínimo dos personas que realicen una misma actividad	Bajo	Bajo	Aceptar	No.	No.								
			EG	GIRI	M	BOGDATA	Servicios	Pérdida de Disponibilidad	Pérdida de confidencialidad e integridad	Pérdida de confidencialidad e integridad de BOGDATA por 1. Pérdida o modificación de información. 2. Fallas Humanas. debido a 1. Ausencia de control de acceso. 2. Desconocimiento de políticas de seguridad de la información.	Cuerpo externo	1. Ausencia de control de acceso. 2. Desconocimiento de políticas de seguridad de la información.	1 2 3	1	Solicitud de soporte o renovación a SIG	Moderado	Moderado	Reducir (mitigar)	Realizar reporte trimestral sobre mantenimiento de equipos informáticos	Reportes recibidos / reportes programados	4	1	1	1	1	Recursos Humanos, Técnicos y Tecnológicos	Subgerente Administrativa y Financiera
			EG	GIRI	M	BOGDATA	Servicios	Pérdida de Disponibilidad	Pérdida de Disponibilidad de BOGDATA por 1. Pérdida o borrado de información. 2. Fallas Humanas. debido a 1. Ausencia de copias de respaldo por parte de OTI 2. Desconocimiento de políticas de seguridad de la	1. Ausencia de copias de respaldo por parte de OTI 2. Desconocimiento de políticas de seguridad de la	Cuerpo externo	1. Pérdida o borrado de información. 2. Fallas Humanas.	1 2 3	1.2	Solicitud de soporte o renovación a SIG	Moderado	Bajo	Aceptar	No.	No.								
Gestión Documental	implementar y consolidar un modelo de gestión documental que permita el desarrollo de las funciones de preservación de el capital humano y la memoria institucional, mediante instrumentos archivísticos que permitan el uso de las tecnologías de la información para mejorar la calidad de los procesos y satisfacer las expectativas de los grupos de valor.	administrar la gestión documental de la entidad mediante la actualización de políticas, planes, programas y instrumentos archivísticos que permitan la adecuada administración de la documentación funcionaria y ciudadana a los grupos de interés, con el fortalecimiento a la cultura de la gestión, asegurando la información como un activo institucional.	EG	GDOC	A	1. COMUNICACIONES OFICIALES RECIBIDAS 2. INVENTARIOS DOCUMENTALES CENTRO DOCUMENTAL	Información analógica	Pérdida de confidencialidad e integridad	Pérdida de confidencialidad e integridad de 1. COMUNICACIONES OFICIALES RECIBIDAS 2. INVENTARIOS DOCUMENTALES CENTRO DOCUMENTAL por 1. Pérdida de información. 2. Desfoliación material. 3. Fallas Humanas 4. Eliminación de Documentos. 5. Fallas Humanas en la ejecución de procesos técnicos debido a 1. Ausencia de Controles de acceso físico inadecuados. 2. Controles de acceso lógicos inadecuados. 3. Desconocimiento de Políticas de Seguridad de la información	Cuerpo externo	1. Trabajo no supervisado de personal de aseo y/o limpieza. 2. Controles de acceso físico inadecuados. 3. Desconocimiento de Políticas de Seguridad de la información	1. Hurto de documentos. 2. Desfoliación no controlada. 3. Fallas Humanas 4. Eliminación de documentos. 5. Fallas Humanas en la ejecución de procesos técnicos	1 2 3 4 5	1	Desarrollar mesas de trabajo mensual con la Gerencia de Tecnología para articular la gestión para mitigar el riesgo	Moderado	Moderado	Reducir (mitigar)	Realizar correcciones en el formato de inventarios documentales y/o formato de inventario documental para evitar la pérdida de confidencialidad e integridad	Charlas Realizadas / Charlas Programadas	2	1		1		Recursos Humanos y Tecnológicos	Líder de proceso Gestión Documental
			EG	GDOC	A	1. COMUNICACIONES OFICIALES RECIBIDAS 2. INVENTARIOS DOCUMENTALES CENTRO DOCUMENTAL	Información analógica	Pérdida de Disponibilidad	Pérdida de Disponibilidad de 1. COMUNICACIONES OFICIALES RECIBIDAS 2. INVENTARIOS DOCUMENTALES CENTRO DOCUMENTAL por 1. Hurto de Documentos, desaparición extraviada. 2. Fallas Humanas debido a 1. Controles de acceso físico inadecuados. 2. Desconocimiento de Políticas de Seguridad	Cuerpo externo	1. Controles de acceso físico inadecuados. 2. Desconocimiento de Políticas de Seguridad	1. Hurto de Documentos, desaparición no controlada	1 2	1	Desarrollar mesas de trabajo mensual con la Gerencia de Tecnología para articular la gestión para mitigar el riesgo	Moderado	Moderado	Reducir (mitigar)	Realizar correcciones en el formato de inventarios documentales y/o formato de inventario documental para evitar la pérdida de confidencialidad e integridad en los inventarios (archivos físicos) (carpetas de documentos)	Charlas Realizadas / Charlas Programadas	2	1		1		Recursos Humanos y Tecnológicos	Líder de proceso Gestión Documental
			EG	GDOC	A	1. Cuadro de Clasificación (SACI) 2. Cuadro de Clasificación (SACI) 3. Inventarios	Software	Pérdida de confidencialidad e integridad	Pérdida de confidencialidad e integridad de 1. Cuadro de Clasificación (SACI) 2. Cuadro de Clasificación (SACI) 3. Inventarios por 1. Borrado, pérdida y modificación de información 2. Fallas Humanas 3 y 4. Abuso de Derechos debido a 1. Ausencia de Controles de Acceso 2. Desconocimiento de Políticas de Seguridad de la información 3. Deficiencias bien comunicadas en el software 4. Ausencia de pistas de auditoría 5. 6. Inexistencia de los procedimientos de preservación digital 7. Falta de conocimientos de los conceptos básicos de la preservación digital a largo plazo 8. Desconocimiento del volumen real de los documentos objeto de preservación 9. No aplicación de las Tablas de Retención Documental. TRD. 10. Lineamientos técnicos incompletos	Tecnología	1. Ausencia de Controles de Acceso 2. Desconocimiento de políticas de seguridad de la información 3. Deficiencias bien comunicadas en el software 4. Ausencia de pistas de auditoría 5. Inexistencia de los procedimientos de preservación digital 6. Falta de conocimientos de los conceptos básicos de la preservación digital a largo plazo 7. Desconocimiento del volumen real de los documentos objeto de preservación 8. No aplicación de las Tablas de Retención Documental. TRD. 9. Lineamientos técnicos	1. Borrado, pérdida y modificación de la información 2. Fallas Humanas y 3. Abuso de Derechos	1 2 3 4 5 6 7 8 9 10	1.2 0.5 1	Desarrollar mesas de trabajo mensual con la Gerencia de Tecnología para articular la gestión para mitigar el riesgo	Moderado	Bajo	Aceptar	No.	No.								
			EG	GDOC	A	1. Cuadro de Clasificación (SACI) 2. Cuadro de Clasificación (SACI) 3. Inventarios	Software	Pérdida de Disponibilidad	Pérdida de Disponibilidad de 1. Cuadro de Clasificación (SACI) 2. Cuadro de Clasificación (SACI) 3. Inventarios por 1. Pérdida de información. 2. Fallas Humanas. debido a 1. Ausencia de Copias de Respaldo Controlador 2. Fallas tecnológicas. debido a 1. Ausencia de Copias de Respaldo 2. Ausencia de planes de contingencia 3. Deficiencias bien comunicadas del software 4. Parametrización inadecuada del Software 5. 6. Inexistencia de los procedimientos de preservación digital 7. Falta de conocimientos de los conceptos básicos de la preservación digital a largo plazo Controlador 8. Falta de personal especializado en el MCC debido a su nivel de complejidad	Tecnología	1. Ausencia de Copias de Respaldo 2. Ausencia de planes de contingencia 3. Deficiencias bien comunicadas del software 4. Parametrización inadecuada del Software 5. 6. Inexistencia de los procedimientos de preservación digital 7. Falta de conocimientos de los conceptos básicos de la preservación digital a largo plazo Controlador 8. Falta de personal especializado en el MCC debido a su nivel de complejidad	1. Pérdida o destrucción de información con / sin intervención por parte de usuario Controlador 2. Fallas tecnológicas.	1 2 3 4 5 6 7 8	1.2 0.5 1 1 1 1 1 1	Desarrollar mesas de trabajo mensual con la Gerencia de Tecnología para articular la gestión para mitigar el riesgo	Alto	Bajo	Aceptar	No.	No.								
			EG	GDOC	S	1. Archivos Central 2. Gestor Documental (Archivo Intermedio)	Interacciones	Pérdida de confidencialidad e integridad	Pérdida de confidencialidad e integridad 1. Archivo Central 2. Gestor Documental (Archivo Intermedio) por 1. Pérdida, destrucción de documentos 2. Fallas Humanas debido a 1. Uso inadecuado o descuidado del control de acceso físico a las edificaciones y/o recintos 2. Desconocimiento de Políticas de Seguridad	Cuerpo externo	1. Uso inadecuado o descuidado del control de acceso físico a las edificaciones y/o recintos 2. Desconocimiento de Políticas de Seguridad	1. Pérdida, destrucción de documentos 2. Fallas Humanas	1 2 3 4 5 6 7 8	1.2 0.5 1 1 1 1 1 1	Desarrollar mesas de trabajo mensual con la Gerencia de Tecnología para articular la gestión para mitigar el riesgo	Moderado	Moderado	Reducir (mitigar)	Realizar correcciones en el formato de inventarios documentales y/o formato de inventario documental para evitar la pérdida de confidencialidad e integridad	Charlas Realizadas / Charlas Programadas	2	1		1		Recursos Humanos y Tecnológicos	Líder de proceso Gestión Documental
			EG	GDOC	S	1. Archivos Central 2. Gestor Documental (Archivo Intermedio)	Interacciones	Pérdida de Disponibilidad	Pérdida de Disponibilidad de 1. Archivo Central 2. Gestor Documental (Archivo Intermedio) por 1. Inundación 2. Pérdida, hurto o destrucción de documentos 3.Pérdida o destrucción de información con / sin intervención por parte de usuario 4. Extravío del sistema de información accidental. 5. Fallas Humanas debido a 1. Ubicación en zon zonas susceptibles de inundación 2. Ausencia de protección física de la edificación, puertas y	Cuerpo externo	1. Ubicación en zon zonas susceptibles de inundación 2. Ausencia de protección física de la edificación, puertas y ventanas 3. Ausencia de Controles de Acceso a ambientes de almacenamiento de Tablas de Control de Acceso. TCA.	1. Inundación 2. Pérdida, hurto o destrucción de documentos 3.Pérdida o destrucción de información con / sin intervención por parte de usuario 4. Extravío del sistema de información accidental.	1 2 3 4 5 6 7 8	1.2 0.5 1 1 1 1 1 1	Desarrollar mesas de trabajo mensual con la Gerencia de Tecnología para articular la gestión para mitigar el riesgo	Moderado	Moderado	Reducir (mitigar)	Realizar correcciones en el formato de inventarios documentales y/o formato de inventario documental para evitar la pérdida de disponibilidad de	Charlas Realizadas / Charlas Programadas	2	1		1		Recursos Humanos y Tecnológicos	Líder de proceso Gestión Documental

Gestión de servicios administrativos	Implementar y normalizar un sistema de gestión institucional que permita el desarrollo de las competencias y características de los servidores públicos, a la adopción de procesos optimizados y el uso de las herramientas de la información para mejorar la satisfacción de las necesidades y expectativas de los grupos de valor.	Garantizar el suministro de los bienes y servicios de infraestructura y los servicios administrativos, así como propiciar los impactos ambientales y ergonómicos a actividades que se desarrollan, con el fin de apoyar el cumplimiento de la misión de la entidad	R1	GSA6	1	Control de accesos Sistema Biométrico SIGAPTIA-ERP- SIA-SAE SIGAPTIA-ERP- GPROY (Software)	Software	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e Integridad Control de acceso Sistema Biométrico** **SIGAPTIA-ERP- SIA-SAE** **SIGAPTIA-ERP- GPROY** **(Software)** **por 1. Ataques cibernéticos.** **2. Pérdida, consultificación de la información.** **3. Suplantación de usuarios autorizados.** **4. Error en el uso / Fallas humanas. 5. Debilidad en parámetros de seguridad.** **6. Fallas en la asignación de privilegios y permisos en la aplicación.** **7. Defectos conocidos en software.** **8. Desconocimiento de políticas de seguridad de la información.** **9. Falta de mantenimientos preventivos y correctivos.**	Tecnología	1. Debilidad en parámetros de seguridad. 2. Fallas en la asignación de privilegios y permisos en la aplicación. 3. Desconocimiento de políticas de seguridad de la información. 4. Desconocimiento de políticas de seguridad de la información. 5. Falta de mantenimientos preventivos y correctivos	1. Ataques cibernéticos. 2. Pérdida de información. 3. Error en el uso / Fallas Humanas	1	Revisar acceso de usuarios, verificando que el usuario que se encuentra en el aplicativo de Control de Acceso, sea el mismo que se encuentra en la base de datos, con el fin de verificar los permisos y accesos asignados al mismo. En caso de que los credenciales de acceso no pertenezcan a un usuario activo, se debe proceder a bloquear el acceso a la información y/o aplicativo. Lo anterior, con el fin de evitar la materialización de riesgos y/o pérdida de activos de información.	1.5	Revisar acceso de usuarios, verificando que el usuario que se encuentra en el aplicativo de Control de Acceso, sea el mismo que se encuentra en la base de datos, con el fin de verificar los permisos y accesos asignados al mismo. En caso de que las

			R1	GD06	08	Mesa de Servicios de la Dirección de Contratación	Servicios	Pérdida de Disponibilidad	**2.y 3.Error en el uso.** **- Indisponibilidad de la mesa de servicio de TI, debidos a 1. Actualización de las políticas de roques de respaldo.** **1a. Ausencia de mecanismos de monitoreo** **2. Ausencia de documentación** **2aConfiguración incorrecta de parámetros** **3. Ausencia de recurso humano especializado que conozca el manejo completo de la herramienta.** **4. Ausencia de planes de contingencia**	Tecnología	1. Ausencia de mecanismos de monitoreo 2. Ausencia de documentación 2a.Configuración incorrecta de parámetros 3. Ausencia de recurso humano especializado que conozca el manejo completo de la herramienta.	Mesa de servicios no es accesada a la información 1a. 2a. 3 Mesa de servicios 2.y 3.Error en el uso Indisponibilidad de la Mesa de servicio de TI.	1	El administrador de la plataforma documenta cada caso que se presenta en la herramienta GLPI, en donde se registra la fecha de la solicitud, el nombre del usuario que reporta el caso, el tipo de incidente, la descripción del caso, el nombre del administrador de plataforma, el tiempo de atención, la prioridad, la fecha de cierre y la solución del caso. Se evidencia que no se cuenta con un formato que permita la documentación de los mantenimientos preventivos, se evidencia que no registraron una mesa de ayuda para el mantenimiento preventivo.	1	Revisaremos de las configuraciones de la herramienta.	Moderado	Bajo	Aceptar								
			R1	GD06	01	Pandora - Módulo de Contratación	Servicios	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de Pandora - Módulo de Contratación por: a. Pérdida, corrupción, o modificación no autorizada de la información.** **b. Explotaje remoto** **c. Fallas Humanas, Error en el uso debidos a. Deficiencia en la satisfacción de pruebas y acceso de la información.** **d. Acceso intencionado por parte de personal no autorizado.** **e. Ausencia o insuficiencia de pruebas de software** **d. Defectos bien conocidos en el software**	Tecnología	c. Deficiencia en la satisfacción de pruebas y acceso de la información. d. Acceso intencionado por parte de personal no autorizado. e. Ausencia o insuficiencia de pruebas de software d. Defectos bien conocidos en el software	b. Pérdida, corrupción, o modificación no autorizada de la información. b. Explotaje remoto c. Fallas Humanas, Error en el uso	1	El administrador de la plataforma documenta cada caso que se presenta en la herramienta GLPI, en donde se registra la fecha de la solicitud, el nombre del usuario que reporta el caso, el tipo de incidente, la descripción del caso, el nombre del administrador de plataforma, el tiempo de atención, la prioridad, la fecha de cierre y la solución del caso. Se evidencia que no se cuenta con un formato que permita la documentación de los mantenimientos preventivos, se evidencia que no registraron una mesa de ayuda para el mantenimiento preventivo.	1	Revisaremos de la configuración de la herramienta e información.	Moderado	Bajo	Aceptar	No	No						
			R1	GD06	02	Pandora - Módulo de Contratación	Servicios	Pérdida de Disponibilidad	**Pérdida de Disponibilidad de Pandora - Módulo de Contratación por: a. Pérdida, corrupción, o modificación no autorizada de la información.** **b. Explotaje remoto** **c. Fallas Humanas, Error en el uso debidos a. a. Acceso intencionado por parte de personal no autorizado. e.Infraestructura del Sistema** **b. Ausencia o insuficiencia de pruebas de software** **c Defectos bien conocidos en el software**	Tecnología	a. Acceso intencionado por parte de personal no autorizado. e. Infraestructura del Sistema b. Ausencia o insuficiencia de pruebas de software c. Defectos bien conocidos en el software	b. Pérdida, corrupción, o modificación no autorizada de la información. b. Explotaje remoto c. Fallas Humanas, Error en el uso	1	El administrador de la plataforma documenta cada caso que se presenta en la herramienta GLPI, en donde se registra la fecha de la solicitud, el nombre del usuario que reporta el caso, el tipo de incidente, la descripción del caso, el nombre del administrador de plataforma, el tiempo de atención, la prioridad, la fecha de cierre y la solución del caso. Se evidencia que no se cuenta con un formato que permita la documentación de los mantenimientos preventivos, se evidencia que no registraron una mesa de ayuda para el mantenimiento preventivo.	1	Revisaremos de la configuración de la herramienta e información.	Moderado	Bajo	Aceptar	No	No						
			R1	GD06	03	Filenuver	Servicios	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de Filenuver por 1.Acceso no autorizado a la información** **2. Fallas Humanas** **3. Fallas técnicas** **debidos a 1. Ausencia de mecanismo regulares por parte del jefe de dependencia** **2.Desconocimiento de políticas de seguridad de la información**	Tecnología	1. Ausencia de mecanismo regulares por parte del jefe de dependencia 2.Desconocimiento de políticas de seguridad de la información	1.Acceso no autorizado de la información 2. Fallas Humanas 3. Fallas técnicas	1	El propietario del activo solicita que se registre un incidente de seguridad debido a reportes y/o sugerencias de terceros, se registra en Filenuver mismo y se evidencia que cuenta con un reporte registrado en la Mesa de Servicios de TI.	1	Revisión periódica de los usuarios que tienen acceso a la información	Moderado	Bajo	Aceptar	Realizar migración al repositorio de información digital.	Reporte de la depuración del Filenuver de la Subgerencia de Contratación.	2		1		1	Recursos Humanos, Tecnológicos	Subgerente de Contratación
			R1	GD06	04	Filenuver	Servicios	Pérdida de Disponibilidad	**Pérdida de Disponibilidad de Filenuver por Pérdida o acceso no autorizado a la información** **Fallas Humanas** **Insuficiencias en el mantenimiento del Filenuver debido a 1. Ausencia de copias de respaldo** **2.Desconocimiento de políticas de seguridad de la información** **3. Ausencia de mantenimiento al Filenuver**	Tecnología	1. Ausencia de copias de respaldo 2.Desconocimiento de políticas de seguridad de la información 3. Ausencia de mantenimiento al Filenuver	Pérdida o acceso no autorizado a la información Fallas Humanas Insuficiencias en el mantenimiento del Filenuver	1	El Responsable Información / Administrador de Carpetas realiza la actividad de acceso a la información de la carpeta de Filenuver, de acuerdo a los lineamientos establecidos por parte del personal técnico. El propietario de carpeta / administrador de carpetas realiza el registro de la actividad de acceso a la información de la carpeta de Filenuver, y que sea la que corresponda con la información registrada en la Mesa de Servicios de TI.	1	Revisión periódica de los usuarios que tienen acceso a la información y control de cambios	Moderado	Bajo	Aceptar	No	No						
Gestión Jurídica	Implementar y consolidar un modelo de gestión institucional que permita el desarrollo de las competencias y capacidades del recurso humano, la adopción de buenas prácticas, optimización y el uso de las Tecnologías de la Información para mejorar la satisfacción de los ciudadanos y grupos de interés y grupos de valor.	Fortalecer jurídicamente la entidad, a través de la gestión de los conocimientos administrativos, asesoría en asuntos normativos, el ejercicio de la defensa judicial y extrajudicial, para el cumplimiento de mandatos y la prevención del daño antijurídico en aras de garantizar condiciones legales aplicables.	R1	GJ01	1	Expediente de Procesos Judiciales (Información Analógica)	Información analógica	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de Expediente de Procesos Judiciales** **(Información Analógica) por: 1. Acceso no autorizado a los expedientes con Datos Personales** **1.1 Pérdida, modificación y hurto de información debido a 1. Ausencia de control de acceso a los expedientes**	Daños externos	1. Ausencia de control de acceso a los expedientes	1. Acceso no autorizado a los expedientes con Datos Personales 1.1 Pérdida, modificación y hurto de información	1	El proceso Gestión Jurídica cada que ejecuta el proceso contractual registra diariamente con su carpeta de prioridad cual sea: copia oficina de gestión, verifica cuota automáticamente registra en línea con el file encender al acceso correspondiente. En caso que el funcionario ingrese en línea con el file encender al acceso correspondiente. En caso que el funcionario administrador de plataforma / Nexus de Metro revisan la herrata y procede ser revisado y administrado de carpetas colectivas acceso registrado a través de un ticket. Tic. registro Jurídica y Administración de Carpetas Colectivas. Se evidencia que no se cuenta con un formato que permita la documentación de los mantenimientos preventivos.	1	Garantizar que el 100% de los servidores y contratistas del proceso Gestión Jurídica (Ej: y SDQ) asistan y participen de las capacitaciones y/o programadas relacionadas con el riesgo.	Moderado	Moderado	Reducir (mitigar)	Continuar con las capacitaciones en temas de seguridad de la información en la entidad y la información digital/electrónica para los servidores y contratistas del proceso Gestión Jurídica	Charlas de seguridad ejecutadas / Charlas de Seguridad programadas	6		1		Recursos Humanos, Tecnológicos	Gerente Jurídico
			R1	GJ01	2	Expediente de Procesos Judiciales (Información Analógica)	Información analógica	Pérdida de Disponibilidad	**Pérdida de Disponibilidad de Expediente de Procesos Judiciales** **(Información Analógica) por 1. Acceso no autorizado a los expedientes con Datos Personales** **1. Fallas Humanas debido a 1. Ausencia de control de acceso a los expedientes** **2.Desconocimiento de Políticas de seguridad de la información** **3. Ausencia de planes de contingencia**	Daños externos	1. Ausencia de control de acceso a los expedientes 2.Desconocimiento de Políticas de seguridad de la información 3. Ausencia de planes de contingencia	1.y 3. Pérdida o destrucción de la información (datos personales) 2. Fallas Humanas	1	El proceso Gestión Jurídica cada que ejecuta el proceso contractual registra diariamente con su carpeta de prioridad cual sea: copia oficina de gestión, verifica cuota automáticamente registra en línea con el file encender al acceso correspondiente. En caso que el funcionario ingrese en línea con el file encender al acceso correspondiente. En caso que el funcionario administrador de plataforma / Nexus de Metro revisan la herrata y procede ser revisado y administrado de carpetas colectivas acceso registrado a través de un ticket. Tic. registro Jurídica y Administración de Carpetas Colectivas. Se evidencia que no se cuenta con un formato que permita la documentación de los mantenimientos preventivos.	1	Garantizar que el 100% de los servidores y contratistas del proceso Gestión Jurídica (Ej: y SDQ) asistan y participen de las capacitaciones y/o programadas relacionadas con el riesgo.	Moderado	Bajo	Aceptar								
			R1	GJ01	3	Expediente de Procesos Judiciales (Información Digital (Contenidos)	Información digital	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de Expediente de Procesos Judiciales** **(Información Electrónica) por 1. Pérdida, borrado, modificación de información o daños no autorizados a los expedientes digitales con Datos Personales** **2. Abuso intencionado de acceso a la información digital** **3. Fallas Humanas debidos a** **1. Ausencia de control de acceso a la información digital** **2. Deficiencia en la asignación de permisos** **3.Desconocimiento de Políticas de seguridad de la información**	Tecnología	1. Ausencia de control de acceso a la información digital 2. Deficiencia en la asignación de permisos 3.Desconocimiento de Políticas de seguridad de la información	1. Pérdida, borrado, modificación de información o daños no autorizado a los expedientes digitales con Datos Personales 2. Abuso intencionado de acceso a la información digital 3. Fallas Humanas	1.y 3.	El jefe de dependencia revisa cada día hasta la copia de respaldo respectiva, verifica que se haya realizado correctamente y que no haya sido alterada. Si la copia de respaldo presenta alguna inconsistencia, informa inmediatamente a la dependencia. El jefe de dependencia revisa la matriz y en caso de no encontrar información en modificaciones permanentes, no evidencia queda registrado en el control.	1	Garantizar que el 100% de los servidores y contratistas del proceso Gestión Jurídica (Ej: y SDQ) asistan y participen de las capacitaciones y/o programadas relacionadas con el riesgo.	Alto	Moderado	Reducir (mitigar)	Continuar con las capacitaciones en temas de seguridad de la información en la entidad y la información digital/electrónica para los servidores y contratistas del proceso Gestión Jurídica	Charlas de seguridad ejecutadas / Charlas de Seguridad programadas	6		1		Recursos Humanos, Tecnológicos	Gerente Jurídico
			R1	GJ01	4	Expediente de Procesos Judiciales (Información Digital (Contenidos)	Información digital	Pérdida de Disponibilidad	**Pérdida de Disponibilidad de Expediente de Procesos Judiciales** **(Información Electrónica) por 1.y 3. Pérdida, borrado, modificación de información o daños no autorizados a los expedientes digitales con Datos Personales** **2. Fallas Humanas** **CONTINUIDAD: 3. Fallas tecnológicas debido a** **1. Ausencia de control de acceso a la información digital** **2.Desconocimiento de Políticas de Seguridad de la información** **3. Ausencia de Planes de contingencia**	Tecnología	1. Ausencia de control de acceso a la información digital 2.Desconocimiento de Políticas de seguridad de la información 3. Ausencia de Planes de contingencia	1.y 3. Pérdida, borrado, modificación de información o daños no autorizados a los expedientes digitales con Datos Personales 2. Fallas Humanas CONTINUIDAD: 3. Fallas tecnológicas	1.y 3.	El jefe de dependencia revisa cada día hasta la copia de respaldo respectiva, verifica que se haya realizado correctamente y que no haya sido alterada. Si la copia de respaldo presenta alguna inconsistencia, informa inmediatamente a la dependencia. El jefe de dependencia revisa la matriz y en caso de no encontrar información en modificaciones permanentes, no evidencia queda registrado en el control.	1	Garantizar que el 100% de los servidores y contratistas del proceso Gestión Jurídica (Ej: y SDQ) asistan y participen de las capacitaciones y/o programadas relacionadas con el riesgo.	Moderado	Moderado	Reducir (mitigar)	Continuar con las capacitaciones en temas de seguridad de la información en la entidad y la información digital/electrónica para los servidores y contratistas del proceso Gestión Jurídica	Charlas de seguridad ejecutadas / Charlas de Seguridad programadas	6		1		Recursos Humanos, Tecnológicos	Gerente Jurídico
			R1	GJ01	5	Archivo de Gestión GERENCIA JURÍDICA	Interacciones	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de Archivo de Gestión GERENCIA JURÍDICA por 1. Acceso no autorizado a los expedientes con Datos Personales** **1.1 Pérdida, modificación y hurto de información debido a 1. Ausencia de control de acceso a los expedientes**	Daños externos	1. Ausencia de control de acceso a los expedientes	1. Acceso no autorizado a los expedientes con Datos Personales 1.1 Pérdida, modificación y hurto de información	1	El proceso Gestión Jurídica cada que ejecuta el proceso contractual registra diariamente con su carpeta de prioridad cual sea: copia oficina de gestión, verifica cuota automáticamente registra en línea con el file encender al acceso correspondiente. En caso que el funcionario ingrese en línea con el file encender al acceso correspondiente. En caso que el funcionario administrador de plataforma / Nexus de Metro revisan la herrata y procede ser revisado y administrado de carpetas colectivas acceso registrado a través de un ticket. Tic. registro Jurídica y Administración de Carpetas Colectivas. Se evidencia que no se cuenta con un formato que permita la documentación de los mantenimientos preventivos.	1	Garantizar que el 100% de los servidores y contratistas del proceso Gestión Jurídica (Ej: y SDQ) asistan y participen de las capacitaciones y/o programadas relacionadas con el riesgo.	Moderado	Moderado	Reducir (mitigar)	Continuar con las capacitaciones en temas de seguridad de la información en la entidad y la información digital/electrónica para los servidores y contratistas del proceso Gestión Jurídica	Charlas de seguridad ejecutadas / Charlas de Seguridad programadas	6		1		Recursos Humanos, Tecnológicos	Gerente Jurídico
			R1	GJ01	6	Archivo de Gestión GERENCIA JURÍDICA	Interacciones	Pérdida de Disponibilidad	**Pérdida de Disponibilidad de Archivo de Gestión GERENCIA JURÍDICA por 1.y 3. Pérdida o destrucción de la información (datos personales)** **2. Fallas Humanas debido a 1. Ausencia de control de acceso a los expedientes** **2.Desconocimiento de Políticas de seguridad de la información** **3. Ausencia de planes de contingencia**	Daños externos	1. Ausencia de control de acceso a los expedientes 2.Desconocimiento de Políticas de seguridad de la información 3. Ausencia de planes de contingencia	1.y 3. Pérdida o destrucción de la información (datos personales) 2. Fallas Humanas	1.y 3.	El proceso Gestión Jurídica cada que ejecuta el proceso contractual registra diariamente con su carpeta de prioridad cual sea: copia oficina de gestión, verifica cuota automáticamente registra en línea con el file encender al acceso correspondiente. En caso que el funcionario ingrese en línea con el file encender al acceso correspondiente. En caso que el funcionario administrador de plataforma / Nexus de Metro revisan la herrata y procede ser revisado y administrado de carpetas colectivas acceso registrado a través de un ticket. Tic. registro Jurídica y Administración de Carpetas Colectivas. Se evidencia que no se cuenta con un formato que permita la documentación de los mantenimientos preventivos.	1	Garantizar que el 100% de los servidores y contratistas del proceso Gestión Jurídica (Ej: y SDQ) asistan y participen de las capacitaciones y/o programadas relacionadas con el riesgo.	Moderado	Bajo	Aceptar	No	No						
Gestión y Innovación de TI	Implementar y consolidar un modelo de gestión institucional que permita el desarrollo de las competencias y capacidades del recurso humano, la adopción de buenas prácticas, optimización y el uso de las Tecnologías de la Información para mejorar la satisfacción de los ciudadanos y grupos de interés y grupos de valor.	Gestionar adecuadamente los requerimientos de los usuarios que deben estar contenidos en el Plan Estratégico de Tecnologías de la Información (PETI), alineados con los criterios establecidos en la Planeación Estratégica TI, Arquitectura TI y apropiación en el de documentar la transformación digital de la SHD, en cumplimiento de la política gobierno y el cumplimiento de las objetivos institucionales.	R1	GD01	1	MIER_QA MIGPRO2 - Producción MIGPRO3 - Producción MIGPRO4 - Producción MIGPRO5 - Producción MIGPRO6 - Producción MIGDES - Desarrollo - pruebas BASES DE DATOS DE CATASTRO MULTIPROPÓSITO (TEMPORAL) CATASTRAL - Producción TRIAMBIAL - Producción CARTOTEN - Cartagena por 1. Abuso de derechos 1a. Perdida, Hurto o modificación de la información 3. Falsificación de derechos. 4.y 5. Fallas Humanas debidos a 1. Asignación errada de los derechos de acceso a nivel de administración de la base de datos 2. Información Sensible sin cifrado a nivel de base de datos 3. Falsificación de derechos. 4. Desconocimiento de la configuración de la base de datos 5. Desconocimiento de las políticas de seguridad de la información 6. Desconocimiento de la configuración de la base de datos 7. Desconocimiento de las políticas de seguridad de la información	Tecnología	1. Asignación errada de los derechos de acceso a nivel de administración de la base de datos 2. Información Sensible sin cifrado a nivel de base de datos 3. Falsificación de derechos. 4. Desconocimiento de la configuración de la base de datos 5. Desconocimiento de las políticas de seguridad de la información	1. Abuso de derechos 1a. Perdida, Hurto o modificación de la información 3. Falsificación de derechos. 4y 5. Fallas Humanas	1	El proceso de control sensible de la base de datos cada vez que un administrador de bases de datos actualiza/crea las cuentas/roles administrados registrados en bases de datos corporativas, con el fin de verificar los permisos / perfiles otorgados. El administrador de bases de datos cada vez que ejecuta el proceso de control sensible de la base de datos, el proceso de control sensible de la base de datos registra de manera diaria en la herramienta de control sensible de la base de datos del sistema de incidencias en mesa de ayuda. - ARSENTINA	1	Bloqueo de usuarios y/o cuentas de permisos	Alto	Moderado	Reducir (mitigar)	1. Revisar de forma permanente las funciones establecidas en el instructivo de Gestión de bases de datos, ejecutando actividades de control sobre los cambios de usuarios y/o usuarios privilegiados asignados a los administradores.	Acta actividades de activación de usuarios ejecutadas / # de solicitudes de activación de usuarios programadas	6	1	1	1	1	Recursos Humanos y Tecnológicos	Gerente de Tecnología / Subgerente de Infraestructura Tecnológica (Administradores de Bases de datos)

			R6	GDTI	R6	(Producción, Pruebas / desarrollo) Servidores Virtualizados en IaaS de Azure (Pasbuesta)	Servicios	Pérdida de confidencialidad e integridad	**Pérdida, modificación de la información** **2. Error en el acceso a la plataforma Ebiblio o Acceso de control de acceso** **2. Desconocimiento en el uso de la plataforma virtualizada en cada una de las nubes**	Tecnología	1. Desconocimiento en el uso de la plataforma virtualizada en cada una de las nubes. 2. Error en el uso de la plataforma	4	1. Desconocimiento en las herramientas administrativas de la plataforma virtualizada en cada una de las nubes. 2. Error en el uso de la plataforma	1	Soporte uso presencial del servicio	Moderado	Moderado	Reducir (mitigar)								
																			5	Transferencia de procesos administrativos/funcionales con la configuración de la plataforma virtualizada en cada una de las nubes a terceros. Los procesos administrativos/funcionales de la plataforma virtualizada en cada una de las nubes, son de manejo y mantenimiento de la plataforma virtualizada. Por lo que en caso de no poder contar con el administrador de la plataforma, este debe ser asumido al interior de la entidad. Lo anterior, con el objeto de no generar dependencia con un tercero.	2												
			R6	GDTI	R6	Servidores Virtualizados en IaaS de AZURE - DCI (Pasbuesta) (Producción, Pruebas / desarrollo) Servidores Virtualizados en IaaS de Azure (Pasbuesta)	Servicios	Pérdida de disponibilidad	**Pérdida de Disponibilidad de Servidores Virtualizados en IaaS de DCI (Producción, Pruebas / desarrollo)** **Servidores Virtualizados en IaaS de AZURE - DCI (Pasbuesta) (Producción, Pruebas / desarrollo) por 1. Alto funcionamiento del equipo y/o software Ebiblio o** **1. Indisponibilidad de los servidores en la plataformas de nube azure y DCI** **2. Falta de backup de los servidores virtuales en las plataformas de nube Azure y DCI** **3. Evitar, en el hipotesis que gestiones los servidores virtuales en cada una de las nubes**	Tecnología	1. Indisponibilidad de los servidores en la plataformas de nube azure y DCI 2. Falta de backup de los servidores virtuales en las plataformas de nube Azure y DCI 3. Evitar, en el hipotesis que gestiones los servidores virtuales en cada una de las nubes	1. Alto funcionamiento del equipo y/o software	1	Soporte uso presencial del servicio	Alto	Bajo	Aceptar								
																			2	El SGI a través de la herramienta Bitácora provee las herramientas de administración los servidores virtualizados mediante las herramientas nativas de la infraestructura tecnológica.	1												
																			3	El administrador de la plataforma virtualizada en cada una de las nubes, es quien tiene los privilegios para realizar los procesos administrativos. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	1												
																			4	Los administradores de la plataforma virtualizada en cada una de las nubes, son los encargados de realizar los procesos administrativos. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	1												
																			5	Cada uno que se presente una indisponibilidad que requiera de un registro entre un servidor virtualizado, algunos administradores de plataforma, varios personas de mesa de ayuda, son los encargados que se tenga del interno. En caso que no se cuente con el respaldo, no debe haber la intermediación para su solución y se debe de quedar a la mesa de ayuda de N.	1												
																			6	El SGI a través de la herramienta Bitácora provee las herramientas de administración los servidores virtualizados mediante las herramientas nativas de la infraestructura tecnológica.	1												
																			7	El administrador de la plataforma virtualizada en cada una de las nubes, es quien tiene los privilegios para realizar los procesos administrativos. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	1												
																			8	El administrador de la plataforma virtualizada en cada una de las nubes, es quien tiene los privilegios para realizar los procesos administrativos. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	1												
																			9	Cada uno que se presente una indisponibilidad que requiera de un registro entre un servidor virtualizado, algunos administradores de plataforma, varios personas de mesa de ayuda, son los encargados que se tenga del interno. En caso que no se cuente con el respaldo, no debe haber la intermediación para su solución y se debe de quedar a la mesa de ayuda de N.	1												
																			10	Los administradores de la plataforma configuran las políticas de backup dentro de dichas las actividad, tipo de copia, y tiempo de retención y las políticas de servidores.	1												
			R6	GDTI	R6	Infraestructura - Nube de Azure - DCI (IaaS)	Servicios	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de Infraestructura - Nube de Azure - DCI (IaaS) por 1. Pérdida, borrado, modificación o acceso no autorizado a la Información.** **2. Error en el uso Ebiblio o 1. Desconocimiento de políticas de seguridad relacionado con la gestión de contraseñas.** **2. Desconocimiento del funcionamiento de la infraestructura**	Tecnología	1. Desconocimiento de políticas de seguridad relacionado con la gestión de contraseñas 2. Desconocimiento del funcionamiento de la infraestructura	1. Pérdida, borrado, modificación o acceso no autorizado a la Información. 2. Error en el uso	1	Soporte uso presencial del servicio	Moderado	Bajo	Aceptar								
																			2	Gestión de accesos a la infraestructura de nube, de acuerdo a los roles establecidos en la categoría de infraestructura tecnológica	1												
																			3	Gestión de logs de auditoría por parte de los administradores de plataforma a nuestro soporte tecnológico proveedor	1												
																			4	Transversalidad de las configuraciones de infraestructura de nube (matrices de backup)	1												
																			5	Copias de respaldo de las configuraciones de la plataforma IaaS	1												
			R6	GDTI	R6	Infraestructura - Nube de Azure - DCI (IaaS)	Servicios	Pérdida de disponibilidad	**Pérdida de Disponibilidad de Infraestructura - Nube de Azure - DCI (IaaS) por 1. Indisponibilidad a la infraestructura tecnológica de la redundancia en Redes DCI y Azure** **2. Vulnerabilidad de la seguridad de la información en la infraestructura desplegada en las Redes de DCI y Azure** **3. Errores en la ejecución de procesos de la SAD Ebiblio o 1. Desconocimiento de políticas de seguridad de la información** **2. Desconocimiento en la ejecución de procesos de la plataforma SAD**	Tecnología	1. Desconocimiento de políticas de seguridad de la información 2. Desconocimiento en la ejecución de procesos de la plataforma SAD	1. Indisponibilidad a la infraestructura tecnológica de la redundancia en Redes DCI y Azure 2. Vulnerabilidad de la seguridad de la información en la infraestructura desplegada en las Redes de DCI y Azure 3. Errores en la ejecución de procesos de la SAD	1	Soporte uso presencial del servicio	Alto	Moderado	Reducir (mitigar)	1. Realizar la actualización del inventario de activos de información a cargo de la Subgerencia de Infraestructura	4 Activos actualizados en el inventario / 4 Activos programados	4	1	1	1	1	Recursos Humanos y Tecnológicos	Gerente de Tecnología / Subgerente de Infraestructura Tecnológica (equipo de administración de servidores)
																			2	Ejecutar de forma permanente las actividades de mantenimiento y actualización de los recursos tecnológicos bajo responsabilidad de la	4 Actividades de actualización de recursos tecnológicos ejecutadas / 4 de actividades de actualización que mantenimiento programadas	4	1	1	1	1	Recursos Humanos y Tecnológicos	Gerente de Tecnología / Subgerente de Infraestructura Tecnológica (equipo de administración de servidores)
																			3	3. Realizar seguimiento preventivos al uso de los recursos tecnológicos programados periódicos de la separación Horas requeridas	12 informes de seguimiento periódicos / 12 de informes de separación programados	12	1	1	1	1	Recursos Humanos y Tecnológicos	Gerente de Tecnología / Subgerente de Infraestructura Tecnológica (equipo de administración de servidores)
																			4	4. Realizar seguimiento preventivos al uso de los recursos tecnológicos programados periódicos de la separación Horas requeridas	12 informes de separación periódicos / 12 de informes de separación programados	12	1	1	1	1	Recursos Humanos y Tecnológicos	Gerente de Tecnología / Subgerente de Infraestructura Tecnológica (equipo de administración de servidores)
			R6	GDTI	R6	SWITCH DE CORE SWITCH Wide	Hardware	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad SWITCH DE CORE SWITCH Wide por 1. Alaques externos** **2. Error en el uso** **1. Modificación configuración de los equipos Ebiblio o 1. Configuración incorrecta de parametros** **2. Desconocimiento en el funcionamiento de la herramienta** **3. Deficiencia en la gestión de acceso**	Tecnología	1. Configuración incorrecta de parametros 2. Desconocimiento en el funcionamiento de la herramienta 3. Deficiencia en la gestión de acceso	1. Alaques externos 2. Error en el uso 3. Modificación de configuración de los equipos	1	Ex ineficaz diagnostico preliminar del problema en escaparse el incidente no pasa a ser consignado por el administrador de la plataforma, este debe ser resuelto al presentarse para su solución de acuerdo a la gavanta o contratos de mantenimiento.	Moderado	Bajo	Aceptar	NA	NA							
																			2	El proceso establecido cada uno del fortalecimiento regular establecimiento con un tercero de prioridad ubicado a un área cuyos jerarquías (archivo magistrales), verifica cada actividad que se lleva a cabo en la plataforma. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	1												
																			3	El administrador de los switches, no es el responsable de los artículos de configuración y/o hacer actualizaciones, los cuales pueden ser ejecutados por el proveedor de chancapiedra o por	1												
																			4	El administrador de los switches, solo es que no requiere, necesita el proceso de restauración de los artículos de configuración de los switches.	1												
			R6	GDTI	R6	SWITCH DE CORE SWITCH Wide	Hardware	Pérdida de disponibilidad	**Pérdida de Disponibilidad de SWITCH DE CORE SWITCH Wide por 1. Incumplimiento en el mantenimiento de las herramientas tecnológicas** **1a. Fallas en los equipos disponibles** **2. Polvo, corrosión, congelamiento** **3. Error en el uso** **4. Explosiva remoto** **5. Pérdida del suministro de energía Ebiblio o 1. Mantenimiento insuficiente/inestable/fallido de la media de almacenamiento** **1a. Ausencia de Mantenimiento al mantenimiento de equipos** **2. Susceptibilidad a la humedad, el polvo y la suciedad** **3. Desconocimiento en la configuración de las herramientas** **4. Ampliaciones inseguras de la red** **5. Susceptibilidad a las variaciones de voltaje** **6. Errores en el sistema operativo (Firmware) de las plataformas**	Tecnología	1. Mantenimiento insuficiente/inestable/fallido de la media de almacenamiento 1a. Ausencia de Mantenimiento al mantenimiento de los equipos 2. Susceptibilidad a la humedad, el polvo y la suciedad 3. Desconocimiento en la configuración de las herramientas 4. Ampliaciones inseguras de la red 5. Susceptibilidad a las variaciones de voltaje 6. Errores en el sistema operativo (Firmware) de las plataformas	1. Incumplimiento en el mantenimiento de las herramientas tecnológicas 1a. Fallas en los equipos disponibles 2. Polvo, corrosión, congelamiento 3. Error en el uso 4. Explosiva remoto 5. Pérdida del suministro de energía	1	Ex ineficaz diagnostico preliminar del problema en escaparse el incidente no pasa a ser consignado por el administrador de la plataforma, este debe ser resuelto al presentarse para su solución de acuerdo a la gavanta o contratos de mantenimiento.	Moderado	Bajo	Aceptar	NA	NA							
																			2	El modo de la herramienta SAE junto con las herramientas de administración los switch mantienen permanente los servicios de Conectividad	1a												
																			3	El administrador de la plataforma virtualizada (sistema) (Firmware) de mantenimientos/soportes con el proveedor de servicio de acuerdo como una descripción del servicio de mantenimiento, es quien debe hacer el control de los procesos administrativos y programas virtualizada. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	1												
																			4	Cuando se presenta un incidente/actividad/evento con la configuración de la plataforma a errores de la misma con una plataforma, el administrador debe ser la falla y no necesariamente del equipo. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	4.2												
			R6	GDTI	R6	Servicio de Internet - Sede Principal	Servicios	Pérdida de disponibilidad	**Pérdida de confidencialidad e Integridad de Servicio de Internet - Sede Principal por 1. Sectorización de equipo y medio** **2. Fuente de equipo** **1. Falta de cables o fibras dañadas o porqueria de contractorias o mantenimiento de la Ciudad Ebiblio o 1. Uso inadecuado o desuidado del control de acceso física a los edificaciones y los accesos** **2. Ausencia de protección física de la edificación, puertas y ventanas** **3. Conexión deficiente de los cables** **4. Punto único de falla**	Eventos externos	1. Uso inadecuado o desuidado del control de acceso física a los edificaciones y los accesos 2. Ausencia de protección física de la edificación, puertas y ventanas 3. Conexión deficiente de los cables 4. Punto único de falla	1. Sectorización de equipo y medio 2. Fuente de equipo 3. Falta de cables o fibras dañadas o porqueria de contractorias o mantenimiento de la Ciudad	1	En caso que el incidente no pasada por consignado por el administrador de red, este debe ser resuelto al presentarse para su solución	Moderado	Bajo	Aceptar	NA	NA							
																			2	Monitoreo por parte de los administradores de Internet de la disponibilidad de los canales de internet	1.4												
																			3	Monitoreo por parte de los administradores de Internet de la disponibilidad de los canales de internet	1.4												
																			4	El proceso establecido cada uno del fortalecimiento regular establecimiento con un tercero de prioridad ubicado a un área cuyos jerarquías (archivo magistrales), verifica cada actividad que se lleva a cabo en la plataforma. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	4.2												
																			5	Cuando se presenta un incidente/actividad/evento con la configuración de la plataforma a errores de la misma con una plataforma, el administrador debe ser la falla y no necesariamente del equipo. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	4.2												
			R6	GDTI	R6	Servicio de Internet - Sede Principal	Servicios	Pérdida de disponibilidad	**Pérdida de Disponibilidad de Servicio de Internet - Sede Principal por 1. Sectorización de equipo y medio** **2. Fuente de equipo** **Falta de cables o fibras dañadas o porqueria de contractorias o mantenimiento de la Ciudad Ebiblio o 1. Uso inadecuado o desuidado del control de acceso física a los edificaciones y los accesos** **2. Ausencia de protección física de la edificación, puertas y ventanas** **3. Conexión deficiente de los cables** **4. Punto único de falla**	Eventos externos	1. Uso inadecuado o desuidado del control de acceso física a los edificaciones y los accesos 2. Ausencia de protección física de la edificación, puertas y ventanas 3. Conexión deficiente de los cables 4. Punto único de falla	1. Sectorización de equipo y medio 2. Fuente de equipo Falta de cables o fibras dañadas o porqueria de contractorias o mantenimiento de la Ciudad	1	En caso que el incidente no pasada por consignado por el administrador de red, este debe ser resuelto al presentarse para su solución	Moderado	Bajo	Aceptar	NA	NA							
																			2	Monitoreo por parte de los administradores de Internet de la disponibilidad de los canales de internet	1.4												
																			3	Monitoreo por parte de los administradores de Internet de la disponibilidad de los canales de internet	1.4												
																			4	El proceso establecido cada uno del fortalecimiento regular establecimiento con un tercero de prioridad ubicado a un área cuyos jerarquías (archivo magistrales), verifica cada actividad que se lleva a cabo en la plataforma. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	4.2												
																			5	Cuando se presenta un incidente/actividad/evento con la configuración de la plataforma a errores de la misma con una plataforma, el administrador debe ser la falla y no necesariamente del equipo. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	4.2.3.4												
			R6	GDTI	R6	Administradores de Seguridad Informática Administradores de Bases de Datos	Recurso Humano	Pérdida de Confidencialidad	**Pérdida de Confidencialidad de Administradores de Seguridad Informática Administradores de Bases de Datos por Ataques de Ingeniería social Ebiblio o Desconocimiento de políticas de seguridad de la información**	Talento humano	Desconocimiento de políticas de seguridad de la información	Ataques de ingeniería social	1	Contar mínimo dos personas que conocen una misma actividad	Moderado	Bajo	Aceptar	NA	NA							
																			2	El dificultar seguridad de la información cruzar los roles programadas de servidor/bases de seguridad/roles informacion, con el fin de evitar los dependencias en procesos/ procesos programados. Verificar las personas que ejecutaron y las que no ejecutaron y las correspondientes a los procesos programados. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	1												
																			3	El Ataque Intencionado de Ingeniería Social no se puede evitar en forma total, pero se puede minimizar el riesgo de ocurrencia y el impacto que pueda ocasionar a la entidad. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	1												
			R6	GDTI	R6	Administradores de Seguridad Informática Administradores de Bases de Datos	Recurso Humano	Pérdida de disponibilidad	**Pérdida de Disponibilidad de Administradores de Seguridad Informática Administradores de Bases de Datos por 1. Incumplimiento en la disponibilidad del personal** **2. Abuso de derechos Ebiblio o 1. Ausencia del personal** **2. Desconocimiento de políticas de seguridad de la información**	Talento humano	1. Ausencia del personal 2. Desconocimiento de políticas de seguridad de la información	1. Incumplimiento en la disponibilidad del personal 2. Abuso de derechos	1	Contar mínimo dos personas que conocen una misma actividad	Moderado	Bajo	Aceptar	NA	NA							
																			2	El dificultar seguridad de la información cruzar los roles programadas de servidor/bases de seguridad/roles informacion, con el fin de evitar los dependencias en procesos/ procesos programados. Verificar las personas que ejecutaron y las que no ejecutaron y las correspondientes a los procesos programados. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	1												
																			3	La persona designada para el jefe de dependencia cada vez que se retira un funcionario o contratista, es quien debe informar a la mesa de ayuda, para que se inactive el usuario y el registro inactivo/ya que manejaba ayuda a gestionar a un funcionario correspondiente y/o una persona nos evidencia. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	1												
																			4	El dificultar seguridad de la información cruzar los roles programadas de servidor/bases de seguridad/roles informacion, con el fin de evitar los dependencias en procesos/ procesos programados. Verificar las personas que ejecutaron y las que no ejecutaron y las correspondientes a los procesos programados. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos. Es caso de que no se encuentre disponible, y se encuentre en mantenimiento, es quien debe hacer el control de los procesos administrativos.	1												
																			5	Sistema de personal no respaldo para el desarrollo de las actividades	1												
Evaluación de riesgos de seguridad	mejoramiento y consultas en medio de gestión documental que permita el desarrollo de las actividades y características de la capital Humana la adopción de procesos / procedimientos / uso de las tecnologías de la información que requiere la participación de las necesidades y expectativas de las partes de valor	Mejorar y proteger el valor de la unidad proporcionando información objetiva, oportuna y analítica basada en hechos y datos por la evaluación independiente del Sistema de Control Interno y la información generada permanente a la gestión, garantiza el cumplimiento de los objetivos institucionales y la toma de decisiones en la actuación de los recursos asignados.	R6	GIGD	1	Auditorías Internas (Información Electrónica)	Información digital	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de Auditorías Internas (Información Electrónica) por 1. Pérdida, borrado, modificación de información o Acceso no autorizado a los expedientes digitales con Datos Personales** **2. Abuso Intencionado de acceso a la información digital** **2. Falta Humanas Ebiblio o** **1,2,3 Ausencia de control de acceso a información digital** **2. Deficiencia en la asignación de permisos.** **3. Desconocimiento de Políticas de seguridad de la información**	Tecnología	1,2,3 Ausencia de control de acceso a la información digital 2. Deficiencia en la asignación de permisos 3. Desconocimiento de Políticas de seguridad de la información	1. Pérdida, borrado, modificación de información o Acceso no autorizado a los expedientes digitales con Datos Personales 2. Abuso Intencionado de acceso a la información digital 2. Falta Humanas	1	Implementar de manera correctiva las ajustes realizados	Moderado	Moderado	Reducir (mitigar)	Revisiones semestral por parte de la jefe de oficina a la matrícula permisos de los expositores de información de la Oficina de Control Interno en la rutas, revisiones que el Control Interno en la rutas, revisiones que el Control Interno en la rutas, revisiones semestrales y/o cada vez que se presenten actualizaciones y/verificaciones y/o necesidades y/ otros ideas las	Revisiones realizadas /revisiones programadas	2		1		1	Recurso humano	jefe de la oficina
																			2	El proceso interno establecido cada uno que requiere de un tercero de seguridad debe reportar la ocurrencia de un evento de seguridad a la mesa de ayuda y/o verificar el interno a la entidad para que pueda ejecutar la Mesa de Servicios de T	Charlas ejecutadas/ Charlas Programadas	1				1	Recurso humano	jefe de la oficina
																			3	Verificar mensualmente la actualización de la información GD en los expositores	Ejecuciones realizadas / revisiones programadas	12	1	1	1	1	Recurso humano	jefe de la oficina
			R6	GIGD	2	Auditorías Internas (Información Electrónica)	Información digital	Pérdida de disponibilidad	**Pérdida de Disponibilidad de Auditorías Internas (Información Electrónica) por 1. 1,2. Pérdida, borrado, modificación de información o Acceso no autorizado a los expedientes digitales con Datos Personales** **2. Falta Humanas** **Contingencia 1. Fallas tecnológicas Ebiblio o 1. Ausencia de control de acceso a la información digital** **2. Desconocimiento de Políticas de Seguridad de la información** **3. Ausencia de Planes de continuidad**	Tecnología	1. Ausencia de control de acceso a la información digital 2. Desconocimiento de Políticas de Seguridad de la información 3. Ausencia de Planes de continuidad	1,2. Pérdida, borrado, modificación de información o Acceso no autorizado a los expedientes digitales con Datos Personales 2. Falta Humanas Contingencia 1. Fallas tecnológicas	1	Implementar de manera correctiva las ajustes realizados	Moderado	Moderado	Reducir (mitigar)	Revisiones semestral por parte de la jefe de oficina a la matrícula permisos de los expositores de información de la Oficina de Control Interno en la rutas, revisiones que el Control Interno en la rutas, revisiones semestrales y/o cada vez que se presenten actualizaciones y/verificaciones y/o necesidades y/ otros ideas las	Revisiones realizadas /revisiones programadas	2		1		1	Recurso humano	jefe de la oficina
																			2	El proceso interno establecido cada uno que requiere de un tercero de seguridad debe reportar la ocurrencia de un evento de seguridad a la mesa de ayuda y/o verificar el interno a la entidad para que pueda ejecutar la Mesa de Servicios de T	Charlas ejecutadas/ Charlas Programadas	1				1	Recurso humano	jefe de la oficina
																			3	Verificar mensualmente la actualización de la información GD en los expositores	Ejecuciones realizadas / revisiones programadas	12	1	1	1	1	Recurso humano	jefe de la oficina
			R6	GIGD	3	Auditorías Internas (Información Electrónica)	Información digital	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de Auditorías Internas (Información Electrónica) por 1. Pérdida, borrado, modificación de información o Acceso no autorizado a los expedientes digitales con Datos Personales** **2. Abuso Intencionado de acceso a la información digital** **3. Falta Humanas Ebiblio o** **1,2,3 Ausencia de control de acceso a información digital**	Tecnología	1,2,3 Ausencia de control de acceso a la información digital 3. Deficiencia en la asignación de permisos 3. Desconocimiento de	1. Pérdida, borrado, modificación de información o Acceso no autorizado a los expedientes digitales con Datos Personales 2. Abuso Intencionado de acceso a la información digital	1	Implementar de manera correctiva las ajustes realizados	Moderado	Moderado	Reducir (mitigar)	Revisiones semestral por parte de la jefe de oficina a la matrícula permisos de los expositores de información de la Oficina de Control Interno en la rutas, revisiones que el Control Interno en la rutas, revisiones semestrales y/o cada vez que se presenten actualizaciones y/verificaciones y/o necesidades y/ otros ideas las	Revisiones realizadas /revisiones programadas	2		1		1	Recurso humano	jefe de la oficina
																			2	El proceso interno establecido cada uno que requiere de un tercero de seguridad debe reportar la ocurrencia de un evento de seguridad a la mesa de ayuda y/o verificar el interno a la entidad para que pueda ejecutar la Mesa de Servicios de T	Charlas ejecutadas/ Charlas Programadas	1				1	Recurso humano	jefe de la oficina
																			3	Verificar mensualmente la actualización de la información GD en los expositores	Ejecuciones realizadas / revisiones programadas	12	1	1	1	1	Recurso humano	jefe de la oficina

			R6	GGD	8	Auditorías Internas (Información Electrónica)	Información digital	Pérdida de Disponibilidad	Tecnología	1. Ausencia de control de acceso a la información digital 2. Desconocimiento de Políticas de Seguridad de la información 3. Ausencia de Planes de continuidad	1 y 3. Pérdida, borrado, modificación de información digital y/o expedientes digitales con fines Personales 2. Fallas Humanas Continuidad: 3. Fallas tecnológicas	1. Ausencia de control de acceso a la información digital 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de Planes de continuidad	1. Pérdida de información digital 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso a la información digital 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de Planes de continuidad	1. Pérdida de información digital 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso a la información digital 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de Planes de continuidad	1. Pérdida de información digital 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso a la información digital 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de Planes de continuidad	1. Pérdida de información digital 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	75	Implementar medidas de control adicionales.	Moderado	Moderado	Reducir (mitigar)	Verificar mensualmente la actualización de la información GD en los repositorios	Revisiones realizadas / revisiones programadas	12	3	3	3	3	Recurso humano	Jefe de la oficina
			R6	GGD	5	Redes de la GD (Servicio)	Servicios	Pérdida de confidencialidad e integridad	Tecnología	Ausencia de control de acceso	Uso no autorizado de la información Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	75	Identificar y documentar ausencias los roseores específicos para la GD, en caso de estar en ausencia y implementar de manera inmediata los ajustes necesarios.	Alto	Moderado	Reducir (mitigar)	Solicitar sensibilizaciones de seguridad de la información para el personal (funcionarios y colaboradores) de la oficina, en temas de responsabilidad y seguridad	Sensibilizaciones realizadas / Total servidores GD	1		1		Recurso humano	Jefe de la oficina
			R6	GGD	6	Redes de la GD (Servicio)	Servicios	Pérdida de confidencialidad e integridad	Tecnología	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo Desconocimiento de políticas de seguridad de la información Ausencia de mantenimiento al Firewarr - nube Ausencia de control de acceso	Pérdida o acceso no autorizado a la información Fallas Humanas Incumplimiento en el mantenimiento del Firewarr - nube	1. Ausencia de copias de respaldo 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de mantenimiento al Firewarr - nube 4. Ausencia de control de acceso	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo 4. Ausencia de mantenimiento al Firewarr - nube	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo 4. Ausencia de mantenimiento al Firewarr - nube	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	75 75 75 75	Identificar y documentar ausencias los roseores específicos para la GD, en caso de estar en ausencia y implementar de manera inmediata los ajustes necesarios.	Alto	Moderado	Reducir (mitigar)	Realizar comentarios de seguridad de la información para el personal (funcionarios y colaboradores) de la oficina, en temas de responsabilidad y seguridad Seguimiento mensual por parte del jefe de la oficina, en el tema de gestionar la disponibilidad de la información en los repositorios disponibles.	Revisiones realizadas / revisiones programadas Sensibilizaciones realizadas / Total servidores GD Revisiones realizadas / revisiones programadas	2 1 12	1 1 3	1 1 3	1 1 3	1 1 3	Recurso humano Recurso humano Recurso humano	Jefe de la oficina Jefe de la oficina Jefe de la oficina
Gestión disciplinaria	Implementar y consolidar un modelo de gestión disciplinaria que permita el desarrollo de las competencias y conocimientos a los servidores públicos en capital humano, la adopción de procesos y procedimientos, el uso de las tecnologías de la información, que requiere la articulación de las necesidades y expectativas de los grupos de valor	Desarrollar la gestión disciplinaria cumpliendo los principios, términos, competencias y legajos del debido proceso, con el propósito de prevenir conductas disciplinables, fortalecer la cultura de la prevención que permitan mitigar la ocurrencia de faltas disciplinarias. Sustentar la integralidad de la función pública	R6	GDD	1	1. Actas de reparto 2. Procesos disciplinarios primera instancia (notificación) 3. Actas de reparto (expediente) (Información Electrónica)	Información digital	Pérdida de confidencialidad e integridad	Tecnología	1. Deficiencia en la asignación de permisos de la información 2. Ausencia interoperabilidad con parte de personal con autoridad 3. Ausencia de control de acceso 4. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	75 75 75 75 75 75 75 75 75 75 75 75	1. Revisar y actualización de los roseores de usuarios activos 2. Realizar revisión de los repositorios para encontrar la causa raíz y ajustar controles.	Alto	Alto	Reducir (mitigar)	Revisión comentarios del reporte de roseores de usuario Solicitar sensibilizaciones de seguridad de la información para el personal (funcionarios y colaboradores) de la GDD, en temas de responsabilidad en seguridad	Revisiones realizadas / revisiones programadas Charlas Realizadas / Charlas Generadas	2 1		1 1		1 1	Recurso humano Recurso humano	Jefe de Dependencia de la Oficina de Control Disciplinario Interno Jefe de Dependencia de la Oficina de Control Disciplinario Interno
			R6	GDD	2	1. Actas de reparto 2. Procesos disciplinarios primera instancia (notificación) 3. Actas de reparto (expediente) (Información Electrónica)	Información digital	Pérdida de Disponibilidad	Tecnología	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo	1. Pérdida, modificación, borrado o uso o autenticidad de la información. 2. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	75 75 75 75 75 75 75 75 75 75 75 75	1. Revisar y actualización de los roseores de usuarios activos 2. Realizar revisión de los repositorios para encontrar la causa raíz y ajustar controles.	Alto	Bajo	Aceptar	Revisión comentarios del reporte de roseores de usuario Solicitar sensibilizaciones de seguridad de la información para el personal (funcionarios y colaboradores) de la GDD, en temas de responsabilidad en seguridad	Revisiones realizadas / revisiones programadas Charlas Realizadas / Charlas Generadas	2 1		1 1		1 1	Recurso humano y tecnológico Recurso humano y tecnológico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno Jefe de Dependencia de la Oficina de Control Disciplinario Interno
			R6	GDD	3	1. Base de datos de los procesos disciplinarios 2. Bases de datos con información relacionada con los procesos disciplinarios 3. Base de datos cuadro de términos de los procesos disciplinarios	Bases de datos	Pérdida de confidencialidad e integridad	Tecnología	1. Deficiencia en la asignación de permisos de la información 2. Ausencia interoperabilidad con parte de personal con autoridad 3. Ausencia de control de acceso 4. Desconocimiento de políticas de seguridad	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	75 75 75 75 75 75 75 75 75 75 75 75	Realizar revisión de los repositorios para encontrar la causa raíz y ajustar controles.	Alto	Alto	Reducir (mitigar)	Revisión comentarios del reporte de roseores de usuario Solicitar sensibilizaciones de seguridad de la información para el personal (funcionarios y colaboradores) de la GDD, en temas de responsabilidad en seguridad	Revisiones realizadas / revisiones programadas Charlas Realizadas / Charlas Generadas	2 1		1 1		1 1	Recurso humano y tecnológico Recurso humano y tecnológico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno Jefe de Dependencia de la Oficina de Control Disciplinario Interno
			R6	GDD	4	1. Base de datos de los procesos disciplinarios 2. Bases de datos con información relacionada con los procesos Disciplinarios 3. Base de datos cuadro de términos de los procesos disciplinarios	Bases de datos	Pérdida de Disponibilidad	Tecnología	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo	1. Pérdida, modificación, borrado o uso o autenticidad de la información. 2. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información 3. Ausencia de copias de respaldo	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	75 75 75 75 75 75 75 75 75 75 75 75	Realizar revisión de los repositorios para encontrar la causa raíz y ajustar controles.	Alto	Moderado	Reducir (mitigar)	Revisión comentarios del reporte de roseores de usuario Seguimiento mensual por parte del jefe de la dependencia, en el Eje de gestionar la información en los repositorios disponibles.	Revisiones realizadas / revisiones programadas Revisiones realizadas / revisiones programadas	2 12	1 3	1 3	1 3	1 3	Recurso humano y tecnológico Recurso humano y tecnológico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno Jefe de Dependencia de la Oficina de Control Disciplinario Interno
			R6	GDD	5	Archivos de gestión de la GDD	Instalaciones	Pérdida de confidencialidad e integridad	Infraestructura	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida, modificación, borrado o uso o autenticidad de la información. 2. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	75 75 75 75 75 75 75 75 75 75 75 75	Identificar y documentar ausencias los roseores específicos para la GD, en caso de estar en ausencia y implementar de manera inmediata los ajustes necesarios.	Alto	Alto	Reducir (mitigar)	Verificar, cuando se requiera, en conexión de la Dependencia como responsable de la información en el Sistema, con el fin de contestar al usuario al interno. Solicitar sensibilizaciones de seguridad de la información para el personal contratista (prestadores) de la GDD, en temas de responsabilidad en seguridad	1 Gestor designado Charlas Realizadas / Charlas Generadas	1 1	1 1				Recurso humano y tecnológico Recurso humano y tecnológico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno Jefe de Dependencia de la Oficina de Control Disciplinario Interno
			R6	GDD	6	Archivos de gestión de la GDD	Instalaciones	Pérdida de Disponibilidad	Infraestructura	1. Desconocimiento de políticas de seguridad de la información 2. Uso inadecuado o descuidado del control de acceso físico a las edificaciones y a los recintos 3. Ubicación en un área susceptible de inundación	1. Fallas Humanas 2. Destrucción de documentos 3. Inundación	1. Desconocimiento de políticas de seguridad de la información 2. Uso inadecuado o descuidado del control de acceso físico a las edificaciones y a los recintos 3. Ubicación en un área susceptible de inundación	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Desconocimiento de políticas de seguridad de la información 2. Uso inadecuado o descuidado del control de acceso físico a las edificaciones y a los recintos 3. Ubicación en un área susceptible de inundación	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Desconocimiento de políticas de seguridad de la información 2. Uso inadecuado o descuidado del control de acceso físico a las edificaciones y a los recintos 3. Ubicación en un área susceptible de inundación	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	75 75 75 75 75 75 75 75 75 75 75 75	Identificar y documentar ausencias los roseores específicos para la GD, en caso de estar en ausencia y implementar de manera inmediata los ajustes necesarios.	Bajo	Bajo	Aceptar	Verificar, cuando se requiera, en conexión de la Dependencia como responsable de la información en el Sistema, con el fin de contestar al usuario al interno. Solicitar sensibilizaciones de seguridad de la información para el personal contratista (prestadores) de la GDD, en temas de responsabilidad en seguridad	1 Gestor designado Charlas Realizadas / Charlas Generadas	1 1	1 1				Recurso humano y tecnológico Recurso humano y tecnológico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno Jefe de Dependencia de la Oficina de Control Disciplinario Interno
			R6	GDD	7	1. Sistema de graduación 2. Correo electrónico y redes sociales 3.Sistema de Información Disciplinario Distrital	Servicios	Pérdida de confidencialidad e integridad	Tecnología	1. Ausencia de control de acceso 2. Desconocimiento de políticas de control de acceso	1. Pérdida o acceso no autorizado 2. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de control de acceso	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de control de acceso	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de control de acceso	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de control de acceso	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	75 75 75 75 75 75 75 75 75 75 75 75	Determinar cuales tienen los autoridades requeridos y documentarlos de manera inmediata.	Alto	Moderado	Reducir (mitigar)	Cuando se requiera, designar al servidor de la Dependencia como responsable de la información en el Sistema, de actualizaciones en el Sistema con el fin de contestar al usuario al interno de manera oportuna de mensajes y peticiones de ciudadanos. Solicitar sensibilizaciones de seguridad de la información para el personal contratista (prestadores) de la GDD, en temas de responsabilidad en seguridad	1 Gestor designado para cada tema Charlas Realizadas / Charlas Generadas	1 1	1 1				Recurso humano y tecnológico Recurso humano y tecnológico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno Jefe de Dependencia de la Oficina de Control Disciplinario Interno
			R6	GDD	8	1. Sistema de graduación 2. Correo electrónico y redes sociales 3.Sistema de Información Disciplinario Distrital	Servicios	Pérdida de Disponibilidad	Tecnología	1. Desconocimiento en el uso de los dispositivos 2. Mantenimiento inadecuado o ausencia de fuentes de los dispositivos móviles. 3. Ausencia de copias de respaldo (gmail/correo) 4. Desconocimiento de políticas de seguridad	1. Incumplimiento en el mantenimiento de los dispositivos 2. Pérdida o acceso no autorizado a las grabaciones y/o correos electrónicos 3. Fallas Humanas 4. Fallas de los dispositivos	1. Desconocimiento en el uso de los dispositivos 2. Mantenimiento inadecuado o ausencia de fuentes de los dispositivos móviles. 3. Ausencia de copias de respaldo (gmail/correo) 4. Desconocimiento de políticas de seguridad	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Desconocimiento en el uso de los dispositivos 2. Mantenimiento inadecuado o ausencia de fuentes de los dispositivos móviles. 3. Ausencia de copias de respaldo (gmail/correo) 4. Desconocimiento de políticas de seguridad	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Desconocimiento en el uso de los dispositivos 2. Mantenimiento inadecuado o ausencia de fuentes de los dispositivos móviles. 3. Ausencia de copias de respaldo (gmail/correo) 4. Desconocimiento de políticas de seguridad	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	75 75 75 75 75 75 75 75 75 75 75 75	Determinar cuales tienen los autoridades requeridos y documentarlos de manera inmediata.	Alto	Moderado	Reducir (mitigar)	Cuando se requiera, designar al servidor de la Dependencia como responsable de la información en el Sistema, de actualizaciones en el Sistema con el fin de contestar al usuario al interno de manera oportuna de mensajes y peticiones de ciudadanos. Solicitar sensibilizaciones de seguridad de la información para el personal contratista (prestadores) de la GDD, en temas de responsabilidad en seguridad	1 Gestor designado para cada tema Charlas Realizadas / Charlas Generadas	1 1	1 1				Recurso humano y tecnológico Recurso humano y tecnológico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno Jefe de Dependencia de la Oficina de Control Disciplinario Interno
			R6	GDD	9	Filezarver de GGDD Filezarver disciplinario_seguimientos	Servicios	Pérdida de confidencialidad e integridad	Tecnología	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Uso no autorizado de la información 2. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	1. Ausencia de control de acceso 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información 3. Fallas Humanas	75 75 75 75 75 75 75 75 75 75 75 75	Identificar y documentar ausencias los roseores específicos para la GD, en caso de estar en ausencia y implementar de manera inmediata los ajustes necesarios.	Alto	Moderado	Reducir (mitigar)	Revisiones comentarios del reporte de roseores de usuario Solicitar sensibilizaciones de seguridad de la información para el personal (funcionarios y colaboradores) de la GDD, en temas de responsabilidad en seguridad	Revisiones realizadas / revisiones programadas Charlas Realizadas / Charlas Generadas	2 1	1 1	1 1		1 1	Recurso humano y tecnológico Recurso humano y tecnológico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno Jefe de Dependencia de la Oficina de Control Disciplinario Interno
			R6	GDD	10	Filezarver de GGDD	Servicios	Pérdida de Disponibilidad	Tecnología	1. Ausencia de copias de respaldo 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida o acceso no autorizado a la información	1. Ausencia de copias de respaldo 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información	1. Ausencia de copias de respaldo 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información	1. Ausencia de copias de respaldo 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información	1. Ausencia de copias de respaldo 2. Desconocimiento de políticas de seguridad de la información	1. Pérdida de información 2. Pérdida, Corrupción, modificación no autorizada de la información	75 75 75 75 75 75 75 75 75 75 75 75	Identificar y documentar ausencias los roseores específicos para la GD, en caso de estar en ausencia y implementar de manera inmediata los ajustes necesarios.	Alto	Moderado	Reducir (mitigar)	Revisiones comentarios del reporte de roseores de usuario Solicitar sensibilizaciones de seguridad de la información para el personal (funcionarios y colaboradores) de la GDD, en temas de responsabilidad en seguridad	Revisiones realizadas / revisiones programadas Charlas Realizadas / Charlas Generadas	2 1	1 1	1 1		1 1	Recurso humano y tecnológico Recurso humano y tecnológico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno Jefe de Dependencia de la Oficina de Control Disciplinario Interno

			R6	GDIS	I6	Fileserver disciplinario_juegoserio	Servidores	Disponibilidad	**1. Inoperatividad en el mantenimiento del fileserver - nube dédicta 1. Ausencia de copias de respaldo** **2. Desconocimiento de políticas de seguridad de la información** **3. Ausencia de mantenimiento al fileserver - nube** **4. Ausencia de control de acceso**	Tecnología	1. Ausencia de mantenimiento al fileserver - nube 2. Ausencia de control de acceso	2. Fallas Humanas 1. Inoperatividad en el mantenimiento del fileserver - nube	5	Realizar seguridad de la información en las fechas programadas de actualizaciones de seguridad de la información, con el fin de que las dependencias asistan al proceso programado. Verificar las personas que asistieron y las que no asistieron a las capacitaciones y actividades. Establecer políticas que no permitan realizar cambios en el sitio de cada dependencia ya que se programan y los funcionarios y contratistas. Dar llamas programa y los funcionarios y contratistas a los siguientes establecimiento a actividades de capacitación. Dar mensajes recordatorios a las dependencias sobre el control que deben ejercer en el sitio de cada dependencia y los funcionarios contratistas responsables.	15	Falta en el control a los usuarios que deben ejecutar inmediatas las ajustes necesarios.	Alto	Moderado	Reducir (mitigar)	Seguimiento mensual por parte del jefe de la oficina, con el fin de garantizar la disponibilidad de la información en los espacios temas disponeles.	Revisiones realizadas / revisiones programadas	12	1	1	1	1	Recurso humano y tecnologico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno
																		6	Seguimiento mensual por parte del jefe de la oficina, con el fin de garantizar la disponibilidad de la información en los espacios temas disponeles.	24,16,20											
			R5	GDIS	I5	Equipos de computo	Hardware	Pérdidas de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de Equipos de computo por 1. Error en clave** **2. Fuete de equipo** **3. Uso no autorizado del equipo dédicto 1. Ausencia de un ativiante control de cambios en la configuración** **2. Almacenamiento sin protección** **3. Copia no controlada** **4. Desconocimiento de políticas de seguridad de la información**	Tecnología	1. Ausencia de un ativiante control de cambios en la configuración 2. Almacenamiento sin protección 3. Copia no controlada 4. Desconocimiento de políticas de seguridad de la información	1. Error en el uso 2. Fuete de equipo 3. Uso no autorizado del equipo	5	El jefe de dependencia verificara mensualmente los agendamientos de personas dentro, asegurar que ninguna de las personas de la dédicto, con el propósito de hedger el borrado de información y/o alteración de la información de los equipos de computo. Realizar seguimiento a los equipos por parte del jefe de dependencia, revisando los permisos, de un manera aleatoria, el grado de acceso, con modificaciones de los permisos. Los cambios a pasada registrada en el sitio de seguimiento a los equipos de computo. Realizar seguimiento a los equipos de computo.	24,16,20	Implementar de nuevos inmediatas los ajustes necesarios.	Moderado	Bajo	Aceptar	No	No							
																		6	Realizar seguridad de la información en las fechas programadas. Asegurar que ninguna de las personas ajenas a la dédicto, con el fin de que las dependencias asistan al proceso programado. Verificar las personas que asistieron y las que no asistieron a las capacitaciones y actividades. Establecer políticas que no permitan realizar cambios en el sitio de cada dependencia ya que se programan y los funcionarios y contratistas. Dar llamas programa y los funcionarios y contratistas a los siguientes establecimiento a actividades de capacitación. Dar mensajes recordatorios a las dependencias sobre el control que deben ejercer en el sitio de cada dependencia y los funcionarios contratistas responsables.	15											
			R6	GDIS	I2	Equipos de computo	Hardware	Pérdida de Disponibilidad	**Pérdida de disponibilidad de Equipos de computo por 1. Inoperatividad en el mantenimiento del hardware** **Fuete de equipo**	Tecnología	Inoperatividad en el mantenimiento del hardware Falla de los medios de almacenamiento	Inoperatividad en el mantenimiento del hardware Fuete de equipo	4	El jefe de la Dependencia , cada uno que lo requiera , solicita permiso de servicio TI al mantenimiento de los equipo dentro DDI.	24,16,20	Implementar de nuevos inmediatas los ajustes necesarios	Moderado	Moderado	Reducir (mitigar)	Solicitud permiso en requisito, al mantenimiento a cambio de los equipo de la DDI.	Mesa de servicios gerencia	1				1	Recurso humano y tecnologico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno
			R6	GDIS	I3	Dro Drive - SHARE Point	Servidores	Pérdida de confidencialidad e integridad	**Pérdida de confidencialidad e integridad de Dro Drive - SHARE Point por 1. Suelte clave de información** **2. Fuiteo de clave** **3. Inexistencia de copias de seguridad** **4. Robo de medios o documentos 1. Ausencia de control de acceso** **2. Desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información**	Tecnología	1. Ausencia de control de acceso 2. Desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información	1. Deficiencias por daños por agua o fuego 2. Fenómenos sísmicos 3. Robo de medios o documentos de los datos personales 4. Robo de medios o documentos	5	El administrador de la plataforma de herramientas colaborativas cuando se requiera realizar configuración de las herramientas, verificar asegurar la confidencialidad de la integridad de la información de los datos de la dédicto, con el propósito de no tener inconvenientes de la información en caso que se presente una calidad.	16,20	Restauración de la información de acuerdo con lo decuelto en el acuerdo firmado con el presidente con la Unidad	Alto	Moderado	Reducir (mitigar)	Revisiones semestral de la matriz de permisos de los repositorios de la DDI por parte del(a) jefe de Dependencia, con el fin de que garantice que el instrumento de la matriz se encuentre actualizado y/o ajustado conforme los requerimientos.	Revisiones realizadas /revisiones programadas	2		1		1	Recurso humano y tecnologico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno
																		6	El administrador de la plataforma de herramientas colaborativas cuando se requiera realizar configuración de las herramientas, verificar asegurar la confidencialidad de la integridad de la información de los datos de la dédicto, con el propósito de no tener inconvenientes de la información en caso que se presente una calidad.	16							Solicitar concientizaciones de seguridad de la información para el personal de la dédicto, en temas de responsabilidad en seguridad	Charlas Realizadas / Charlas Programadas	4		1			Recurso humano y tecnologico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno
																		5	El administrador de la plataforma de herramientas colaborativas cuando se requiera realizar configuración de las herramientas, verificar asegurar la confidencialidad de la integridad de la información de los datos de la dédicto, con el propósito de no tener inconvenientes de la información en caso que se presente una calidad.	16											
																		6	El proveedor de servicio de nube realiza el respaldo de las herramientas colaborativas de Drive Share Point a nuestros Firewalls en la dédicto	15											
																		5	El proveedor de servicio de nube realiza el respaldo de las herramientas colaborativas de Drive Share Point a nuestros Firewalls en la dédicto	15											
			R6	GDIS	I4	Dro Drive - SHARE Point	Servidores	Pérdidas de disponibilidad	**Pérdida de Disponibilidad de Dro Drive - SHARE Point por 1. Suelte clave de información 2. Fuiteo de clave** **Fuiteo de clave** **3. Corrupción de los datos dédicto 1. Desconocimiento de las políticas de seguridad de la información** **2. Ausencia de control de acceso** **3. Asignación errónea de los derechos de acceso**	Tecnología	1. Desconocimiento de las políticas de seguridad de la información 2. Ausencia de copias de respaldo 3. Asignación errónea de los derechos de acceso	1. Pérdida y fuete de información 2. Fuiteo de clave 3. Corrupción de los datos	6	El proveedor de servicio de nube realiza el respaldo de las herramientas colaborativas de Drive Share Point a nuestros Firewalls en la dédicto	15	Restauración de la información de acuerdo con lo decuelto en el acuerdo firmado con el presidente con la Unidad	Alto	Moderado	Reducir (mitigar)	Revisiones semestral de la matriz de permisos de los repositorios de la DDI por parte del(a) jefe de oficina, este con el fin de garantizar que el instrumento de la matriz se encuentre actualizado y/o ajustado conforme los requerimientos.	Revisiones realizadas /revisiones programadas	2		1		1	Recurso humano y tecnologico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno
																		5	El administrador de la plataforma de herramientas cuando se requiera realizar configuración de las herramientas, verificar asegurar la confidencialidad de la integridad de la información de los datos de la dédicto, con el propósito de no tener inconvenientes de la información en caso que se presente una calidad.	15							Solicitar concientizaciones de seguridad de la información para el personal de la dédicto, en temas de responsabilidad en seguridad	Charlas Realizadas / Charlas Programadas	4		1			Recurso humano y tecnologico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno
																		6	Realizar seguridad de la información en las fechas programadas de actualizaciones de seguridad de la información, con el fin de que las dependencias asistan al proceso programado. Verificar las personas que asistieron y las que no asistieron a las capacitaciones y actividades. Establecer políticas que no permitan realizar cambios en el sitio de cada dependencia ya que se programan y los funcionarios y contratistas. Dar llamas programa y los funcionarios y contratistas a los siguientes establecimiento a actividades de capacitación. Dar mensajes recordatorios a las dependencias sobre el control que deben ejercer en el sitio de cada dependencia y los funcionarios contratistas responsables.	15							Seguimiento mensual por parte del jefe de la oficina, con el fin de garantizar la disponibilidad de la información en los espacios temas disponeles.	Revisiones realizadas / revisiones programadas	12	1	1	1	1	Recurso humano y tecnologico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno
																		5	El administrador de la plataforma de herramientas cuando se requiera realizar configuración de las herramientas, verificar asegurar la confidencialidad de la integridad de la información de los datos de la dédicto, con el propósito de no tener inconvenientes de la información en caso que se presente una calidad.	15											
			R6	GDIS	I1	Servidores	Recurso Humano	Pérdidas de confidencialidad e integridad	**Pérdida de confidencialidad e integridad 1. Jefe de Oficina** **2. Profesional especializado y universitario** **3. Gargas contratistas** **4. Contratista. por 1. Inexistencia en la disciplina del personal** **2. Error en Usuarios dédicto 1. Ausencia del personal** **2. Entrenamiento insuficiente en seguridad**	Talento humano	1. Ausencia del personal 2. Entrenamiento insuficiente en seguridad 3. Falta de conocimiento acerca de la seguridad	1. Inexistencia en la disciplina del personal 2. Error en Usuarios	6	El jefe de dependencia verificara mensualmente personas que renuncian una vez los contratistas que desarrolla en la dependencia con el fin que no el contratista que una persona sea la encargada las actividades correspondientes , las ordenes del control ejercen a personas contratistas en el sitio de seguimiento de la dependencia.	16,17,20	Identificar y documentar documente las nuevos respectivos por las cuales de prevención y falta y reforzar capacitación en seguridad	Moderado	Moderado	Reducir (mitigar)	Solicitar concientizaciones de seguridad de la información para el personal de la dédicto, en temas de responsabilidad en seguridad	Charlas Realizadas / Charlas Programadas	4		1			Recurso humano y tecnologico	Jefe de Dependencia de la Oficina de Control Disciplinario Interno
			R6	GDIS	I8		Recurso Humano	Pérdidas de confidencialidad e integridad	1. Jefe de Oficina 2. Profesional especializado y universitario 3. Gargas contratistas 4. Contratista. **Pérdida de Disponibilidad de 1. Jefe de Oficina** **2. Profesional especializado y universitario** **3. Gargas contratistas** **4. Contratista. por 1. Perdida, Fuga de información.** **2. Entrega de información a terceros dédicto 1. Alta Rotación de Personal especializado** **2. Desconocimiento de políticas de seguridad de la información**	Talento humano	1. Alta Rotación de Personal especializado 2. Desconocimiento de políticas de seguridad de la información	1. Perdida, Fuga de información. 2. Entrega de información a terceros	6	Realizar seguridad de la información en las fechas programadas de actualizaciones de seguridad de la información, con el fin de que las dependencias asistan al proceso programado. Verificar las personas que asistieron y las que no asistieron a las capacitaciones y actividades. Establecer políticas que no permitan realizar cambios en el sitio de cada dependencia ya que se programan y los funcionarios y contratistas. Dar llamas programa y los funcionarios y contratistas a los siguientes establecimiento a actividades de capacitación. Dar mensajes recordatorios a las dependencias sobre el control que deben ejercer en el sitio de cada dependencia y los funcionarios contratistas responsables.	15,20	Identificar y documentar documente las nuevos respectivos por las cuales de prevención y falta y reforzar capacitación en seguridad	Bajo	Bajo	Aceptar	No	No							
																		6	El jefe de dependencia verificara mensualmente personas que renuncian una vez los contratistas que desarrolla en la dependencia con el fin que no el contratista que una persona sea la encargada las actividades correspondientes , las ordenes del control ejercen a personas contratistas en el sitio de seguimiento de la dependencia.	15											