Confidencial Riesgos SGSI 27001 CAR

Mapa de riesgo de gestión, fraude y seguridad de la información

Identificación del riesgo															Análisis del riesgo - Zonal o nivel de riesgo inherente									
Referencia	Macroproceso	Proceso	Dependencia	Tipo de riesgo	Clasificación del riesgo	Activo de información (aplica únicamente a riesgos de seguridad de la información)	Tipo de activo de información (aplica únicamente a riesgos de seguridad de la información)	Impacto	Fuentes generadoras de riesgos	Causa inmediata	Causa raiz	Amenazas (Causa inmediata) (aplica únicamente a riesgos de seguridad de la información)	Vulnerabilidades (Causa raiz) (aplica únicamente a riesgos de seguridad de la información)	Descripción del riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad inherente	%	Criterios de impacto	Observación de criterio	Impacto inherente	%	Zona o nivel de riesgo inherente	No. Control	Temáticas asociadas a los controles
TIC-RIG	Estratégico	Todos los Procesos	Oficina de Tecnologías de la Información y las Comunicaciones	Seguridad_de_la_información	Pérdida de integridad	Infraestructura que soporta los servicios y activos de información de TI	Hardware	Reputacional	Factor Interno: Tecnología			Manipulación con hardware	Falta de conciencia en seguridad	Posibilidad de pérdida de la integridad de información soportada en la infraestructura de TI, que soporta los servicios y activos de información, por vulneración de contraseñas o ingreso indebido a equipos de cómputo o dispositivos de almacenamiento de información.	365	Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	Menor	40%	Moderado	TIC-RIG1-C01	Custodia apropiada de la información
												Espionaje remoto	Almacenamiento sin protección											Copias de seguridad, contingencias y respaldo de información, planes de continuidad del negocio
	Estratégico	Todos los Procesos	Todas las Dependencias	Seguridad_de_la_información	Pérdida de confidencialidad	Infraestructura que soporta los servicios y activos de información de TI	Hardware	Reputacional	Factor Interno: Tecnología			Hurto de equipo	Uso inadecuado de los controles de acceso al edificio	Posibilidad de pérdida de la confidencialidad de información soportada en la infraestructura de TI, por falta de monitoreo en los controles de acceso físico a las edificaciones y recintos de la corporación, hurto de dispositivos electrónicos donde se almacene información, como computadores, servidores, discos duros externos y cualquier tipo de medio magnético.	365	Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	Menor	40%	Moderado	TIC-RIG1-C02	Custodia apropiada de la información
												Hurto de medios o documentos	Falta de conciencia en seguridad											Custodia apropiada de la información
	Estratégico	Todos los Procesos	Todas las Dependencias	Seguridad_de_la_información	Pérdida de disponibilidad	Infraestructura que soporta los servicios y activos de información de TI	Hardware	Reputacional	Factor Interno: Tecnología			Destrucción del equipo o medios	Mantenimiento insuficiente	Posibilidad de pérdida de la disponibilidad de la información, por fallas en la infraestructura que soporta los servicios y activos de información de TI, por falta de mantenimiento y revisiones periódicas o fallas catastróficas	365	Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	Menor	40%	Moderado	TIC-RIG1-C03	Mantenimiento preventivo y correctivo
												Accidente Importante	Conexión deficiente de cableado											Mantenimiento preventivo y correctivo
												Polvo, corrosión, congelamiento	Mantenimiento insuficiente											Mantenimiento preventivo y correctivo
	Estratégico	Todos los Procesos	Oficina de Tecnologías de la Información y las Comunicaciones	Seguridad_de_la_información	Pérdida de integridad	Sistemas de información que soporta los servicios y activos de información de TI para la prestación de los Servicios y ejecución del PAC.	Software	Reputacional	Factor Interno: Tecnología			Manipulación con software	Ausencia de mecanismos de monitoreo para brechas en la seguridad	Posibilidad de pérdida de integridad por la alteración de la información almacenada en los sistemas de información y bases de datos de la Corporación teniendo una afectación reputacional por demandas, investigaciones disciplinarias y o reclamos por parte de usuarios.	365	Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	Menor	40%	Moderado	TIC-RIG1-C04	Seguimiento a bases de datos
												Uso no autorizado del equipo	Almacenamiento sin protección											Custodia apropiada de la información
												Corrupción de los datos	Ausencia de procedimientos y/o de políticas en general											Validación de información por parte de una persona o comité (revisión, comparación, verificación, validación, inspección, conciliación)

Confidencial - Riesgos SGSI 27001 CAR

Mapa de riesgo de gestión, fraude y seguridad de la información

Evaluación del riesgo - Diseño y valoración de controles											Evaluación del riesgo - Zonal o nivel de riesgo residual					Tratamiento del riesgo - Plan de acción				
Descripción del control	Afectación	Tipo	Implementación	Calificación	Documentación	Indicar documento	Frecuencia	Evidencia	Indicar registro		Probabilidad residual	%	Impacto residual	%	Zona o nivel de riesgo residual	Tratamiento	No. Acción	Acción	Responsable	Registro/producto o evidencia de la acción	Fecha límite (dd-mm-aaaa)
El profesional de la OTIC encargado de la administración de usuarios de acuerdo a las solicitudes recibidas por el Sistema de Gestión de Usuarios - SIGU, crea los usuarios para el acceso a los aplicativos y bases de datos, siguiendo el Procedimiento TIC-PR-13 Administración Cuentas de Usuario, dándole acceso solo a los sistemas y roles que requiera para el desarrollo de su trabajo, evidencia: registros del SIGU. Controles Anexo A ISO 27001 2022 - .5.1 - Políticas de seguridad de la información; 5.4 - Responsabilidades de gestión; 5.36 - Cumplimiento de las políticas, reglas y normas de seguridad de la información, 6.3 - Concienciación, educación y formación en seguridad de la información, 8.9 Gestión de la configuración El profesional líder de redes y comunicaciones monitorea diariamente la barrera electrónica de protección (Firewall), para garantizar la protección contra ataques cibernéticos, analizando el tráfico del firewall, revisando intentos de penetración repetidos, bloqueos, Malware y Phishing. Si se detectan nuevas amenazas se hace las recomendaciones y se establecen nuevas políticas. Evidencia: informe mensual de seguridad gestionada. Controles Anexo A ISO 27001 2022 - .5.1 - Políticas de seguridad de la información; 5.4 - Responsabilidades de gestión; 5.36 - Cumplimiento de las políticas, reglas y normas de seguridad de la información, 6.3 - Concienciación, educación y formación en seguridad de la información, 8.9 Gestión de la configuración, El profesional líder de infraestructura monitorea periodicamente la consola de antivirus para detectar vulnerabilidades. Evidencia: registros consola antivirus - Controles Anexo A ISO 27001 2022 - .5.1 - Políticas de seguridad de la información; 5.4 - Responsabilidades de gestión; 5.36 - Cumplimiento de las políticas, reglas y normas de seguridad de la información, 6.3 - Concienciación, educación y formación en seguridad de la información, 8.7 Protección contra malware 8.9 Gestión de la configuración	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-13 Administración Cuentas de Usuario	Continua	Con registro	Registros SIGU informa mensual de seguridad gestionada. registros consola antivirus	36,0%	Bajo	36%	Menor	40%	Moderado	Reducir (mitigar)	TIC-001-A01	1. Seguimiento a la aplicación de Procedimiento TIC-PR-13 Administración Cuentas de Usuario 2. Seguimiento Matriz de Seguimiento Políticas de Seguridad de la Información TIC-PI-02-MT-01 3. Seguimiento Informe mensual de seguridad gestionada. 4. Seguimiento Registros consola antivirus 5. Capacitación en Seguridad y privacidad de la información 6. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 7. Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional OTIC Gestión de usuarios Profesional líder de redes y comunicaciones Profesional líder de infraestructura Profesional seguridad de la información	1. Reporte SIGU 2. Matriz de Seguimiento Políticas de Seguridad de la Información TIC-PI-02-MT-01 3. Informe mensual de seguridad gestionada. 4. Registros consola antivirus 5. Registro de asistencia 6. Reporte de Socialización y Registro de asistencia 7. Reporte de Socialización y Registro de asistencia	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-13 Administración Cuentas de Usuario	Continua	Con registro	Registros SIGU informa mensual de seguridad gestionada. registros consola antivirus	36,0%	Bajo	36%	Menor	40%	Moderado	Reducir (mitigar)	TIC-001-A02	1. Seguimiento a la aplicación de Procedimiento TIC-PR-13 Administración Cuentas de Usuario 2. Seguimiento Matriz de Seguimiento Políticas de Seguridad de la Información TIC-PI-02-MT-01 3. Seguimiento Informe mensual de seguridad gestionada. 4. Seguimiento Registros consola antivirus 5. Capacitación en Seguridad y privacidad de la información 6. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 7. Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional OTIC Gestión de usuarios Profesional líder de redes y comunicaciones Profesional líder de infraestructura Profesional seguridad de la información	1. Reporte SIGU 2. Matriz de Seguimiento Políticas de Seguridad de la Información TIC-PI-02-MT-01 3. Informe mensual de seguridad gestionada. 4. Registros consola antivirus 5. Registro de asistencia 6. Reporte de Socialización y Registro de asistencia 7. Reporte de Socialización y Registro de asistencia	31/12/2024
El profesional del DAF encargado del seguimiento al contrato con la empresa de vigilancia contratada realiza supervisión a las actividades pactadas contractualmente a través de los informes entregados por dicha empresa. Evidencia: Informe de supervisión - Controles Anexo A ISO 27001:2022 - 7.1 - Perímetros de seguridad física; 7.2 - Entrada física; 7.3 - Seguridad de oficinas, salas e instalaciones; 7.4 - Vigilancia de la seguridad física. El Profesional de la OTIC encargado del control de ingreso y salida del centro de computo realiza el registro y control de acceso de acuerdo con el procedimiento TIC-PR-09 Control de Acceso al Centro de Cómputo y registro en el formato TIC-PR-09-FR-03. Evidencia: Registro en el formato TIC-PR-09-FR-03 - Controles Anexo A ISO 27001:2022 - 7.1 - Perímetros de seguridad física; 7.2 - Entrada física; 7.3 - Seguridad de oficinas, salas e instalaciones; 7.4 - Vigilancia de la seguridad física.	Probabilidad	Preventivo	Manual	40%	Documentado	Informes de supervisión	Continua	Con registro	Informes de supervisión	36,0%	Bajo	36%	Menor	40%	Moderado	Reducir (mitigar)	TIC-002-A01	1. Seguimiento mensual al informe desupervisión 2. Capacitación en Seguridad y privacidad de la información 3. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 4. Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional de DAF Profesional seguridad de la información	1. Informe de supervisión firmado 2. Registros de asistencia 3. Reporte de Socialización y Registro de asistencia 4. Reporte de Socialización y Registro de asistencia	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-09 Control de Acceso al Centro de Cómputo y registro en el formato TIC-PR-09-FR-03.	Continua	Con registro	TIC-PR-09 Control de Acceso al Centro de Cómputo Formato TIC-PR-09-FR-03.	36,0%	Bajo	36%	Menor	40%	Moderado	Reducir (mitigar)	TIC-002-A02	1. Seguimiento a la aplicación de Procedimiento TIC-PR-09 Control de Acceso al Centro de Cómputo 2. Capacitación en Seguridad y privacidad de la información 3. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 4. Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional de OTIC Profesional seguridad de la información	1. Formato TIC-PR-09-FR-03. 2. Registros de asistencia 3. Reporte de Socialización y Registro de asistencia 4. Reporte de Socialización y Registro de asistencia	31/12/2024
El profesional de la OTIC encargado de la mesa de servicio realiza anualmente la programación para el mantenimiento preventivo de los equipos de acuerdo al procedimiento TIC-PR-04 Mantenimiento de Hardware y mediante el Sistema de Mesa de Ayuda hace seguimiento a la prestación del servicio de soporte técnico. Evidencia: programación de mantenimientos y reporte de requerimientos generado por la mesa de ayuda. Controles Anexo A ISO 27001 2022 - 7.13 Mantenimiento de los equipos El profesional de Gestión de Apoyo Logístico encargado del Programa de Mantenimiento General de Sedes Administrativas realiza la programación y seguimiento de los mantenimientos de acuerdo al procedimiento GAL-PR-08 Programa de Mantenimiento General de Sedes Administrativas . Evidencia: Registro formato GAL-PR-08-FR-05 Programa de Mantenimiento General de Sedes Administrativas - Controles Anexo A ISO 27001 2022 - 7.13 Mantenimiento de los equipos El profesional de DAF encargado del mantenimiento y revisión del correcto funcionamiento de las UPS del centro de datos, los dos circuitos y los dos tableros independientes alimentados por dos subestaciones independientes (Subestación Puente Acacia y Subestación Salitre) funcionen correctamente. Evidencia: Informe de mantenimiento y revisión -Controles Anexo A ISO 27001 2022 - 7.11 Servicios de apoyo	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-04 Mantenimiento de Hardware	Continua	Con registro	TIC-PR-04 Mantenimiento de Hardware	36,0%	Bajo	36%	Menor	40%	Moderado	Reducir (mitigar)	TIC-RSI-A01	1. Seguimiento a la aplicación de procedimiento TIC-PR-04 Mantenimiento de Hardware	Profesional OTIC	1. Informe de seguimiento al mantenimiento	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-04 Mantenimiento de Hardware	Continua	Con registro	TIC-PR-04 Mantenimiento de Hardware	36,0%	Bajo	36%	Menor	40%	Moderado	Reducir (mitigar)	TIC-RSI-A02	1. Seguimiento a la aplicación de procedimiento TIC-PR-04 Mantenimiento de Hardware	Profesional OTIC	1. Informe de seguimiento al mantenimiento	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	GAL-PR-08 Mantenimiento General de Sedes Administrativas Formato GAL-PR-08-FR-05 Programa de Mantenimiento General de Sedes Administrativas	Continua	Con registro	Formato GAL-PR-08-FR-05 Programa de Mantenimiento General de Sedes Administrativas	36,0%	Bajo	36%	Menor	40%	Moderado	Reducir (mitigar)	TIC-RSI-A03	1. Seguimiento a la aplicación de procedimiento GAL-PR-08 Mantenimiento General de Sedes Administrativas 2. Revisión del informe de mantenimiento y revisión UPS, circuitos y los dos tableros	Profesional DAF	1. Formato GAL-PR-08-FR-05 Programa de Mantenimiento General de Sedes Administrativas 2. Informe de mantenimiento y revisión UPS, circuitos y los dos tableros	31/12/2024
El profesional líder de redes y comunicaciones monitorea diariamente la barrera electrónica de protección (Firewall), para garantizar la protección contra ataques cibernéticos, analizando el tráfico del firewall, revisando intentos de penetración repetidos, bloqueos, Malware y Phishing. Si se detectan nuevas amenazas se hace las recomendaciones y se establecen nuevas políticas. Evidencia: informe mensual de seguridad gestionada, teniendo en cuenta el TIC-PR-10 - Gestión de Incidentes de Seguridad de la Información. Controles Anexo A ISO 27001 2022 - .5.1 - Políticas de seguridad de la información; 5.4 - Responsabilidades de gestión; 5.36 - Cumplimiento de las políticas, reglas y normas de seguridad de la información, 6.3 - Concienciación, educación y formación en seguridad de la información, 8.9 Gestión de la configuración	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-10 - Gestión de Incidentes de Seguridad de la Información	Continua	Con registro	TIC-PR-10 - Gestión de Incidentes de Seguridad de la Información	36,0%	Bajo	36%	Menor	40%	Moderado	Reducir (mitigar)	TIC-004-A01	1. Seguimiento a la aplicación del procedimiento TIC-PR-10 - Gestión de Incidentes de Seguridad de la Información 2. Capacitación en Seguridad y privacidad de la información 3. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 4. Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional líder de redes y comunicaciones Profesional seguridad de la información	1. Informe Gestión de Incidentes de Seguridad de la Información 2. Registros de asistencia 3. Reporte de Socialización y Registro de asistencia 4. Reporte de Socialización y Registro de asistencia	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-10 - Gestión de Incidentes de Seguridad de la Información	Continua	Con registro	TIC-PR-10 - Gestión de Incidentes de Seguridad de la Información	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-004-A02	1. Seguimiento a la aplicación del procedimiento TIC-PR-10 - Gestión de Incidentes de Seguridad de la Información 2. Capacitación en Seguridad y privacidad de la información 3. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 4. Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional líder de redes y comunicaciones Profesional seguridad de la información	1. Informe Gestión de Incidentes de Seguridad de la Información 2. Registros de asistencia 3. Reporte de Socialización y Registro de asistencia 4. Reporte de Socialización y Registro de asistencia	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-10 - Gestión de Incidentes de Seguridad de la Información	Continua	Con registro	TIC-PR-10 - Gestión de Incidentes de Seguridad de la Información	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-004-A03	1. Seguimiento a la aplicación del procedimiento TIC-PR-10 - Gestión de Incidentes de Seguridad de la Información 2. Capacitación en Seguridad y privacidad de la información 3. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 4. Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional líder de redes y comunicaciones Profesional seguridad de la información	1. Informe Gestión de Incidentes de Seguridad de la Información 2. Registros de asistencia 3. Reporte de Socialización y Registro de asistencia 4. Reporte de Socialización y Registro de asistencia	31/12/2024

Confidencial - Riesgos SGSI 27001 CAR

Mapa de riesgo de gestión, fraude y seguridad de la información

TIC-GRD	Estratégico	Todos los Procesos	Todas las Dependencias	Seguridad_de_la_información	Pérdida de confidencialidad	Sistemas de Información que soporta los servicios y activos de información de TI para la prestación de los Servicios y ejecución del PAC.	Software	Reputacional	Factor Interno: Tecnología			Divulgación	Almacenamiento sin protección	Posibilidad de pérdida de la confidencialidad debido a la divulgación de información reservada o confidencial, teniendo una afectación reputacional por demandas, investigaciones disciplinarias y o reclamos por parte de usuarios.	365	Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	Menor	40%	Moderado	TIC-RSG-C05	Custodia apropiada de la información
												Procesamiento ilegal de datos	Ausencia de procedimientos y/o de políticas en general												Validación de información por parte de un sistema o aplicativo
	Estratégico	Todos los Procesos	Todas las Dependencias	Seguridad_de_la_información	Pérdida de disponibilidad	Sistemas de Información que soporta los servicios y activos de información de TI para la prestación de los Servicios y ejecución del PAC.	Software	Reputacional	Factor Interno: Tecnología			Pérdida de suministro de energía	Red eléctrica inestable	Posibilidad de afectación reputacional por interrupción de los tramites, servicios y procesos internos de la corporación debido a la perdida de disponibilidad de la información.	365	Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	Menor	40%	Moderado	TIC-RSG-C06	Mantenimiento preventivo y correctivo
												Falla en equipo de telecomunicaciones	Mantenimiento insuficiente												Mantenimiento preventivo y correctivo
												Saturación del sistema de información	Ausencia de procedimientos y/o de políticas en general												Seguimiento al cumplimiento de normas o tiempos de respuesta
												Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente												Mantenimiento preventivo y correctivo
												Vencimiento de licencias de software	Ausencia de controles y gestión para la renovación de licencias												Licencias de software
	Todos los Macroprocesos	Todos los Procesos	Todas las Dependencias	Seguridad_de_la_información	Pérdida de integridad	Información Documentada que soporta los servicios y activos de información para la prestación de los Servicios y ejecución del PAC.	Información	Reputacional	Factor Interno: Procesos			Hurto de medios o documentos	Almacenamiento sin protección	Posibilidad de pérdida de la integridad de la Información física (documentos y expedientes) que soportan los servicios que presta la CAR, por vulneración en el acceso no autorizado y mal almacenamiento de la información.	365	Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	Menor	40%	Moderado	TIC-RSG-C07	Custodia apropiada de la información
												Manipulación con software	Falta de conciencia en seguridad												Copias de seguridad, contingencias y respaldo de información, planes de continuidad del negocio
TIC-GRD	Todos los Macroprocesos	Todos los Procesos	Todas las Dependencias	Seguridad_de_la_información	Pérdida de confidencialidad	Información Documentada que soporta los servicios y activos de información para la prestación de los Servicios y ejecución del PAC.	Información	Reputacional	Factor Interno: Procesos			Divulgación	Almacenamiento sin protección	Posibilidad de pérdida de la confidencialidad de la Información física (documentos y expedientes) que soportan los servicios que presta la CAR, por vulneración en el acceso no autorizado y mal almacenamiento de la información.	365	Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	Menor	40%	Moderado	TIC-RSG-C08	Custodia apropiada de la información
												Manipulación con software	Falta de conciencia en seguridad												Copias de seguridad, contingencias y respaldo de información, planes de continuidad del negocio
	Todos los Macroprocesos	Todos los Procesos	Todas las Dependencias	Seguridad_de_la_información	Pérdida de disponibilidad	Información Documentada que soporta los servicios y activos de información para la prestación de los Servicios y ejecución del PAC.	Información	Reputacional	Factor Interno: Procesos			Hurto de medios o documentos	Almacenamiento sin protección	Posibilidad de pérdida de disponibilidad de la Información física (documentos y expedientes) que soporta los servicios que presta la CAR, por vulneración en el acceso no autorizado y mal almacenamiento de la información.	365	Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	Menor	40%	Moderado	TIC-RSG-C09	Custodia apropiada de la información
												Manipulación con software	Falta de conciencia en seguridad												Capacitación/ divulgación/ socialización

Mapa de riesgo de gestión, fraude y seguridad de la información

El profesional de la OTIC encargado de la administración de usuarios de acuerdo a las solicitudes recibidas por el Sistema de Gestión de Usuarios - SIGU, crea los usuarios para el acceso a los aplicativos y bases de datos, siguiendo el Procedimiento TIC-PR-13 Administración Cuentas de Usuario, dándole acceso solo a los sistemas y roles que requiera para el desarrollo de su trabajo, evidencia: registros del SIGU. Controles Anexo A ISO 27001 2022 - 5.1 - Políticas de seguridad de la información; 5.4 - Responsabilidades de gestión; 5.36 - Cumplimiento de las políticas, reglas y normas de seguridad de la información, 6.3 - Concienciación, educación y formación en seguridad de la información, 8.9 Gestión de la configuración	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-13 Administración Cuentas de Usuario	Continua	Con registro	Registros Sistema de Gestión de Usuarios -SIGU	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-RSI-A01	1. Seguimiento a la aplicación de Procedimiento TIC-PR-13 Administración Cuentas de Usuario 2. Capacitación en Seguridad y privacidad de la información 3. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 4 Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional OTIC Gestión de usuarios Profesional seguridad de la información	1. Reporte SIGU 2. Registro de asistencia 3. Reporte de Socialización y Registro de asistencia 4. Reporte de Socialización y Registro de asistencia	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-13 Administración Cuentas de Usuario	Continua	Con registro	TIC-PI-13 Administración Cuentas de Usuario	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-RSI-A012	1. Seguimiento a la aplicación de Procedimiento TIC-PR-13 Administración Cuentas de Usuario 2. Capacitación en Seguridad y privacidad de la información 3. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 4 Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional OTIC Gestión de usuarios Profesional seguridad de la información	1. Reporte SIGU 2. Registro de asistencia 3. Reporte de Socialización y Registro de asistencia 4. Reporte de Socialización y Registro de asistencia	31/12/2024
El profesional de la OTIC encargado de la mesa de servicio realiza anualmente la programación para el mantenimiento preventivo de los equipos de acuerdo al procedimiento TIC-PR-04 Mantenimiento de Hardware y mediante el Sistema de Mesa de Ayuda hace seguimiento a la prestación del servicio de soporte técnico. Evidencia: programación de mantenimientos y reporte de requerimientos generado por la mesa de ayuda. Controles Anexo A ISO 27001 2022 - 7.13 Mantenimiento de los equipos El profesional de DAF encargado del mantenimiento y revisión del correcto funcionamiento de las UPS del centro de datos, los dos circuitos y los dos tableros independientes alimentados por dos subestaciones independientes (Subestación Puente Aranda y Subestación Salitre) funcionen correctamente. Evidencia: Informe de mantenimiento y revisión -Controles Anexo A ISO 27001 2022 - 7.11 Servicios de apoyo El profesional de la OTIC líder de desarrollo de software, verifica que el software de nuevos desarrollos o modificado sea probado en el ambiente de pruebas, para verificar la seguridad y el correcto funcionamiento, siguiendo los procedimientos TIC-PR-12 Aseguramiento de la Calidad en el Desarrollo de Proyectos de Software y Control de Cambios y en caso de no cumplir con los objetivos se deben realizar los ajustes correspondientes. Evidencia: Formatos diligenciados del procedimiento TIC-PR-12 Aseguramiento de la Calidad en el Desarrollo de Proyectos de Software y Control de Cambios x - Controles Anexo A ISO 27001 2022 8.33 Información de la prueba, 8.32 Gestión del cambio, 8.31 Separación de los entornos de desarrollo, prueba y producción, 8.29 Pruebas de seguridad en el desarrollo y la aceptación, 8.25 Ciclo de vida del desarrollo seguro, 8.26 Requisitos de seguridad de las aplicaciones, El profesional de la OTIC encargado del licenciamiento de software, realiza el proceso precontractual para la renovación y adquisición de licencias teniendo en cuenta la revisión de los términos de vencimiento. Evidencia: Procesos contratuales para adquisición de licencias -Controles Anexo A ISO 27001 2022 - 8.6 Gestión de la capacidad	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-04 Mantenimiento de Hardware	Continua	Con registro	TIC-PR-04 Mantenimiento de Hardware	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-RSI-A05	1. Seguimiento a la aplicación de procedimiento TIC-PR-04 Mantenimiento de Hardware	Profesional OTIC	1. Informe de mantenimiento	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-04 Mantenimiento de Hardware	Continua	Con registro	TIC-PR-04 Mantenimiento de Hardware	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-RSI-A05	1. Seguimiento a la aplicación de procedimiento TIC-PR-04 Mantenimiento de Hardware	Profesional OTIC	1. Informe de mantenimiento	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	GAL-PR-08 Mantenimiento General de Sedes Administrativas Formato GAL-PR-08-FR-05 Programa de Mantenimiento General de Sedes Administrativas	Continua	Con registro	Formato GAL-PR-08-FR-05 Programa de Mantenimiento General de Sedes Administrativas	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-RSI-A03	1. Seguimiento a la aplicación de procedimiento GAL-PR-08 Mantenimiento General de Sedes Administrativas 2. Revisión del informe de mantenimiento y revisión UPS, circuitos y los dos tableros	Profesional DAF	1. Formato GAL-PR-08-FR-05 Programa de Mantenimiento General de Sedes Administrativas 2. Informe de mantenimiento y revisión UPS, circuitos y los dos tableros	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PR-12 Aseguramiento de la Calidad en el Desarrollo de Proyectos de Software y Control de Cambios	Continua	Con registro	Formatos diligenciados del procedimiento TIC-PR-12 Aseguramiento de la Calidad en el Desarrollo de Proyectos de Software y Control de Cambios	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-RSI-A04	1. Seguimiento a la aplicación de procedimiento TIC-PR-12 Aseguramiento de la Calidad en el Desarrollo de Proyectos de Software y Control de Cambios	El profesional de la OTIC líder de desarrollo de software	1. Formatos diligenciados del procedimiento TIC-PR-12 Aseguramiento de la Calidad en el Desarrollo de Proyectos de Software y Control de Cambios	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	Procesos contractuales para adquisición de licencia	Continua	Con registro	Ordenes de compra	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-RSI-A05	1. Seguimiento a la compra de licencias	Profesional OTIC	1. Matriz de control y seguimiento	31/12/2024
El profesional de Gestion Documental debe Liderar la administración de la documentación física y electrónica que se produce, recepciona, distribuye y se organiza durante el ciclo de vida de acuerdo con la normatividad aplicable en la Corporación teniendo en cuenta la Política de Gestión Documental GDO-PL-01, el Manual de Gestion Documental GDO-MN-01 Evidencia: Registro de GDO-PR-07-MT-01 Tabla de Retencion Documental. Controles Anexo A ISO 27001 2022 5.1 - Políticas de seguridad de la información; 5.4 - Responsabilidades de gestión; 5.12 Clasificación de la información, 5.36 - Cumplimiento de las políticas, reglas y normas de seguridad de la información El profesional de la OTIC encargado de la administración de usuarios de acuerdo a las solicitudes recibidas por el Sistema de Gestión de Usuarios - SIGU, crea los usuarios para el acceso a los aplicativos y bases de datos, siguiendo el Procedimiento TIC-PR-13 Administración Cuentas de Usuario, dándole acceso solo a los sistemas y roles que requiera para el desarrollo de su trabajo, Evidencia: registros del SIGU. Controles Anexo A ISO 27001 2022 - 5.1 - Políticas de seguridad de la información; 5.4 - Responsabilidades de gestión; 5.36 - Cumplimiento de las políticas, reglas y normas de seguridad de la información, 6.3 - Concienciación, educación y formación en seguridad de la información, 8.9 Gestión de la configuración El profesional de la OTIC encargado de la seguridad y privacidad de la información de la entidad realiza el del seguimiento al cumplimiento de las políticas, reglas y normas de seguridad de la información teniendo en cuenta el documento TIC-PI-02-MT-01 Matriz de Seguimiento Políticas de Seguridad de la Información y documento TIC-MIN-03-FR-04 Indice de Información Clasificada y Reservada. Controles Anexo A ISO 27001 2022 - 5.1 Políticas de seguridad de la información, 5.9 Inventario de la información y otros activos asociados, 5.12 Clasificación de la información, 5.15 Control de acceso, 5.33 Protección de documentos, 5.36 Cumplimiento de las políticas, reglas y normas de seguridad de la información	Probabilidad	Preventivo	Manual	40%	Documentado	Política de Gestión Documental GDO-PL-01 Manual de Gestion Documental GDO-MN-01 GDO-PR-07-MT-01 Tabla de Retencion Documental TIC-PR-13 Administración Cuentas de Usuario	Continua	Con registro	GDO-PR-07-MT-01 Tabla de Retencion Documental TIC-PR-13 Administración Cuentas de Usuario	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-RSI-A01	1. Seguimiento a la aplicación de la Política de Gestión Documental GDO-PL-01 y Manual de Gestion Documental GDO-MN-01 2. Seguimiento a la aplicación de Procedimiento TIC-PR-13 Administración Cuentas de Usuario 3. Capacitación en Seguridad y privacidad de la información 4. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 5. Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional de Gestion Documental Profesional OTIC Gestión de usuarios Profesional seguridad de la información	1. GDO-PR-07-MT-01 Tabla de Retencion Documental 2. Reporte SIGU 3. Registro de asistencia 4. Reporte de Socialización y Registro de asistencia 5. Reporte de Socialización y Registro de asistencia	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	TIC-PI-02-MT-01 Matriz de Seguimiento Políticas de Seguridad de la Información TIC-MIN-03-FR-04 Indice de Información Clasificada y Reservada	Continua	Con registro	TIC-PI-02-MT-01 Matriz de Seguimiento Políticas de Seguridad de la Información TIC-MIN-03-FR-04 Indice de Información Clasificada y Reservada	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-RSI-A02	1. Seguimiento a la aplicación de los formatos TIC-PI-02-MT-01 Matriz de Seguimiento Políticas de Seguridad de la Información y actualización de la matriz TIC-MIN-03-FR-04 Indice de Información Clasificada y Reservada 2. Capacitación en Seguridad y privacidad de la información 3. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 4 Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional seguridad de la información	1. formatos TIC-PI-02-MT-01 Matriz de Seguimiento Políticas de Seguridad de la Información y TIC-MIN-03-FR-04 Indice de Información Clasificada y Reservada 2. Registro de asistencia 3. Reporte de Socialización y Registro de asistencia 4. Reporte de Socialización y Registro de asistencia	31/12/2024
El profesional de Gestion Documental debe Liderar la administración de la documentación física y electrónica que se produce, recepciona, distribuye y se organiza durante el ciclo de vida de acuerdo con la normatividad aplicable en la Corporación teniendo en cuenta la Política de Gestión Documental GDO-PL-01, el Manual de Gestion Documental GDO-MN-01 Evidencia: Registro de GDO-PR-07-MT-01 Tabla de Retencion Documental. Controles Anexo A ISO 27001 2022 5.1 - Políticas de seguridad de la información; 5.4 - Responsabilidades de gestión; 5.12 Clasificación de la información, 5.36 - Cumplimiento de las políticas, reglas y normas de seguridad de la información El profesional de la OTIC encargado de la administración de usuarios de acuerdo a las solicitudes recibidas por el Sistema de Gestión de Usuarios - SIGU, crea los usuarios para el acceso a los aplicativos y bases de datos, siguiendo el Procedimiento TIC-PR-13 Administración Cuentas de Usuario, dándole acceso solo a los sistemas y roles que requiera para el desarrollo de su trabajo, evidencia: registros del SIGU. Controles Anexo A ISO 27001 2022 - 5.1 - Políticas de seguridad de la información; 5.4 - Responsabilidades de gestión; 5.36 - Cumplimiento de las políticas, reglas y normas de seguridad de la información, 6.3 - Concienciación, educación y formación en seguridad de la información, 8.9 Gestión de la configuración El profesional de la OTIC encargado de la seguridad y privacidad de la información de la entidad realiza el del seguimiento al cumplimiento de las políticas, reglas y normas de seguridad de la información teniendo en cuenta el documento TIC-PI-02-MT-01 Matriz de Seguimiento Políticas de Seguridad de la Información y documento TIC-MIN-03-FR-04 Indice de Información Clasificada y Reservada. Controles Anexo A ISO 27001 2022 - 5.1 Políticas de seguridad de la información, 5.9 Inventario de la información y otros activos asociados, 5.12 Clasificación de la información, 5.15 Control de acceso, 5.33 Protección de documentos, 5.36 Cumplimiento de las políticas, reglas y normas de seguridad de la información	Probabilidad	Preventivo	Manual	40%	Documentado	Política de Gestión Documental GDO-PL-01 Manual de Gestion Documental GDO-MN-01 GDO-PR-07-MT-01 Tabla de Retencion Documental TIC-PR-13 Administración Cuentas de Usuario	Continua	Con registro	GDO-PR-07-MT-01 Tabla de Retencion Documental TIC-PR-13 Administración Cuentas de Usuario	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-RSI-A01	1. Seguimiento a la aplicación de la Política de Gestión Documental GDO-PL-01 y Manual de Gestion Documental GDO-MN-01 2. Seguimiento a la aplicación de Procedimiento TIC-PR-13 Administración Cuentas de Usuario 3. Capacitación en Seguridad y privacidad de la información 4. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 5. Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional de Gestion Documental Profesional OTIC Gestión de usuarios Profesional seguridad de la información	1. GDO-PR-07-MT-01 Tabla de Retencion Documental 2. Reporte SIGU 3. Registro de asistencia 4. Reporte de Socialización y Registro de asistencia 5. Reporte de Socialización y Registro de asistencia	31/12/2024
	Probabilidad	Preventivo	Manual	40%	Documentado	IC-PI-02-MT-01 Matriz de Seguimiento Políticas de Seguridad de la Información TIC-MIN-03-FR-04 Indice de Información Clasificada y Reservada	Continua	Con registro	TIC-PI-02-MT-01 Matriz de Seguimiento Políticas de Seguridad de la Información TIC-MIN-03-FR-04 Indice de Información Clasificada y Reservada	36,0%	Bajo	36%	Leve	0%	Bajo	Reducir (mitigar)	TIC-RSI-A02	1. Seguimiento a la aplicación de los formatos TIC-PI-02-MT-01 Matriz de Seguimiento Políticas de Seguridad de la Información y actualización de la matriz TIC-MIN-03-FR-04 Indice de Información Clasificada y Reservada 2. Capacitación en Seguridad y privacidad de la información 3. Socialización de las Políticas de seguridad de la información adoptadas por la entidad. 4 Socialización del Plan de Seguridad y privacidad de la información TIC-PN-08	Profesional seguridad de la información	1. formatos TIC-PI-02-MT-01 Matriz de Seguimiento Políticas de Seguridad de la Información y TIC-MIN-03-FR-04 Indice de Información Clasificada y Reservada 2. Registro de asistencia 3. Reporte de Socialización y Registro de asistencia 4. Reporte de Socialización y Registro de asistencia	31/12/2024

Confidencial - Riesgos 9001 27001 CAR