

Proceso:		Tecnología de la Información																																	
Objetivo:		Proveer servicios informáticos de calidad a partir de la gestión de la infraestructura para contribuir al desarrollo al desarrollo permanente de la institución.																																	
Alcance:		Aplica desde la prospectiva de las tecnologías informáticas e identificación de los requerimientos hasta la implementación de soluciones tecnológicas para el mejoramiento en la prestación del servicio.																																	
		Código: FMC01																																	
		Versión: 03																																	
Riesgo Tipo de Actividad	Identificación del riesgo	Análisis del riesgo inherente										Evaluación del riesgo - Valoración de los controles								Evaluación del riesgo - Nivel de riesgo residual			Plan de Acción												
		Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de Impacto	Observación de criterio	Impacto Inherente	%	Zona de Riesgo Inherente	N. Control	Descripción del Control	Afectación	Atributos				Probabilidad Residual	Probabilidad de Residual Final	I ²	Zona de Riesgo Final	I ²	Tratamiento	Plan de Acción	Responsable						
																		Tipo	Implementación	Calificación	Documentación									Frecuencia	Efectiva				
1	Proceso Información	Perdida de la confidencialidad	Económico y Reputacional	Abuso de los derechos	<ul style="list-style-type: none"> Privilegios de acceso excesivo o malintencionado Uso abusivo de los privilegios otorgados 	Privilegios otorgados permitiendo abusos en el acceso a los activos informáticos, lo que podría causar la pérdida de confidencialidad sobre los activos de información.	Usuarios, productos y prácticas organizacionales	365	Medio	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	Personal de soporte técnico realiza el mantenimiento al directorio activo de cuentas de usuarios (período de acceso)	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	36,0%	Bajo	36%	60%	Moderado	Reduzir (mitig)	Gestionar el contrato para el personal de soporte técnico anualmente. Creación y divulgación de políticas de control de acceso, orientadas a mantener la confidencialidad de la información.	Coordinación de Informática Corporativa			
																			2	El profesional de la dependencia administra los licenciamientos de software	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	21,6%	Bajo	22%	69%	Moderado	Reduzir (mitig)	Gestionar los contratos para la renovación del licenciamiento anualmente.	Coordinación de Informática Corporativa
2	Proceso Información	Perdida de la confidencialidad	Económico y Reputacional	Hurto de medios o documentos	<ul style="list-style-type: none"> Falta de protección de los copias de seguridad Falta de seguridad en gestión de la información sensible 	Falta de protección de las copias de seguridad y de custodia en gestión de la información sensible puede permitir su hurto, lo que podría causar la pérdida de confidencialidad de la información.	Usuarios, productos y prácticas organizacionales	365	Medio	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	La Coordinación de informática corporativa administra las llaves de acceso al data center	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	36,0%	Bajo	38%	60%	Moderado	Reduzir (mitig)	Gestionar el mantenimiento del acceso al datacenter	Coordinación de Informática Corporativa			
																			2	El ingeniero de soporte técnico programa y verifica los respaldos en el software para backups	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	18,0%	Muy Bajo	18%	60%	Moderado	Reduzir (mitig)		
3	Proceso Software	Perdida de la confidencialidad	Económico y Reputacional	<ul style="list-style-type: none"> Abuso de los derechos Error en el uso Falsificación de derechos Procesamiento legal de datos Mal funcionamiento del software 	<ul style="list-style-type: none"> Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo Asignación errada de los derechos de acceso Configuración incorrecta de parámetros Ausencia de mecanismos de identificación y autenticación Habilitación de servicios innecesarios Software nuevo o modificado 	Ausencia o falencias de mecanismos de identificación y autenticación pueden ocasionar abusos de derechos y error en el uso, lo que causaría la pérdida de confidencialidad en el software o posibilidad de acceso a S.O, memorias de Bases de Datos y/o software institucional, sin ningún tipo de restricción.	Usuarios, productos y prácticas organizacionales	100	Medio	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	Personal de soporte técnico realiza el mantenimiento al directorio activo de cuentas de usuarios	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	36,0%	Bajo	36%	60%	Moderado	Reduzir (mitig)	Coordinar campaña con comunicaciones sobre uso de contraseñas fuertes para aplicaciones en general	Coordinación de Informática Corporativa			
																			2	El profesional universitario parametriza el acceso a las aplicaciones con criterios de contraseñas fuertes y encriptación por medio de algoritmos seguros.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	21,6%	Bajo	22%	60%	Moderado	Reduzir (mitig)	Gestión y divulgación de políticas de control de acceso, orientadas a mantener la confidencialidad en el software	Coordinación de Informática Corporativa
																			3	El profesional universitario parametriza el acceso a las bases de datos con criterios de contraseñas fuertes	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	13,0%	Muy Bajo	13%	60%	Moderado	Reduzir (mitig)		
4	Proceso Hardware	Perdida de la confidencialidad	Económico y Reputacional	Error en el uso	<ul style="list-style-type: none"> Amenazamiento sin protección física Falta de custodia en la disposición final Copias no controlada 	Amenazamiento sin protección física y falta de custodia en la disposición final o Copias no controlada que facilita el error en el uso posibilitando la pérdida de confidencialidad en el hardware	Daños Activos Físicos	365	Medio	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	La coordinación de informática corporativa gestiona la recepción y emisión del diagnóstico del equipo antes de ser de baja	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	30,0%	Bajo	30%	60%	Moderado	Reduzir (mitig)	Formatear a bajo nivel cuando se va dar de baja un equipo	Coordinación de Informática Corporativa			
																			2	La Coordinación informática corporativa administra las llaves de acceso al data center	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	18,0%	Muy Bajo	18%	60%	Moderado	Reduzir (mitig)	Gestión y divulgación de políticas de control de acceso físico.	Coordinación de Informática Corporativa
5	Proceso Hardware	Perdida de la confidencialidad	Económico y Reputacional	Hurto de medios o documentos.	<ul style="list-style-type: none"> Ausencia de un eficiente control de cambios en la configuración 	La falta de políticas de seguridad, de control de acceso físico, mecanismo de autenticación débil, pueden facilitar el hurto, lo cual causaría la pérdida de la confidencialidad en el hardware	Daños Activos Físicos	365	Medio	60%	El riesgo afecta la imagen de alguna área de la organización	El riesgo afecta la imagen de alguna área de la organización	Leve	20%	Moderado	1	La coordinación gestiona el control de usuario y contraseñas para perfil de administrador	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	36,0%	Bajo	38%	20%	Bajo	Reduzir (mitig)					
																			2	El personal de soporte técnico controla los usuarios y contraseñas sin el directorio activo	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	21,6%	Bajo	22%	20%	Bajo	Reduzir (mitig)	Gestión y divulgación de políticas de control de acceso a las aplicaciones físicas a las instalaciones.	Coordinación de Informática Corporativa
																			3	La coordinación gestiona el control de acceso físico	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	13,0%	Muy Bajo	13%	20%	Bajo	Reduzir (mitig)	Gestionar los requisitos de funcionamiento de los accesos físicos.	Coordinación de Informática Corporativa
6	Proceso Servicios	Perdida de la confidencialidad	Económico y Reputacional	<ul style="list-style-type: none"> Error en el uso Abusos de los derechos 	<ul style="list-style-type: none"> Ausencia de procedimientos para el manejo de información clasificada Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos Ausencia de procedimientos formales para el registro y retiro de usuarios 	La ausencia de responsabilidades en seguridad de la información en las funciones del cargo, así como de procedimientos para el manejo de información clasificada y de registro y retiro de usuarios puede generar error en el uso y/o abuso de derechos, lo cual causaría pérdida de confidencialidad en el servicio	Usuarios, productos y prácticas organizacionales	365	Medio	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	1	Hacer cumplir los procedimientos documentados de retiro de usuarios	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	36,0%	Bajo	38%	40%	Menor	Reduzir (mitig)					
																			2		Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	21,6%	Bajo	22%	40%	Menor	Reduzir (mitig)	Coordinar con Gestión Humana la inclusión en la inducción y mentoría de la responsabilidad en la seguridad de la información. Gestionar con aduiciones la inclusión en el "light" de los requisitos de seguridad informática.	Coordinación de Informática Corporativa
7	Proceso Personal	Perdida de la confidencialidad	Económico y Reputacional	Error en el uso	<ul style="list-style-type: none"> Entrenamiento insuficiente en seguridad Uso incorrecto de software y hardware Falta de conciencia acerca de la seguridad 	Un entrenamiento insuficiente en seguridad informática y un uso incorrecto del software y hardware pueden facilitar el error en el uso, lo que causaría la pérdida de confidencialidad en el personal.	Usuarios, productos y prácticas organizacionales	4	Bajo	40%	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	1	Las funciones son distribuidas y asignadas de acuerdo con conocimientos y experiencia	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	24,0%	Bajo	24%	40%	Menor	Reduzir (mitig)	Crear cultura organizacional sobre la seguridad de la información	Coordinación de Informática Corporativa			
																			2		Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	14,4%	Muy Bajo	14%	40%	Bajo	Reduzir (mitig)	Capacitación a usuarios en buen uso de hardware y software	Coordinación de Informática Corporativa
8	Proceso Personal	Perdida de la confidencialidad	Económico y Reputacional	Procesamiento legal de los datos	<ul style="list-style-type: none"> Ausencia de mecanismos de monitoreo 	La ausencia de mecanismos de monitoreo puede facilitar el procesamiento legal de los datos, lo cual podría generar pérdida de confidencialidad de los procesos realizados por el personal	Usuarios, productos y prácticas organizacionales	365	Medio	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	1	Revisión de logs de eventos	Probabilidad	Preventivo	Manual	30%	Documentado	Continua	Con Registro	42,0%	Medio	42%	40%	Menor	Reduzir (mitig)	Creación y divulgación de políticas de registro y auditoría	Coordinación de Informática Corporativa			
																			2		Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	15,0%	Muy Bajo	15%	40%	Bajo	Reduzir (mitig)		
9	Proceso Personal	Perdida de la confidencialidad	Económico y Reputacional	Hurto de medios o documentos.	<ul style="list-style-type: none"> Trabajo no supervisado del personal externo o de implica 	Un trabajo no supervisado del personal externo o de implica puede facilitar el hurto de medios o documentos lo que causaría la pérdida de confidencialidad del personal.	Usuarios, productos y prácticas organizacionales	365	Medio	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	Cámara de vigilancia	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	30,0%	Bajo	30%	60%	Moderado	Reduzir (mitig)	Creación y divulgación de políticas de control de acceso físico	Coordinación de Informática Corporativa			
																			2	Control de acceso biométrico	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	15,0%	Muy Bajo	15%	40%	Bajo	Reduzir (mitig)		
10	Proceso Personal	Perdida de la confidencialidad	Económico y Reputacional	Uso no autorizado del equipo	<ul style="list-style-type: none"> Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y manejo 	La ausencia de políticas para el uso correcto de los medios de telecomunicaciones y manejo puede generar un uso no autorizado del equipo, lo cual podría causar pérdida de confidencialidad en los procesos realizados por el personal	Usuarios, productos y prácticas organizacionales	365	Medio	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	1	Bloqueo de pantalla automático después de un tiempo de inactividad	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	36,0%	Bajo	38%	40%	Menor	Reduzir (mitig)					
																			2	Asignación de cuentas de correo electrónico por solicitud de gestión humana.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	21,6%	Bajo	22%	40%	Menor	Reduzir (mitig)		
																			3	Asignación de cuentas de correo electrónico para estudiantes	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	10,8%	Muy Bajo	11%	40%	Bajo	Reduzir (mitig)	Creación y divulgación de políticas de control de acceso.	Coordinación de Informática Corporativa

11	Proceso Integración	Conocimiento técnico relevante	Perdida de la confidencialidad	Económico	Reprocesos en la gestión de los Sistemas de información institucional	<ul style="list-style-type: none"> Ausencia de políticas de control de acceso a bases de conocimiento con información reservada 	La ausencia de políticas de control de acceso a bases de conocimiento con información reservada puede facilitar el reproceso en la gestión de los sistemas de información lo que causará pérdida de confidencialidad de los entregables	Ejecución y Administración de procesos	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	<p>1. Uso de la base del conocimiento de la dependencia</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>40%</p>	36,0%	36%	Menor	45%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar		
12	Proceso Información	<ul style="list-style-type: none"> Licencia Software Financiero Licencia Software Talento Humano Licencia software Sistema Gestión de Calidad Licencia Oracle Licencia Sistema de gestión documental 	Perdida de la Integridad	Económico y Reputacional	Abuso de los derechos	<ul style="list-style-type: none"> Privilegios de acceso excesivo o mal utilizado • Uso abusivo de los privilegios asignados 	Los privilegios de acceso excesivo o mal utilizado pueden facilitar el abuso de los derechos lo que causará la pérdida de integridad de la información.	Usuarios, productos y practicas , organizacionales	365	Media	60%	El riesgo afecta la imagen de alguna área de la organización	El riesgo afecta la imagen de alguna área de la organización	Leve	20%	Moderado	<p>1. Seguimiento, monitoreo y actualización de privilegios otorgados</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>40%</p>	36,0%	36%	Leve	20%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar	Creación y divulgación de políticas de registro y auditoría	Coordinación de Informática Corporativa
13	Proceso Información	<ul style="list-style-type: none"> Licencia Software Financiero Licencia Software Talento Humano Licencia software Sistema Gestión de Calidad Licencia Oracle Licencia Sistema de gestión documental Licencia Sistemas operativos Windows Licencia VMware Licencia System Center Licencia software administrativo (Otras no incluidas en la lista) Licencia OVS Licencia Software laboratorios Licencia Software Seguridad Perimetral Licencia Autentificación y Acreditación de 	Perdida de la Integridad	Económico y Reputacional	Corrupción de datos	<ul style="list-style-type: none"> • Errores en aplicativos web que permitan la infracción de código malicioso • Fallo o desactualización del software de ciberseguridad • Falta de diagnósticos de vulnerabilidades 	Errores en aplicativos web que producen vulnerabilidades y la falta de actualización del software de seguridad así como la ausencia de diagnóstico de vulnerabilidades, provocara corrupción de datos, lo cual causará la pérdida de integridad de la información	Usuarios, productos y practicas , organizacionales	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	<p>1. Aplicación de parches de seguridad (Software)</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>40%</p>	36,0%	36%	Menor	45%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar	Creación y divulgación de políticas de integridad	Coordinación de Informática Corporativa
14	Proceso Información	<ul style="list-style-type: none"> Licencia Software Financiero Licencia Software Talento Humano Licencia software Sistema Gestión de Calidad Licencia Oracle Licencia Sistema de gestión documental Licencia Sistemas operativos Windows Licencia VMware Licencia System Center Licencia software administrativo (Otras no incluidas en la lista) Licencia OVS Licencia Software laboratorios Licencia Software Seguridad Perimetral Licencia Autentificación y Acreditación de 	Perdida de la Integridad	Económico y Reputacional	Error en el uso	<ul style="list-style-type: none"> • Incorrecta configuración de las bases de datos • Falta de políticas para las auditorías de las bases de datos • Falta de contraseñas de autenticación fuertes para los usuarios de las bases de datos 	La falta de políticas para la configuración y definición de contraseñas de las bases de datos pueden facilitar un error en el uso lo que causará pérdida de integridad de la información.	Usuarios, productos y practicas , organizacionales	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	<p>1. Políticas y procedimientos de configuración de la seguridad de las bases de datos, documentados, aprobados y comunicados</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>40%</p>	36,0%	36%	Menor	45%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar	Creación y divulgación de políticas de integridad	Coordinación de Informática Corporativa
15	Proceso Software	<ul style="list-style-type: none"> Sistemas operativos Aplicaciones institucionales Software de bases de datos 	Perdida de la Integridad	Económico y Reputacional	Amenazas de agentes internos/ externos	<ul style="list-style-type: none"> • Ausencia de actualizaciones de parches. • Configuración equivocada o software • Gestión deficiente de software antiguo. • Descarga y uso no controlado de software 	La ausencia de actualizaciones de parches así como la configuración inadecuada del software antiguo y la falta de control en la descarga de software, puede facilitar Amenazas de agentes internos/ externos y manipulación con software, lo que causará pérdida de integridad en el software	Usuarios, productos y practicas , organizacionales	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	<p>1. Aplicar y desplegar parches sobre los diferentes productos de acuerdo con plan de mantenimiento</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>30%</p>	42,0%	25%	Menor	45%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar	Creación y divulgación de políticas de integridad	Coordinación de Informática Corporativa
16	Proceso Hardware	<ul style="list-style-type: none"> Servidores físicos Computadores área de red Switches Unidades de Backup Dispositivos de conectividad de redes Lineas Cableado estructurado Robots eléctricos 	Perdida de la Integridad	Económico y Reputacional	Error en el uso	<ul style="list-style-type: none"> • Ausencia de un eficiente control de cambios en la configuración 	La ausencia de un eficiente control de cambios en la configuración pueden causar un error en el uso lo que causará la pérdida de integridad del hardware.	Defectos Activos Físicos	365	Media	60%	El riesgo afecta la imagen de alguna área de la organización	El riesgo afecta la imagen de alguna área de la organización	Leve	20%	Moderado	<p>1. Aplicación de políticas y procedimientos del plan de seguridad de la información</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>40%</p>	36,0%	36%	Leve	20%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar	Creación y divulgación de políticas de integridad	Coordinación de Informática Corporativa
17	Proceso Servicios	<ul style="list-style-type: none"> Soporte Técnico Servicios de comunicación (Correo electrónico, reuniones , chat, trabajo colaborativo) Acceso a Internet Soporte telefónico Servicios de autenticación Robots eléctricos 	Perdida de la Integridad	Económico y Reputacional	Error en el uso	<ul style="list-style-type: none"> • Ausencia de políticas sobre el uso de correo electrónico • Equipos de comunicación obsoletos, y/o en mal estado • Personal no capacitado 	Equipos de comunicación obsoletos y/o en mal estado sumado a ausencia de políticas en el uso del correo electrónico y la falta de capacitación puede provocar error en el uso lo que ocasionará pérdida de integridad del Sistema de información lo cual causará pérdida de integridad en el servicio	Usuarios, productos y practicas , organizacionales	365	Media	60%	El riesgo afecta la imagen de alguna área de la organización	El riesgo afecta la imagen de alguna área de la organización	Leve	20%	Moderado	<p>1. Políticas y procedimientos documentados, aprobados y comunicados</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>40%</p>	36,0%	21%	Leve	20%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar	Creación y divulgación de políticas de integridad	Coordinación de Informática Corporativa
18	Proceso Personal	Personal de la Coordinación	Perdida de la disponibilidad	Económico y Reputacional	Error en el uso	<ul style="list-style-type: none"> • Entrenamiento insuficiente en seguridad • Uso incorrecto de software y hardware • Falta de conciencia acerca de la seguridad 	Un entrenamiento insuficiente y la falta de conciencia en la seguridad informática además de un uso incorrecto del software y hardware pueden causar un error en el uso lo que causará pérdida de integridad en el personal.	Usuarios, productos y practicas , organizacionales	365	Media	60%	El riesgo afecta la imagen de alguna área de la organización	El riesgo afecta la imagen de alguna área de la organización	Leve	20%	Moderado	<p>1. Envío de correos tipo de seguridad</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>40%</p>	36,0%	21%	Leve	20%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar	Creación y divulgación de políticas de disponibilidad	Coordinación de Informática Corporativa
19	Proceso Personal	Personal de la Coordinación	Perdida de la Integridad	Económico y Reputacional	Procesamiento legal de los datos	<ul style="list-style-type: none"> • Ausencia de mecanismos de monitoreo 	La ausencia de mecanismos de monitoreo podría desencadenar un procesamiento legal de datos lo cual causará pérdida de integridad en el proceso ejecutado por el personal de la coordinación.	Usuarios, productos y practicas , organizacionales	365	Media	60%	El riesgo afecta la imagen de alguna área de la organización	El riesgo afecta la imagen de alguna área de la organización	Leve	20%	Moderado	<p>1. Aplicación del SGS</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>40%</p>	36,0%	21%	Leve	20%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar	Creación y divulgación de políticas de integridad	Coordinación de Informática Corporativa
20	Proceso Personal	Personal de la Coordinación	Perdida de la Integridad	Económico y Reputacional	Hurto de medios o documentos.	<ul style="list-style-type: none"> • Trabajo no supervisado del personal externo o de limpieza 	Un trabajo no supervisado del personal externo o de limpieza puede provocar el hurto de medios o documentos lo que causará pérdida de integridad del personal.	Usuarios, productos y practicas , organizacionales	365	Media	60%	El riesgo afecta la imagen de alguna área de la organización	El riesgo afecta la imagen de alguna área de la organización	Leve	20%	Moderado	<p>1. Control de acceso físico</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>40%</p>	36,0%	21%	Leve	20%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar	Creación y divulgación de políticas de integridad	Coordinación de Informática Corporativa
21	Proceso Integración	Conocimiento técnico relevante	Perdida de la Integridad	Económico y Reputacional	Reprocesos en la gestión de los Sistemas de información institucional	<ul style="list-style-type: none"> • No se hace revisión por pares a balances o bases de conocimiento • Ausencia de cultura de gestión de conocimiento 	La falta de revisión por pares a balances o bases de conocimiento o la ausencia de cultura de gestión de este, pueden facilitar los reprocesos en la gestión de los sistemas de información, lo que causará pérdida de integridad de los entregables.	Ejecución y Administración de procesos	365	Media	60%	El riesgo afecta la imagen de alguna área de la organización	El riesgo afecta la imagen de alguna área de la organización	Leve	20%	Moderado	<p>1. Revisión por pares a balances o bases de conocimiento</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>30%</p>	42,0%	25%	Leve	20%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar	Creación y divulgación de políticas de integridad	Coordinación de Informática Corporativa
22	Proceso Lugar	Centro de datos	Perdida de la Integridad	Económico y Reputacional	Hurto de medios o documentos	<ul style="list-style-type: none"> • Uso inadecuado o descuido del control de acceso físico a las edificaciones y los recintos • Ausencia de protección física del edificio (Puertas y ventanas) • Red energética sensible • Ubicación en área susceptible de inundación 	La ausencia de protección física y el uso inadecuado del control de acceso físico así como también las redes energéticas sensibles, pueden ocasionar hurto de medios o documentos, destrucción de equipos o medios, falta en equipos de telecomunicaciones, lo cual causará pérdida de integridad en la infraestructura relacionada con el centro de datos	Ejecución y Administración de procesos	365	Media	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	<p>1. Políticas y procedimientos documentados, aprobados y comunicados</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>40%</p>	36,0%	21%	Medio	60%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar	Creación y divulgación de políticas de integridad	Coordinación de Informática Corporativa
23	Proceso Inf	<ul style="list-style-type: none"> Licencia Software Financiero Licencia Software Talento Humano Licencia software Sistema Gestión de 	Perdida de la Integridad	Económico y Reputacional	Hurto de medios o documentos	<ul style="list-style-type: none"> • Falta de protección de las copias de seguridad • Falta de cuidado en gestión de la 	La falta de protección de las copias de seguridad y la falta de cuidado en la gestión de la información sensible	Usuarios, productos y practicas , organizacionales	365	Media	60%	El riesgo afecta la imagen de alguna área de la organización	El riesgo afecta la imagen de alguna área de la organización	Leve	20%	Moderado	<p>1. Coordinación de informática corporativa administra las claves de acceso al data center</p> <p>Probabilidad</p> <p>Preventivo</p> <p>Manual</p> <p>40%</p>	36,0%	36%	Leve	20%	Bajo	Medio	Medio	Recur (ing) (ing)	Aceptar	Creación y divulgación de políticas de integridad	Coordinación de Informática Corporativa

