

MAPA DE RIESGOS DE SEGURIDAD DIGITAL



											Versión 1 Vigente a partir de diciembre 2020		
TIPO DE ACTIVO	ACTIVO	RIESGO	AMENAZA	VULNERABILIDAD	CONSECUENCIAS	CALIFICACIÓN DEL RIESGO			CONTROL QUE MITIGA EL RIESGO	CALIFICACIÓN DEL RESIDUAL	PLAN DE TRABAJO		
						Grado de probabilidad	Grado de impacto	ZONA DE RIESGO	CONTROL ASOCIADO		NUEVA ZONA DE RIESGO	ACCIONES	RESPONSABLE
SERVICIOS	BPM GESTOR DOCUMENTAL; SEVEN; KACTUS; PLATAFORMA DE PAGOS; INVESDOC	PÉRDIDA DE CONFIDENCIALIDAD	Incorrecta parametrización de los permisos sobre la información por un administrador del sistema.	Incorrecta administración de la plataforma	Publicación de información sensible o reservada. Daño jurídico a la Entidad.	1	4	ALTO	Logs de auditoría del sistema. Asignación de roles y perfiles.	ALTO	Realizar tareas de roll back	Profesional de gestión TIC y líderes funcionales	Correo electrónico
			Mal funcionamiento del software	Incorrecta ejecución de un control de cambios					Realización de etapa de pruebas.		Realizar tareas de restauración de backup	Profesional de gestión TIC y líderes funcionales	Correo electrónico
			Incorrecta utilización de la plataforma.	Desconocimiento, descuido o utilización indebida de la información por parte del funcionario.					Capacitación a funcionarios.		Brindar capacitaciones	Profesional de gestión TIC, líderes funcionales y profesional de GH	Evidencia de asistencia a capacitación
			Manipulación o divulgación de la información por parte de un funcionario, contratista o tercero	Intereses particulares o presión por parte de un tercero.					Clausula de confidencialidad de la información, funciones del personal, restricción de acceso a terceros según manual de seguridad		Realizar tareas de roll back	Profesional de gestión TIC y líderes funcionales	Correo electrónico
COMPONENTES DE RED	COMPONENTES DE RED	PÉRDIDA DE CONFIDENCIALIDAD	Manipulación de configuraciones por administrador de red, funcionario o contratista	Incorrecto o mal intencionado manejo de las configuraciones de red	Extracción de información confidencial o de seguridad TI Publicación de información sensible o reservada. Daño jurídico a la Entidad.	1	4	ALTO	Logs de auditoría de las consolas de administración. Asignación de roles y perfiles.	MODERADO	Realizar tareas de restauración de backup	Profesional de gestión TIC y líderes funcionales	Correo electrónico
			Mal funcionamiento parche de actualización	Error de despliegue de actualización en control de cambios.					Se genera cronograma de la ventana con backup y roll back		Realizar tareas de restauración de backup	Profesional de gestión TIC y líderes funcionales	Correo electrónico
			Agente externo o tercero que manipule la información	Intereses particulares o presión por parte de un tercero.					Se genera línea base sobre los equipos de red y seguridad.		Realizar tareas de restauración de backup	Profesional de gestión TIC y líderes funcionales	Correo electrónico
HARDWARE	EQUIPOS DE COMPUTO	PÉRDIDA DE CONFIDENCIALIDAD	Acceso no autorizado al equipo de computo	Contraseña visible, predecible o realizar la Conexión a redes, paginas o programas no seguros	Publicación de información sensible o reservada. Daño jurídico a la Entidad.	3	2	MODERADO	Asignación de usuario por directorio activo y controles de complejidad y caducidad de contraseñas. Línea base de antivirus	BAJO	Realizar la actualización de estados de usuarios en directorio activo según novedades de personal	Profesional de gestión TIC y líderes funcionales	Correo electrónico y Procedimiento TICPRO1
			Perdida o Robo del equipo de computo	Acceso a la información por parte de un tercero					Manual de seguridad de la información donde se implementa usuarios estándar y no administradores, activación e inactivación de usuarios por directorio activo		Realizar la actualización de estados de usuarios en directorio activo según novedades de personal	Profesional de gestión TIC y líderes funcionales	Correo electrónico y Procedimiento TICPRO1
SERVICIOS	BPM GESTOR DOCUMENTAL; SEVEN; KACTUS; PLATAFORMA DE PAGOS; INVESDOC	PÉRDIDA DE INTEGRIDAD	Incorrecta administración sobre la información	Ejecutar de forma incorrecta un query o alguna acción que modifique o elimine la información.	Datos incompletos o inexactos para la ciudadanía y el registro profesional. Daño Jurídico para la entidad. Información inexacta en datos sensibles o financieros. Información inexacta en los procesos misionales de la entidad	1	5	CRITICO	Logs de auditoría de las consolas de administración. Asignación de roles y perfiles. Planes de backup sobre las bases de datos	MODERADO	Realizar tareas de control de acceso, trazabilidad y roll back	Profesional de gestión TIC y líderes funcionales	Correo electrónico

MAPA DE RIESGOS DE SEGURIDAD DIGITAL



						CALIFICACIÓN DEL RIESGO			CONTROL QUE MITIGA EL RIESGO	CALIFICACIÓN DEL RESIDUAL	Versión 1 Vigente a partir de diciembre 2020		
TIPO DE ACTIVO	ACTIVO	RIESGO	AMENAZA	VULNERABILIDAD	CONSECUENCIAS	Grado de probabilidad	Grado de impacto	ZONA DE RIESGO	CONTROL ASOCIADO	NUEVA ZONA DE RIESGO	PLAN DE TRABAJO		
											ACCIONES	RESPONSABLE	REGISTROS
			Falla en funcionamiento del software o hardware	Error o intermitencia de hardware o software que genere pérdida de datos o daño en los existentes				Generación de plan de backup y contratos de mantenimiento y soporte sobre las plataformas tecnológicas		Realizar tareas de control de acceso, trazabilidad y roll back	Profesional de gestión TIC y líderes funcionales	Correo electrónico	
			Incorrecta utilización de la plataforma tecnológica	Acción por parte de un funcionario sobre la plataforma que modifique o elimine datos.				Capacitación a funcionarios. Plan de backup sobre las bases de datos		Realizar tareas de control de acceso, trazabilidad y roll back	Profesional de gestión TIC y líderes funcionales	Correo electrónico	
			Eliminación o modificación de la información por parte de un funcionario, contratista o tercero	Agente externo que logre acceder a la información o ejerza presión sobre alguien que pertenezca a la entidad y elimine o modifique la información				Generación de plan de backup y soporte sobre las plataformas tecnológicas Clausula de confidencialidad de la información, funciones del personal, restricción de acceso a terceros según manual de seguridad		Realizar tareas de control de acceso, trazabilidad y roll back	Profesional de gestión TIC y líderes funcionales	Correo electrónico	
COMPONENTES DE RED	COMPONENTES DE RED	PÉRDIDA DE INTEGRIDAD	Modificación o eliminación de configuraciones por administrador de red, funcionario o contratista	Realizar cambios en las configuraciones de seguridad de la red de la entidad	Datos incompletos o inexactos para la ciudadanía y el registro profesional Daño Jurídico para la entidad Información inexacta en datos sensibles o financieros Información inexacta en los procesos misionales de la entidad	1	4	ALTO	Logs de auditoría de las consolas de administración Asignación de roles y perfiles. Back up sobre las línea base	BAJO	Realizar tareas de control de acceso, trazabilidad y roll back	Profesional de gestión TIC y líderes funcionales	Correo electrónico
			Mal funcionamiento parche de actualización	Generar por medio de actualización la pérdida de configuraciones en la seguridad de la red de la entidad				Back up sobre la línea base		Realizar tareas de control de acceso, trazabilidad y roll back	Profesional de gestión TIC y líderes funcionales	Correo electrónico	
			Agente externo o tercero que modifique o elimine la información	Realizar cambios mal intencionados o no autorizados en las configuraciones de seguridad de la red de la entidad				Generación de plan de backup y contratos de mantenimiento y soporte sobre la infraestructura tecnológica Clausula de confidencialidad de la información, funciones del personal, restricción de acceso a terceros según manual de seguridad		Realizar tareas de control de acceso, trazabilidad y roll back	Profesional de gestión TIC y líderes funcionales	Correo electrónico	
SERVICIOS	BPM GESTOR DOCUMENTAL; SEVEN; KACTUS; PLATAFORMA DE PAGOS; INVESDOC	PÉRDIDA DE DISPONIBILIDAD	Incorrecta administración sobre la información por un usuario con privilegios en el sistema.	Generar por acciones técnicas incorrectas Indisponibilidad de la plataforma tecnológica de la entidad.	Indisponibilidad en la prestación de los servicios internos y externos de la entidad.	3	2	MODERADO	Contratos con disponibilidad de la plataforma de 99.9% Logs de auditoría de las consolas de administración Asignación de roles y perfiles.	BAJO	Realizar monitoreo diario de la disponibilidad de la plataforma tecnológica y reportar en caso de fallas.	Profesional de gestión TIC y líderes funcionales	Correo electrónico

MAPA DE RIESGOS DE SEGURIDAD DIGITAL



						CALIFICACIÓN DEL RIESGO			CONTROL QUE MITIGA EL RIESGO	CALIFICACIÓN DEL RESIDUAL	Versión 1 Vigente a partir de diciembre 2020		
TIPO DE ACTIVO	ACTIVO	RIESGO	AMENAZA	VULNERABILIDAD	CONSECUENCIAS	Grado de probabilidad	Grado de impacto	ZONA DE RIESGO	CONTROL ASOCIADO	NUEVA ZONA DE RIESGO	PLAN DE TRABAJO		
											ACCIONES	RESPONSABLE	REGISTROS
			Falla en funcionamiento del software o hardware	Falla que genere Indisponibilidad de la plataforma tecnologica de la entidad.					Contratos con disponibilidad de la plataforma de 99.9%		Realizar monitoreo diario de la disponibilidad de la plataforma tecnologica y reportar en caso de fallas.	Profesional de gestion TIC y lideres funcionales	Correo electronico
			Agente externo o tercero que afecte el servicio	Generar por acciones tecnicas incorrectas o mal intencionadas Indisponibilidad de la plataforma tecnologica de la entidad.					Contratos con disponibilidad de la plataforma de 99.9% Logs de auditoria de las consolas de administracion Asignación de roles y perfiles.		Realizar monitoreo diario de la disponibilidad de la plataforma tecnologica y reportar en caso de fallas.	Profesional de gestion TIC y lideres funcionales	Correo electronico
COMPONENTES O COMPONENTES DE RED		PÉDIDA DE DISPONIBILIDAD	Incorrecta administracion de red, por funcionario o contratista	Generar por acciones tecnicas incorrectas Indisponibilidad de la plataforma tecnologica de la entidad.	Indisponibilidad en la prestacion de los servicios internos y externos de la entidad.	3	2	MODERADO	Contratos de soporte y mantenimiento sobre la infraestructura de red Logs de auditoria de las consolas de administracion Asignación de roles y perfiles.	BAJO	Realizar monitoreo diario de la disponibilidad de la plataforma tecnologica y reportar en caso de fallas.	Profesional de gestion TIC y lideres funcionales	Correo electronico
			Falla en funcionamiento del software o hardware	Falla que genere Indisponibilidad de la plataforma tecnologica de la entidad.					Contratos de soporte y mantenimiento sobre la infraestructura de red para la ejecucion de ventanas de mantenimiento		Realizar monitoreo diario de la disponibilidad de la plataforma tecnologica y reportar en caso de fallas.	Profesional de gestion TIC y lideres funcionales	Correo electronico
			Agente externo o tercero que afecte el servicio	Generar por acciones tecnicas incorrectas o mal intencionadas Indisponibilidad de la plataforma tecnologica de la entidad.					Contratos de soporte y mantenimiento sobre la infraestructura de red Logs de auditoria de las consolas de administracion Asignación de roles y perfiles.		Realizar monitoreo diario de la disponibilidad de la plataforma tecnologica y reportar en caso de fallas.	Profesional de gestion TIC y lideres funcionales	Correo electronico

CONTROL DE CAMBIOS

VERSIÓN / FECHA	DESCRIPCIÓN
1 / DICIEMBRE 2020	Primera emisión

ELABORADO POR:  
  
**IVAN TORRES**  
 Profesional de gestión del área TIC

APROBADO POR:  
  
**GLOR MATILDE TORRES CRUZ**  
 Directora General ( E )