



ALCALDIA MUNICIPAL DE ACACÍAS


PROCESO GESTION TIC

PLAN DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DIGITAL

Fecha: 19/09/2020

Válida OFC: PL - 10

IDENTIFICACION DEL RIESGO							EVALUACION RIESGO INHERENTE						CONTROL		PROBABILIDAD	
RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/VULNERA - BIENADE	CONSECUENCIAS	PROBABILIDAD		IMPACTO		NIVEL DE RIESGO SIN CONTROLES	RIESGO INHERENTE (ZONA ACTUAL)	CONTROL		PROBABILIDAD	
							DESCRIPTOR	NIVEL	DESCRIPTOR	NIVEL			TIPO	DESCRIPCIÓN	DESCRIPTOR	NIVEL
Pérdida de la Disponibilidad	Bases de datos, información impresa	Robo y/o pérdida parcial o total de información	Pérdida de información	Seguridad digital	<ul style="list-style-type: none">Falta de conocimiento en la gestión de informaciónFalta de capacitación a los funcionarios en temas de riesgos informáticos.Exceso de confianza en la gestión de la informaciónFalta en el proceso de BackupAtaques cibernéticos internos o externosFalta de implementación de la política de escritorio limpioEquipos vulnerables de acceso (Dejar sesiones abiertas o falta de GPO para Bloqueo de sesiones automáticamente)	<ul style="list-style-type: none">Pérdida o fuga de informaciónAtaques en los procesos de la entidadIncumplimientos en la entrega de informesSanciones y pérdidas económicas	IMPROBABLE	2	MAYOR	4	8	MODERADO	PREVENTIVO	<ul style="list-style-type: none">Toma de conciencia, educación y formación en la seguridad de la informaciónInventario de activosPolítica de control de accesoPolítica sobre el uso de los servicios de redControl de acceso a sistemas y aplicacionesRestricción de acceso informaciónSistema de gestión de contraseñasPolítica de escritorio limpio y pantalla limpiaRespaldo de información	RARO	1
Pérdida de la integridad	Bases de datos, información impresa, configuración de equipos	La falta de políticas de seguridad digital, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de los sistemas de información, configuración de equipos y la información impresa	Modificación no autorizada	Seguridad digital	<ul style="list-style-type: none">Contraseñas DébilesAutenticación débilSesiones abiertas o desbloqueadasExposición de contraseñas	<ul style="list-style-type: none">Posible retraso en la recepción de pago de impuestosDañación de servicios	IMPROBABLE	2	MAYOR	4	8	MODERADO	PREVENTIVO	<ul style="list-style-type: none">Política de control de accesoPolítica sobre el uso de los servicios de redRegistro y cancelación del registro de usuariosControl de acceso a sistemas y aplicacionesRestricción de acceso informaciónSistema de gestión de contraseñasPolítica de escritorio limpio y pantalla limpiaRegistro de eventos (Bitácora de aplicaciones)Restricciones sobre la instalación de softwareAcuerdos de confidencialidad o de no divulgación	RARO	1
Pérdida de la confidencialidad	Bases de datos, información impresa	Que se comparta información valiosa o confidencial de la entidad con un tercero	Divulgación ilegal de la información	Seguridad digital	<ul style="list-style-type: none">Falta de Acuerdos de confidencialidadSesiones abiertas o desbloqueadasExceso de confianza en la gestión de la informaciónFalta de implementación de la política escritorio limpio	<ul style="list-style-type: none">Pérdida de la buena imagen de la entidadDaño a la integridad de las personas de la comunidad	IMPROBABLE	2	MODERADO	3	6	MODERADO	PREVENTIVO	<ul style="list-style-type: none">Acuerdos de confidencialidad o de no divulgaciónPolítica de control de accesoRestricción de acceso informaciónPolítica de escritorio limpio y pantalla limpiaRegistro de eventos (Bitácora de actividades)	RARO	1
Pérdida de la integridad, confidencialidad y disponibilidad	Bases de datos, información impresa, configuración de equipos	acceder de manera indebida, abusiva o sin autorización a un sistema informático, con el fin de obtener un beneficio o hacer algún tipo de daño.	Acceso no autorizado	Seguridad digital	<ul style="list-style-type: none">Contraseñas no segurasDivulgación de contraseñas	<ul style="list-style-type: none">Suaplantación de identidadCaptura de informaciónModificaciones en los sistemas de información	POSIBLE	3	MAYOR	4	12	ALTO	PREVENTIVO	<ul style="list-style-type: none">Política de control de accesoPolítica sobre el uso de los servicios de redRegistro y cancelación del registro de usuariosControl de acceso a sistemas y aplicacionesRestricción de acceso informaciónSistema de gestión de contraseñas	IMPROBABLE	2
Pérdida de la disponibilidad	Bases de datos, información impresa, configuración de equipos	Intento por dañar un sistema informático o de red, para obtener beneficios, que por lo general, es de índole económicos.	Ataques informáticos (Hacking no físico)	Seguridad digital	<ul style="list-style-type: none">Falta de FirewallFalta de Antivirus o no actualizados	<ul style="list-style-type: none">Captura de información privilegiadaCifrado de la informaciónSabotaje	RARO	1	CATASTROFICO	5	5	MODERADO	PREVENTIVO	<ul style="list-style-type: none">Controles contra códigos maliciososPolítica sobre el uso de los servicios de redRestricción de acceso informaciónRespaldo de informaciónRegistro de eventosRestricciones sobre la instalación de software	RARO	1
Pérdida de la disponibilidad	Bases de datos, información impresa, configuración de equipos	Problema en un programa informático	Error de Software	Seguridad digital	<ul style="list-style-type: none">Software no actualizadoSoftware no licenciadoFalta de mantenimiento preventivo a los equiposFalta de renovación de licencias	<ul style="list-style-type: none">Indisponibilidad del ServicioTraumatismos en los procesos	IMPROBABLE	2	MODERADO	3	6	MODERADO	PREVENTIVO	<ul style="list-style-type: none">Procedimientos de control de cambios en sistemasPruebas de seguridad de sistemasSeguimiento y revisión de los servicios de los proveedoresRestricciones sobre la instalación de software	RARO	1
Pérdida de la disponibilidad	Infraestructura TI (Servidores, Planta telefónica, Firewall, Switch, Routers, AP, NAS, etc.)	Daño en la infraestructura TI e interrupción de servicios a cargo de la Oficina TIC a causa del manejo inadecuado de equipos tecnológicos o falta de protección en el suministro de energía eléctrica	Daño o mal funcionamiento de la infraestructura TI	Seguridad digital	<ul style="list-style-type: none">Falta de Respaldo de energía (UPS - Planta eléctrica)Malas manipulaciones en las configuraciones de los equiposFalta de procedimientos para la gestión de la infraestructura TI	<ul style="list-style-type: none">Daño en los equipos de la infraestructura TI.Daño configuración de equiposIndisponibilidad de insumos y servicios ofrecidos por la entidad.	POSIBLE	3	MEJOR	2	6	MODERADO	PREVENTIVO	<ul style="list-style-type: none">Protección contra amenazas externas y ambientalesSeguridad del cableadoMantenimiento de equiposProcedimientos de operación documentadosGestión de cambiosGestión de las vulnerabilidades técnicasPlanificación de la continuidad de la seguridad de la informaciónImplementación de la continuidad de la seguridad de la información	IMPROBABLE	2
Pérdida de la disponibilidad	Infraestructura TI (Servidores, Planta telefónica, Firewall, Switch, Routers, AP, NAS, etc.)	Robo y/o pérdida de algún elemento que haga parte de la infraestructura TI de la entidad	Robo de la infraestructura TI	Seguridad digital	<ul style="list-style-type: none">Falta de control de acceso al cuarto equipos	<ul style="list-style-type: none">Indisponibilidad de insumos y servicios ofrecidos por la entidad.Ataques en los procesos de la entidad	RARO	1	CATASTROFICO	4	4	MODERADO	PREVENTIVO	<ul style="list-style-type: none">Perímetro de seguridad físicaProtección contra amenazas externas y ambientales	RARO	1
Pérdida de la disponibilidad	Cuarto de equipos (Data center) y ancho físico de la entidad	Daño o pérdida de información física y digital, así como la afectación de dispositivos de red	Daños estructurales en cuarto de equipos (Data Center) y botijos de archivo	Seguridad digital	<ul style="list-style-type: none">Uso inadecuado o descuido del control de acceso físico a las aplicaciones.Ubicaciones susceptibles de inundacionesRed Eléctrica inestable	<ul style="list-style-type: none">Huerto de dispositivos o documentosUso no autorizado de Dispositivos y documentos	RARO	1	CATASTROFICO	4	4	MODERADO	PREVENTIVO	<ul style="list-style-type: none">Perímetro de seguridad físicaProtección contra amenazas externas y ambientales	RARO	1

											 GOBIERNO DE CHIRIQUÍ SECRETARÍA DE SEGURIDAD Y DEFENSA CALLE 100 N° 1001 CARRERA 100 N° 1001 CARRERA 100 N° 1001	
											Versión 3	
EVALUACION RIESGO RESIDUAL			PLAN DE MANEJO DEL RIESGO									
IMPACTO		NIVEL DE RIESGO SIN CONTROLES	RIESGO RESIDUAL (NUEVA ZONA)	OPCIONES DE MANEJO	ACCIONES	RESPONSABLE	PERIODO DE SEGUIMIENTO	FECHA INICIO	FECHA TERMINACIÓN	REGISTRO EVIDENCIA	OBSERVACIONES	
DESCRIPCIÓN	NIVEL											
Menor	2	2	Bajo	ASUMIR EL RIESGO	<ul style="list-style-type: none">Apropiación de la Política de seguridad de la informaciónGPO Inicio de sesiónGPO BitLocker de la sesiónActualización del GTC - PD - 14 Procedimiento de Gestión y Contratación.	Oficina de Tecnologías de la Información y las Telecomunicaciones	Semanal	1/11/2019		<ul style="list-style-type: none">GPO configuradas en el servidor de dominio.Plantilla de asistencia		
Insuficiente	1	1	Bajo	ASUMIR EL RIESGO	<ul style="list-style-type: none">GPO Contraseñas SegurasAplicación del GTC - PD - 10 Procedimiento Backup.GPO de contraseñas seguras	Oficina de Tecnologías de la Información y las Telecomunicaciones	Semanal	1/11/2019		<ul style="list-style-type: none">GPO configuradas en el servidor de dominio.		
Menor	2	2	Bajo	ASUMIR EL RIESGO	<ul style="list-style-type: none">Firma del GTC - F - 26 Solicitud creación o modificación de cuentas de usuariosApropiación de la Política de seguridad de la información	Oficina de Tecnologías de la Información y las Telecomunicaciones	Semanal	1/11/2019		<ul style="list-style-type: none">GTC - F - 26 Solicitud creación o modificación de cuentas de usuarios.Plantilla de asistencia		
Modificado	3	6	Modificado	ASUMIR EL RIESGO, REDUCIR EL RIESGO	<ul style="list-style-type: none">Equipos registrados en el Dominio con las respectivas GPO.Apropiación de la Política de seguridad de la información.	Oficina de Tecnologías de la Información y las Telecomunicaciones	Semanal	1/11/2019		<ul style="list-style-type: none">GPO configuradas en el servidor de dominio.Plantilla de asistencia		
Modificado	3	3	Bajo	ASUMIR EL RIESGO	<ul style="list-style-type: none">GTC - F - 23 BitLocker Backup.GTC - F - 24 Formato Congratina de BackupProtección de equipos mediante Antivirus y Firewall.	Oficina de Tecnologías de la Información y las Telecomunicaciones	Semanal	1/11/2019		<ul style="list-style-type: none">GTC - F - 23 BitLocker Backup.Escaneo de Antivirus y Firewall actualizados.		
Modificado	3	3	Bajo	ASUMIR EL RIESGO	<ul style="list-style-type: none">Ejecución del plan de mantenimiento preventivo de equipos.Instalación de Software licenciado con sus últimas versiones.GPO para la restricción de instalación de software.	Oficina de Tecnologías de la Información y las Telecomunicaciones	Semanal	1/11/2019		<ul style="list-style-type: none">Plataforma GLPI		
Insuficiente	1	2	Bajo	ASUMIR EL RIESGO	<ul style="list-style-type: none">GTC - PL - 01 Plan de Renovación Tecnológica.Los equipos deberán estar conectados a la red regulada a una UPS.	Oficina de Tecnologías de la Información y las Telecomunicaciones	Semanal	1/11/2019				
Modificado	3	3	Bajo	ASUMIR EL RIESGO	<ul style="list-style-type: none">Diligenciar GTC - F - 08 Reporte ingreso para servicio mantenimiento a cuarto de comunicaciones.	Oficina de Tecnologías de la Información y las Telecomunicaciones	Semanal	1/11/2019		<ul style="list-style-type: none">GTC - F - 08 Reporte ingreso para servicio mantenimiento a cuarto de comunicaciones		
Modificado	3	3	Bajo	ASUMIR EL RIESGO	<ul style="list-style-type: none">Mantenimiento localativo preventivo.Asesoramiento de las medidas ambientales adecuadas.	Secretaría Administrativa y Financiera	Semanal	1/11/2019		<ul style="list-style-type: none">GTC - F - 08 Reporte ingreso para servicio mantenimiento a cuarto de comunicaciones		