





	<b>PROTOCOLO DE SEGURIDAD INFORMÁTICA</b>	Código: GADPRC-TIC-IN-03	
		Dominio: USO INTERNO	
		Fecha primera versión: 02/10/2024	
		Versión: 1.0	Página 3 de 17

## CONTENIDO

1.	Glosario de Términos.....	4
2.	Aspectos Generales .....	4
1.1.	Introducción.....	4
1.2.	Base Legal .....	4
1.3.	Objetivos del protocolo .....	9
1.4.	Alcance .....	9
1.5.	Revisión y Actualización .....	10
1.6.	Cumplimiento .....	10
3.	Roles y normativa de responsabilidades .....	10
2.1.	Rol: Usuario – funcionario/a, autoridad, personal .....	10
2.2.	Rol: Unidad Administrativa - Tecnología y Sistemas de la Información .....	10
2.3.	Rol: Unidad Administrativa - Talento Humano .....	11
2.4.	Rol: Unidad de Asesorías - Comunicación.....	11
2.5.	Rol: Unidad de Secretaría -Secretaría General .....	11
4.	Protocolo para seguridad informática .....	12
4.1.	Proceso protección de credenciales – cuentas de usuarios .....	12
4.2.	Proceso de cuidado dispositivos – Computador .....	12
4.3.	Proceso navegar en la Web – Uso de internet .....	13
4.4.	Proceso de mitigación – Potenciales amenazas encontradas -correo.....	14
4.5.	Proceso de creación y manejo de cuentas.....	14
4.6.	Proceso correctivo en caso de ataque o pérdidas.....	15
4.7.	Proceso uso WIFI – compartir contraseñas .....	16
5.	Anexos .....	17

	<b>PROTOCOLO DE SEGURIDAD INFORMÁTICA</b>	Código: GADPRC-TIC-IN-03	
		Dominio: USO INTERNO	
		Fecha primera versión: 02/10/2024	
		Versión: 1.0	Página 4 de 17

## 1. Glosario de Términos

- i. **APLICATIVOS:** Nombre que reciben los programas especializados en tareas concretas y de una cierta complejidad.
- ii. **SIGAME:** Sistema de gestión interna de la Asociación de Municipalidades Ecuatorianas.
- iii. **GTR:** Sistema interno de gestión, Gestor de Tiempo y Recursos.
- iv. **QUIPUX:** Sistema de documentación gobierno central.
- v. **SITRA:** Sistema de tramites de gestión documental del Municipio de Quito.
- vi. **USUARIO:** Hace referencia cualquier persona que utilice cuentas, plataformas o servicios relacionados con la institución.
- vii. **TICS:** referencia al área de tecnologías y sistemas de información.

## 2. Aspectos Generales

### 1.1. Introducción

El presente instructivo pretende dar lineamientos que permitan poner en ejecución las políticas y procedimientos relacionados al manejo y resguardo de la información generada por las diferentes instancias del Gobierno Autónomo Descentralizado Parroquial Rural de Conocoto, con el fin de mantener la integridad y disponibilidad de la información.

Conforme el Estatuto de Gestión Organizacional por Procesos del GAD Parroquial de Conocoto para el periodo 2023-2024 de fecha 19 de mayo del 2023, es necesario especificar mediante este instrumento las facultades de cada área de manera que permitan mejorar los procesos en lo correspondiente al manejo de las tecnologías.

### 1.2. Base Legal

#### CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR

*Que, el artículo 3.- Son deberes primordiales del Estado:*

*8. Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción.*

*Que, el artículo 66.- Se reconoce y garantiza a las personas: (...)*

*19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la 5 autorización del titular o el mandato de la ley. (...)*

*21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación;*

*Que, el artículo 225.- El sector público comprende:*

*1. Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral y de Transparencia y Control Social.*

2. Las entidades que integran el régimen autónomo descentralizado.
3. Los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado.
4. Las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados para la prestación de servicios públicos.

## LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPD)

**Que, art. 35.-**Acceso a datos personales por parte de terceros. -No se considerará transferencia o comunicación cuando el acceso a datos personales por un tercero sea necesario para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido a datos personales en estas condiciones debió hacerlo legítimamente.

**Que, Art. 37.-**Seguridad de datos personales. -El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos

Entre otras medidas, se podrán incluir las siguientes;

- 1) Medidas de anonimización, seudonomización o cifrado de datos personales;
- 2) Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y
- 3) Medidas dirigidas a mejorar la residencia técnica, física, administrativa, y jurídica.
- 4) Los responsables y encargados del tratamiento de datos personales podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales.

**Que, Art. 38.-**Medidas de seguridad en el ámbito del sector público. -El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales.

El mecanismo gubernamental de seguridad de la información abarcará y aplicará a todas las instituciones del sector público, contenidas en el artículo 225 de la Constitución de la República de Ecuador, así como a terceros que presten servicios públicos mediante concesión u otras figuras legalmente reconocidas. Estas, podrán incorporar medidas adicionales al mecanismo gubernamental de seguridad de la información.

## NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y DE LAS PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS DE LA CONTRALORÍA GENERAL DEL ESTADO (CGE)

**Que, “410-10** Mantenimiento, actualización y control de la infraestructura tecnológica

La unidad de tecnologías de la información y comunicaciones de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades.

Los temas a considerar son:

1. Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios.
2. Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones serán registrados en su correspondiente bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.
3. Control y registro de las versiones del software que ingresa a producción.
4. Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.
5. Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementarán medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.
6. Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.
7. Se mantendrá el control de los activos informáticos a través de un inventario actualizado con el detalle de las características y valoración de la criticidad de los activos, así como también la asignación de responsables a cargo, conciliado con los registros contables.
8. El mantenimiento de los bienes que se encuentren en garantía será proporcionado por el proveedor, sin costo adicional para la entidad.

#### **Que, 410-11 Seguridad de tecnología de información**

La unidad de tecnologías de la información y comunicaciones debe garantizar el cumplimiento de la normativa de protección de datos personales, propiedad intelectual del software, seguridad de la información, utilización de estándares, sistemas o plataformas establecidas para el sector público, y estarán alineadas a los objetivos de la organización, a los principios de calidad de servicio, y constarán en el plan informático y en el plan anual de contrataciones aprobado de la institución. Las excepciones serán al acceso a la información pública, así como de las demás normas que resulten aplicables. Las entidades de la administración pública implementarán una política de seguridad de la información sobre la base de las disposiciones legales y reglamentarias vigentes.

#### **Que, 410-12 Plan de contingencias**

Corresponde a la unidad de tecnologías de la información y comunicaciones la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

Los aspectos a considerar son:

1. Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento.
2. Definición y ejecución de procedimientos de control de cambios, para asegurar que el plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización.
3. Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alternativo propio o de uso compartido en un data center estatal mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.
4. Plan de recuperación de desastres que comprenderá:

- Actividades previas al desastre (bitácora de operaciones).
- Actividades durante el desastre (plan de emergencias, entrenamiento).
- Actividades después del desastre.

5. Es indispensable designar un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia.

6. El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.

7. El plan de contingencias aprobado será difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas, o cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento.

## ACUERDOS MINISTERIALES

**Que, mediante Acuerdo Ministerial No. 15-2019**, del 18 de julio del 2019, se expide la Política Ecuador Digital cuyo objeto es transformar al país hacia una economía basada en tecnologías digitales, mediante la disminución de la brecha digital, el desarrollo de la Sociedad de la Información y del Conocimiento, el Gobierno Digital, la eficiencia de la administración pública y la adopción digital en los sectores sociales y económicos;

**Que, en Acuerdo Ministerial No. 006-2021** de Política de Ciberseguridad establece que el Plan Específico de Defensa Nacional 2019-2030 reconoce al ciberespacio como un competente más del territorio ecuatoriano. Las Implicaciones se vinculan al desarrollo de operaciones en este dominio para la defensa de la soberanía, con el fin de aportar a la ciberseguridad nacional.

## CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP)

**Que, el artículo 178.- Violación a la intimidad.** - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley;

**Que, el artículo 190.- Apropiación fraudulenta por medios electrónicos.-** La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes;

**Que, el artículo 229.- Revelación ilegal de base de datos.** - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o

	<b>PROTOCOLO DE SEGURIDAD INFORMÁTICA</b>	Código: GADPRC-TIC-IN-03	
		Dominio: USO INTERNO	
		Fecha primera versión: 02/10/2024	
		Versión: 1.0	Página 8 de 17

de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años;

**Que, el artículo 230.- Intercepción ilegal de datos.** - Será sancionado con pena privativa de libertad de tres a cinco años: 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. 3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior;

**Que, el artículo 232.- Ataque a la integridad de sistemas informáticos.** - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que: 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad;

**Que, el artículo 233.- Delitos contra la información pública reservada legalmente.** - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad;

**Que, el artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.** -

1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años.

2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

## LEY ORGÁNICA DE TELECOMUNICACIONES

**Que, el artículo 79.- Deber de información.** - en caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de telecomunicaciones, el prestador de servicios de telecomunicaciones deberá informar a sus abonados, clientes y usuarios sobre dicho riesgo y sobre las medidas a adoptar;

	<b>PROTOCOLO DE SEGURIDAD INFORMÁTICA</b>	Código: GADPRC-TIC-IN-03	
		Dominio: USO INTERNO	
		Fecha primera versión: 02/10/2024	
		Versión: 1.0	Página 9 de 17

## DE LEY ORGÁNICA DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

**Artículo 5.- Confidencialidad y reserva.** - Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia;

**Artículo 7.- Información original.** - Cuando la ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la ley, puede comprobarse que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos;

**Artículo 8.- De la conservación de los mensajes de datos.** - Toda información sometida a esta ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos y de acuerdo con varias condiciones;

**Artículo 9.- Protección de datos.** - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros;

**Artículo 10.- Procedencia e identidad de un mensaje de datos.** - Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica;

## CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN

**Artículo 140.- Materia protegible por las bases de datos.** - Las compilaciones de datos o de otros materiales, en cualquier forma, que por razones de la originalidad de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, están protegidas como tales. Esta protección de una base de datos, según el presente Título, no se extiende a los datos o información recopilada, pero no afectará los derechos que pudieren subsistir sobre las obras o prestaciones protegidas por derechos de autor o derechos conexos que la conforman.

### 1.3. Objetivos del protocolo

- i. Garantizar la disponibilidad, integridad y confidencialidad de la información Institucional, mediante la puesta en marcha de las recomendaciones y obligaciones de seguridad informática planteadas en este texto.
- ii. Regular el monitoreo de puntos críticos de vulnerabilidad de la seguridad de la información como servicios, plataformas, cuentas, dispositivos, y respaldos.
- iii. Crear acciones preventivas de seguridad y de respuesta en caso de vulneración de la seguridad que atente con la integridad de los datos.

### 1.4. Alcance

El presente documento tiene por objeto definir responsables y acciones para la obtención de los backups o respaldos de la información propiedad de la GADPRC y que se encuentran en los equipos de cómputo institucionales (computadores personales de escritorio y portátiles), así como en los servidores físicos y virtuales. La información para respaldar

	<b>PROTOCOLO DE SEGURIDAD INFORMÁTICA</b>	Código: GADPRC-TIC-IN-03	
		Dominio: USO INTERNO	
		Fecha primera versión: 02/10/2024	
		Versión: 1.0	Página 10 de 17

incluye aplicativos, bases de datos, documentos e información inherente a las actividades del GADPRC que se encuentre contenida en los computadores o dispositivos tecnológicos de dominio público.

### 1.5. Revisión y Actualización

El presente instructivo, deberá ser revisado anualmente, por necesidad institucional o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológico, económico, entre otros. El instructivo deberá ser presentado en junta o reunión con las autoridades o áreas que cumplen roles de usuario.

### 1.6. Cumplimiento

Con el fin de asegurar el pleno cumplimiento de sus responsabilidades, el cumplimiento del protocolo se extiende a todos los funcionarios, personas y autoridades del Gobierno Autónomo Descentralizado de Conocoto trabajan en beneficio de los ciudadanos a quienes tienen el honor de servir, usando bienes tecnológicos de dominio público.

## 3. Roles y normativa de responsabilidades

### 2.1. Rol: Usuario – funcionario/a, autoridad, personal

**Definición:** Todo funcionario del GADPRC que genera y procesa información propia o externa.

**Responsabilidades generales:**

- Cumplir a cabalidad los protocolos aprobados por la máxima autoridad para las seguridad y buena gestión dentro de la institución.
- Hacer un uso adecuado de la tecnología con los bienes relacionados como computadores.
- Hacer uso adecuado del internet, evitando navegar en sitios de dudosa procedencia.
- Descargar archivos del internet que sean verificados y de procedencia segura.
- Notificar de daños, mal funcionamiento, o actividades extrañas relativas a tecnologías.
- Hacer uso exclusivamente personal de las credenciales asignadas por TICs.
- Cuidar bien de las credenciales asignadas por TICs.
- Notificar a TTHH o TICs en caso de observar o comprobar comportamientos no profesionales relacionados con tecnologías.
- Hacer un uso adecuado de la información, la misma que deberá estar ordenada y clasificada en su computador.
- Firmar acuerdo de confidencialidad para manejo de información cualquiera que sea el cargo.
- Delegar conforme a la ley en caso de que así se requiera la autorización del titular para el uso y custodia de la firma electrónica.
- Firmar acuerdo de responsabilidad de uso, en caso de que utilice una firma electrónica de otro funcionario.
- Seguir las normas establecidas en los protocolos, normas o resoluciones relacionadas con al área de tecnología.
- Notificar daños o averías en el computador o dispositivo tecnológico asignado.
- Notificar de comportamientos extraños en los sistemas, plataformas o recursos con los que tenga interacción.

### 2.2. Rol: Unidad Administrativa - Tecnología y Sistemas de la Información

**Responsabilidades generales:**

- Revisión de los protocolos y procesos de obtención de los respaldos de la información.

- Llevar a cabo el acompañamiento con los funcionarios que se incorporan para la instalación de la firma electrónica.
- Llevar a cabo el acompañamiento con los funcionarios que terminan su relación laboral para la desinstalación de la firma electrónica.
- Otorgarle y respaldarse de una constancia a los funcionarios que terminan su relación laboral de la respectiva desinstalación de la firma electrónica.
- Aprobación de revisión de los protocolos y procesos de obtención de los respaldos de la información.
- Funcionario de la institución encargado de ejecutar los protocolos y procesos para obtener los respaldos de la información.
- Realizar la obtención de los respaldos de la información contenida en los equipos de cómputo de los demás funcionarios, de forma periódica o en situaciones especiales exigidas por la institución.
- Garantizar que los respaldos sean copiados y almacenados al área de secretaría.
- Proporcionar a los funcionarios solicitantes una copia de los respaldos de acuerdo con el requerimiento debidamente justificado y apegado a la normativa vigente.
- Funcionario de la institución encargado de generar protocolos y procesos para la obtención de los respaldos de información.
- Revisar y validar los respaldos de información obtenidos y copiados en el equipo destinado para el proceso de backup.
- Revisión y análisis de vulnerabilidades informáticas en la institución.
- Capacitación continua sobre educación tecnológica en el ámbito de seguridad informática.
- Prevención y mitigación de vulnerabilidades.
- Asistencia y ejecución de acciones en caso de ataques, robos o vulneraciones de seguridad.

### **2.3. Rol: Unidad Administrativa - Talento Humano**

**Definición:** funcionarios o funcionario que pertenezca a la unidad de Talento o Recursos Humanos.

**Responsabilidades generales:**

- Notificar a TICs sobre ingresos de personal para la creación de credenciales.
- Notificar a TICs sobre egresos de personal para la revocación de credenciales.
- Notificar a TICs sobre cambios de personal para la actualización de credenciales.
- Notificar al usuario un llamado de atención en caso de que se compruebe actividades o comportamientos peligrosos para la seguridad informática de la institución.

### **2.4. Rol: Unidad de Asesorías - Comunicación**

**Definición:** funcionarios o funcionario que pertenezca a la unidad de comunicación.

- Unidad de Comunicación Institucional hace referencia al funcionario o funcionarios del área de comunicación.
- Realizar la difusión de los protocolos de uso interno como comunicación interna promoviendo las buenas prácticas del Gobierno Autónomo Descentralizado Parroquial Rural de Conocoto, como se indica en el Estatuto Orgánico.

### **2.5. Rol: Unidad de Secretaría -Secretaría General**

**Definición:** funcionario o funcionario que pertenezca a la unidad de secretaría.

- Mantener el archivo institucional del trabajo de los funcionarios como respaldos realizados por el área de TICs.

	<b>PROTOCOLO DE SEGURIDAD INFORMÁTICA</b>	Código: GADPRC-TIC-IN-03	
		Dominio: USO INTERNO	
		Fecha primera versión: 02/10/2024	
		Versión: 1.0	Página 12 de 17

- Proteger la integridad de los datos almacenándolos en un lugar indicado.

## 4. Protocolo para seguridad informática

Detalle de las actividades a seguir en cada proceso, para la gestión de respaldos de información.

### 4.1. Proceso protección de credenciales – cuentas de usuarios

Los usuarios funcionarios, autoridades o personal que trabaja de una u otra forma en la institución se le entrega credenciales para el uso de los servicios, cuentas o plataformas, estas credenciales deben ser renovadas cada cierto tiempo y es de responsabilidad del usuario cuidar la privacidad de esta, sin compartirla, sin utilizar la misma en diferentes cuentas, de ocultarla. Se recuerda que el eslabón más débil en la cadena de seguridad informática es el usuario.

Nro.	Actividad	Responsable	Descripción
1	Solicitud de credenciales	TTHH / Usuario	Talento humano deberá solicitar las credenciales para las cuentas existentes para los usuarios nuevos, o a su vez el usuario puede solicitar a TICS nuevas credenciales. TTHH deberá proporcionar datos básicos como, cedula, correo personal, si es firma electrónica token o archivo, fecha de nacimiento, teléfono celular y dirección.
2	Entrega de credenciales	TICS	El área de TICS entrega credenciales al usuario final mediante una hoja impresa para los usuarios nuevos, o mediante otros medios a los usuarios antiguos. <i>Anexo I</i>
3	Cambio de contraseña	Usuario	Una vez recibidas las credenciales el usuario deberá cambiar su contraseña a una que cumple los siguientes criterios: <ul style="list-style-type: none"> <li>• Mínimo 8 caracteres.</li> <li>• Mínimo una letra mayúscula.</li> <li>• Mínimo un carácter especial (;,@,.\$,&amp;.,?!,)</li> <li>• No utilizar la misma contraseña de otra cuenta.</li> </ul>
4	Protección de las credenciales	Usuario	Una vez establecida la contraseña personal, deberá guardarla en un lugar seguro como un gestor de contraseñas que tenga doble autenticación. <ul style="list-style-type: none"> <li>• Utilizar gestor de contraseñas para almacenarla.</li> </ul>
5	Renovación de credenciales	TICS	Cada tres meses como periodo máximo, el área de tecnologías deberá realizar el cambio de contraseñas para correo institucional en Zimbra. De igual forma deberá sugerir el cambio de contraseñas de otras cuentas como: SITRA, QUIPUX, SIGAME, GTR, Windows.

### 4.2. Proceso de cuidado dispositivos – Computador

El respaldo de la información contenida en los equipos de cómputo personales de los funcionarios salientes se realizará según lo establecido.

Nro.	Actividad	Responsable	Descripción
1	Asignación	TICS	Una vez entregados los bienes a cada usuario es el departamento de TICS se encargará de entregar las credenciales para su uso, una cuenta de usuario.

	<b>PROTOCOLO DE SEGURIDAD INFORMÁTICA</b>	Código: GADPRC-TIC-IN-03	
		Dominio: USO INTERNO	
		Fecha primera versión: 02/10/2024	
		Versión: 1.0	Página 13 de 17

2	Protección física	Usuario	<p>Como custodio del bien asignado es responsabilidad el usuario cuidar del mismo, para lo cual se sugiere lo siguiente:</p> <ul style="list-style-type: none"> <li>• Examinar con el antivirus cualquier memoria USB antes de utilizar la información del dispositivo de memoria.</li> <li>• Desconectar el dispositivo de la corriente en caso de tormenta eléctrica.</li> <li>• No desconectar de forma imprevista al apagar, hacerlo desde el sistema operativo.</li> </ul>
3	Protección cuenta	Usuario	<p>Es preciso realizar las siguientes acciones para cuidar su información del dispositivo. Para ello lo mas importante es no dejar su sesión abierta.</p> <ul style="list-style-type: none"> <li>• No dejar abierta la sesión cuando no este ocupando o deje el puesto de trabajo. Bloquear la sesión en Windows con: Teclas: WIN + L</li> </ul>
4	Supervisión	Seguridad / TTHH / TICS / Usuario	<p>A modo de control cualquier área será encargada de notificar el mal uso a TTHH, para emitir la recomendación respectiva del buen uso de los dispositivos en la institución, de las credenciales, y de la responsabilidad de navegar en internet.</p>

### 4.3. Proceso navegar en la Web – Uso de internet

Se respaldará la información de los equipos reportados como dañados o que sean actualizados requiriendo un proceso de formateo del sistema operativo, para evitar pérdida de información.

Nro.	Actividad	Responsable	Descripción
1	Escoger navegador	Usuario	<p>El usuario deberá escoger que navegador usar y para qué tipo de actividades. Se recomienda usar Google Chrome, debido a la conexión directa con las cuentas de Gmail, las mismas que se pueden configurar con doble factor de autenticación ayudando a mejorar la seguridad.</p>
2	Navegación en internet	Usuario	<p>Se establecen ciertos parámetros o comportamientos en actividades relacionadas con el uso de internet para mejorar la seguridad:</p> <ul style="list-style-type: none"> <li>• Si tiene antivirus, habilitar la extensión para navegador</li> <li>• No entrar en páginas sospechosas, es decir, con nombres extraños, con caracteres extraños.</li> <li>• Evitar presionar o dar clic en ventanas emergentes de propagandas o publicidad,</li> <li>• Evitar descargar archivos de dudosa procedencia.</li> </ul>
3	Uso de correo	Usuario	<p>Se establecen normas para uso de correo, las mismas que pueden ayudar a mitigar potenciales peligros:</p> <ul style="list-style-type: none"> <li>• No dar clic en los enlaces de correos que sean desconocidos o parezcan sospechosos.</li> <li>• No dar información de sus credenciales a ninguna página, persona o plataforma a menos que sea de fuente fidedigna.</li> <li>• Evitar reenviar cadenas de correos, ni aceptarlos, enviarlos a spam.</li> <li>• Reportar cualquier error, peligro o duda de amenaza al área de TICS.</li> </ul>

	<b>PROTOCOLO DE SEGURIDAD INFORMÁTICA</b>	Código: GADPRC-TIC-IN-03	
		Dominio: USO INTERNO	
		Fecha primera versión: 02/10/2024	
		Versión: 1.0	Página 14 de 17

#### 4.4. Proceso de mitigación – Potenciales amenazas encontradas -correo

Debido a que el correo electrónico es uno de los medios de uso externo, que sirve para comunicarse con entidades externas de otras instituciones de índole público o privado, se establecen pasos básicos de prevención en caso de recibir correos malintencionados. Hay que tener en cuenta que al ser una institución pública y como estos están al alcance de cualquier persona o grupo, las instituciones públicas son más propensas a estar en listas de ataques.

Nro.	Actividad	Responsable	Descripción
1	Encuentra posible amenaza	Usuario	Una vez que el usuario encuentre una amenaza deberá reportar al área de TICS
2	Notificación de amenaza	TICS	Una vez que TICS reciba la notificación de amenaza, deberá realizar las siguientes acciones: <ul style="list-style-type: none"> <li>• Obtener los datos de la posible amenaza, dirección de correo, y dirección de enlace.</li> <li>• Notificar a entidad que administra firewall, apuntadores DNS, de los correos recibidos, solicitando el bloqueo de las direcciones.</li> <li>• Emitir una notificación por GTR, o grupo de WhatsApp indicando el reporte de amenaza y solicitando tener cuidado.</li> </ul>
3	Informe mensual	TICS	Se deberá crear un reporte mensual sobre las amenazas detectadas y mitigadas

#### 4.5. Proceso de creación y manejo de cuentas

El área de TICs al implementar diferentes niveles de seguridad para las cuentas asociadas a las actividades de la institución es preciso establecer pasos a seguir como los que se muestran a continuación, los pasos pueden ser secuenciales y en caso de que las cuentas ya estén creadas puede tomar los mismos después de la creación.

Nro.	Actividad	Responsable	Descripción
1	Creación de cuentas	TICS	Creación de cuentas de diversos indoes para la gestión de actividades institucionales: <ul style="list-style-type: none"> <li>• Correo institucional: admin Zimbra</li> <li>• Correos alternativos: servicio Google con Gmail</li> <li>• Licencias ofimáticas: Windows Office 365</li> <li>• Redes sociales: Comunicación (IG,FB,TW, otros)</li> <li>• Métodos remotos de conexión: Rust Desk, Any Desk</li> <li>• Gestión interna: SIGAME, GTR</li> <li>• Datos de biométrico: ZKteco</li> <li>• Datos video vigilancia interna: Hikevision</li> <li>• Sistema operativo Windows: admin password</li> <li>• Dispositivo de autenticación: Yubico</li> <li>• Página web: wordpress – Cpanel</li> <li>• Antivirus: plataforma gestión licencias</li> <li>• Rastreo satelital: Omnilogik</li> <li>• Routers: routers principales de servicio</li> <li>• Accesos internet: DECO Wifi</li> <li>• Dispositivos impresión: configuración</li> </ul>

2	Asignación de contraseñas	TICS	<p>Las contraseñas creadas para las cuentas, plataformas, servicios, dispositivos u otros que tengan índole de administración o que se utilicen para configurar deberán tener los siguientes aspectos.</p> <ul style="list-style-type: none"> <li>• Cantidad de caracteres mínimos: 12</li> <li>• Cantidad de mayúsculas mínimas: 1</li> <li>• Cantidad de caracteres especiales mínimo: 3</li> <li>• No usar palabras</li> <li>• De sugerencia utilizar claves aleatorias</li> <li>• Usar siempre doble factor de autenticación</li> <li>• Utilizar método de validación con Yubikey</li> </ul>
3	Cambio de contraseña	TICS	<p>Se establece periodicidad de cambio de contraseña para todas las cuentas administrativas de <i>3 meses máximo</i>, las cuales no deben ser parecidas a las anteriores.</p>

#### 4.6. Proceso correctivo en caso de ataque o perdidas.

Nro.	Actividad	Responsable	Descripción
1	Detección de ataque	Usuario / TICS	Una vez que se verifique que se haya sido victima de ataque de cualquier índole, notificar a TICS.
2	Acciones correctivas	TICS	<p>Una vez recibida la notificación de ataque o perdida se deberán tomar las siguientes acciones:</p> <ul style="list-style-type: none"> <li>• En caso de secuestro de credenciales: desde el área administrativa del servicio, bloquear y cambiar contraseñas.</li> <li>• En caso de creadores de spam: notificar a administradores de firewall de red y apuntadores para desbloqueo.</li> <li>• En caso de pérdida: restablecer el ultimo respaldo.</li> <li>• En caso de posible o confirmada infección: formateo de máquina.</li> <li>• Cambio de contraseñas en todas las cuentas del usuario, si se corrompe una es posible que otras se hayan corrompido.</li> </ul>
3	Informe de evento	TICS	<ul style="list-style-type: none"> <li>• Se deberá crear un reporte de lo sucedido, indicando posibles causas del evento, si es de conclusión determinante mejor.</li> <li>• Notificar a TTHH en caso de que sea falla del usuario.</li> <li>• Notificar de ataque y perdidas al equipo mediante correo u otro medio oficial para prevención, si uno fue atacado es posible que otro este en camino, este siendo atacado o ya haya sido vulnerado.</li> </ul>
4	Notificar	TTHH	Al ser un acto de descuido que representa una ventada de vulnerabilidad para todos los usuarios es preciso que TTHH realice una notificación con copia a la máxima autoridad haciendo un llamado de atención, indicando que debe tener mas cuidado y responsabilidad de sus credenciales e información.

#### 4.7. Proceso uso WIFI – compartir contraseñas

Nro.	Actividad	Responsable	Descripción
1	Creación de claves y perfiles	TICS	<p>TICS deberá crear dos redes, una para los funcionarios y otra para los visitantes o externos, con las siguientes características:</p> <ul style="list-style-type: none"> <li>• Red interna: red oculta con ssid oculto.</li> <li>• Deberá compartir esta red mediante QR, en lugar donde solo puedan acceder los funcionarios o personal interno.</li> <li>• Red externa: red publica</li> <li>• Deberá compartir credenciales mediante QR, en lugar de uso público, y establecer una clave fácil de recordar para uso de computadores.</li> </ul>
2	Uso de credenciales	Usuarios	<p>Los usuarios tendrán las siguientes responsabilidades:</p> <ul style="list-style-type: none"> <li>• No compartir las credenciales de conexión inalámbrica con usuarios exteriores a la institución.</li> <li>• Mencionar a los que deseen servicio de internet que existe una red pública para conexión a internet.</li> </ul>

	<b>PROTOCOLO DE SEGURIDAD INFORMÁTICA</b>	Código: GADPRC-TIC-IN-03	
		Dominio: USO INTERNO	
		Fecha primera versión: 02/10/2024	
		Versión: 1.0	Página 17 de 17

## 5. Anexos

*Ejemplo de hoja de entrega de credenciales:*

	PROCESOS DE CREACIÓN, OTORGAMIENTO Y REVOCACIÓN DE CREDENCIALES		Código: GADPRC-TIC-IN-02	
			Dominio: USO INTERNO	
			Fecha actual:: 02/01/2024	
			Versión: 1.0	Página 1
<b>RECEPCIÓN DE CREDENCIALES</b>				
Se obtienen los datos básicos del funcionario entrante, a quien se otorgará y revocará las credenciales.				
<b>NOMBRES COMPLETOS:</b>	Alexander Regist	<b>CEDULA:</b>	010TTTTTTT0533	
<b>CARGO:</b>	JEFE DE OBRAS PUBLICAS	<b>TELÉFONO:</b>	593RREDFSF5	
<b>CORREO PERSONAL:</b>	alsddsderazi@asddsil.com	<b>SECTOR DOMICILIO:</b>	Casdrresf	
<b>CORREO INSTITUCIONAL</b>				
Correo que permite enviar y recibir información, puede cambiar la contraseña cuando desee.				
<b>CORREO:</b>	aesdsddsdo@gadconocoto.gob.ec	<b>CONTRASEÑA</b>	sdsddD9Wymz1!	
<b>SISTEMA INTERNO APP</b>				
Sistema para gestión interna y proceso de datos abiertos por cada área				
<b>CORREO:</b>	obsdsdsdao@gsdsdmail.com	<b>CONTRASEÑA:</b>	Osdsdasd3434	
<b>USUARIO:</b>	Ak Ersdsd	<b>CONTRASEÑA:</b>	0d874sd	
<b>CONEXIÓN A INTERNET</b>				
<b>NOMBRE WIFI:</b>	GADCTO	<b>CONTRASEÑA:</b>	GadPRC24	
<b>CONTROL DE IMPRESORA</b>				
<b>USUARIO:</b>	x	<b>CONTRASEÑA:</b>	x	

RECIBIDO:

OTORGA:

Alejandro Ortiz