GUÍA PARA LA IMPLEMENTACIÓN DEL

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

MINISTERIO DE TELECOMUNICACIONES
Y DE LA SOCIEDAD DE LA INFORMACIÓN

Lenín
Toda una Vida
EL GOBIERNO DE TODOS

Contenido

INTRODUCCIÓN

Esta guía se ha preparado para proporcionar los requisitos para establecer, implementar y mantener el mejoramiento continuo del Esquema Gubernamental de Seguridad de la Información, que pretende ser el Sistema de Gestión de Seguridad en las instituciones Públicas de la APCID.

El establecimiento y la implementación del Esquema Gubernamental de Seguridad de la Información, están influenciados por las necesidades y objetivos de la institución, los requisitos de seguridad, los procesos utilizados, el tamaño y estructura de la institución.

El Esquema Gubernamental de Seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados.

OBJETIVO

Brindar los primeros lineamientos para que las instituciones de la APCID inicien con la implementación del Esquema Gubernamental de Seguridad de la Información.

ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN EN LAS INSTITUCIONES DE LA APCID

La asignación de responsabilidades se definió en los artículos 5, 6, 7 y 8 del acuerdo ministerial, sin embargo, en esta guía se esclarece la estructura organizacional en materia seguridad de la información en las instituciones públicas de la APCID. A continuación, se presenta las 2 figuras o roles que son base para el trabajo en seguridad de la información, estableciendo las responsabilidades que cada uno debería tener.

Queda abierto el realizar ampliaciones en cada institución, a las responsabilidades definidas, de manera que se adapte a cada realidad particular y se cumpla con la implementación del EGSI.

Oficial de Seguridad de la Información (OSI)

El Comité de Seguridad de la Información (CSI) designará al interior de su Institución a un funcionario como Oficial de Seguridad de la Información (OSI).

El Oficial de Seguridad debe tener conocimiento en Seguridad de la Información y Gestión de Proyectos, podrá ser si existiere el responsable de la Unidad de Seguridad de la Información, se recomienda que no pertenezca al área de Tecnologías de la Información.

El Oficial de Segundad de la Información, será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información. Es recomendable que el oficial de Seguridad de la Información sea un miembro independiente de las áreas de tecnología o sistemas, puesto que deberá mantener su independencia para observar las necesidades de seguridad entre la estrategia de la institución y tecnología.

Es importante que este funcionario cuente con la aceptación y apoyo de todas las áreas de la institución, es por esto que a la hora de elegir al funcionario que lleve adelante este rol es necesario que sea elegido en consenso.

Cualidades como: liderazgo, capacidad para lograr acuerdos, aceptación de sus pares, poder de gestión; son fundamentales para llevar con éxito la tarea de Oficial de Seguridad de la Información -OSI-.

Dentro de sus principales responsabilidades se encuentra:

a) Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI:

- Identificar convenientemente las partes interesadas relacionadas con el negocio y en especial con la seguridad de la información.
- Identificar los requisitos / necesidades de las partes interesadas.
- Identificar los canales de comunicación con las partes interesadas especialmente con las autoridades y grupos de interés especiales.
- Ejercer una labor de coordinación con las tareas y medios de protección de datos personales.

b) Generar propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI):

- Política de Seguridad de la información

- Política de control de la Documentación
- Política de control de accesos
- Uso aceptable de los activos
- Evaluación de riesgos
- Metodología de tratamiento de riesgos
- Declaración de aplicabilidad
- Plan de tratamiento de riesgos
- Política de revisión y actualización de la documentación

c) Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas:

- Formación interna a los funcionarios propietarios de los activos de información, para que colaboren en la realización de la evaluación de riesgos
- Coordinar el proceso de evaluación del riesgo.
- Proponer la selección de controles para el tratamiento del riesgo.
- Proponer plazos de aplicación para los controles.

d) Elaborar el Plan de concienciación en Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información (EGSI):

- Preparar el plan de formación y concienciación para la seguridad de la información y el cumplimiento del EGSI.
- Realizar actividades continuas relacionadas con la concienciación.
- Planificar charlas de Seguridad de Información para nuevos funcionarios.
- Plan de medidas disciplinarias para violaciones a la seguridad de la Información.

e) Elaborar un plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas:

- Plan de control de implementación de las medidas de mejora o acciones correctivas.
- Control de la efectividad de las medidas adoptadas

f) Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información:

- Coordinar la elaboración de un plan de continuidad de seguridad de la información.
- Coordinar la revisión del plan con ejercicios y pruebas.
- Verificar los planes de recuperación después de incidentes.

g) Orientar y generar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información detectados o reportados.

h) Coordinar la gestión de incidentes de seguridad con nivel de criticidad alto a través de otras instituciones gubernamentales.

i) Mantener la documentación de la implementación del EGSI debidamente organizada.

j) Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.

k) Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), así como las alertas que impidan su implementación:

- Plan de comunicación de los beneficios de la Seguridad de la Información
- Proponer objetivos de Seguridad de la Información
- Informe de resultados sobre indicadores medibles
- Propuestas de mejoras en la Seguridad de la Información
- Evaluación de recursos necesarios para la Seguridad de la Información

l) Previa la terminación de sus funciones el Oficial de Seguridad realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de Seguridad, en caso de ausencia, al Comité de Seguridad de la Información.

Comité de Seguridad de la Información (CSI)

El Comité de Seguridad de la Información (CSI), estará integrado por los responsables de las siguientes áreas o quienes haga sus veces: Talento Humano, Administrativa, Planificación y Gestión Estratégica, Comunicación Social, Tecnologías de la Información, Unidades Agregadores de Valor y el Área Jurídica participará como asesor.

Este comité tendrá reuniones bimensualmente, de manera recomendada durante el transcurso del primer año de implementación, desde la emisión del acuerdo ministerial.

Es imprescindible que desde las primeras reuniones del comité, puedan estar presentes todos los lideres/responsables de las áreas, con el fin de estimular la aprobación de políticas y normativas en relación a la Seguridad de la Información en cada institución; en las siguientes reuniones el enfoque puede orientarse a la planificación estratégica y gestión de aspectos vinculados a la seguridad de la información, por lo que se podría delegar la participación a los representantes de las respectivas áreas involucradas.

El Comité tendrá como principales responsabilidades:

a) Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución.

b) Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto.

d) Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.

e) Promover la difusión de la seguridad de la información dentro de la institución.

f) Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.

g) El comité deberá convocarse trimestralmente o cuando las circunstancias lo ameriten, se deberá llevar registros y actas de las reuniones.

h) Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

i) Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

j) Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

Para lograr el objetivo planteado con la Implementación del Esquema Gubernamental de Seguridad de la Información – EGSI -, es decir que la implementación sea orientada como un Sistema de Gestión de Seguridad de la Información (SGSI), es primordial conocer los principios, beneficios, modelo, entre otros aspectos de un SGSI.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

El Sistema de Gestión de Seguridad de la Información es el elemento más importante de la norma ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información institucional.

Principios

El Sistema de Gestión de Seguridad de la Información tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información:

Figura No.1 PRINCIPIOS DE LA S.I., Fuente: https://infosegur.wordpress.com/tag/disponibilidad/

- **Confidencialidad**: La información solo tiene que ser accesible o divulgada a aquellos que están autorizados.
- **Integridad**: La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.
- **Disponibilidad**: La información debe estar siempre accesible para aquellos que estén autorizados.

Beneficios

Entre los beneficios relevantes de un SGSI podemos citar los siguientes:

- Establece una metodología de Gestión de la Seguridad estructurada y clara.
- Reduce el riesgo de pérdida, robo o integridad de la información sensible.
- Los riesgos y los controles son continuamente revisados.
- Se garantiza la confianza de los usuarios en los servicios institucionales.
- Facilita la integración con otros sistemas de gestión.
- Se garantiza la continuidad de negocio tras un incidente grave.
- Cumple con la legislación vigente sobre información personal, propiedad intelectual y otras.
- La imagen de la institución mejora.
- Aumenta la confianza y las reglas claras para los miembros de la institución.
- Reduce los costes y la mejora de los procesos y el servicio.
- Se incrementa la motivación y la satisfacción del personal.
- Aumenta la seguridad en base la gestión de procesos en lugar de una compra sistemática de productos y tecnologías.

CICLO DE VIDA (modelo PDCA)

Es recomendable que los sistemas de gestión sean desarrollados bajo la metodología de la "mejora continua" o ciclo de Deming, conocido como círculo PDCA, del inglés Plan-Do-Check-Act.

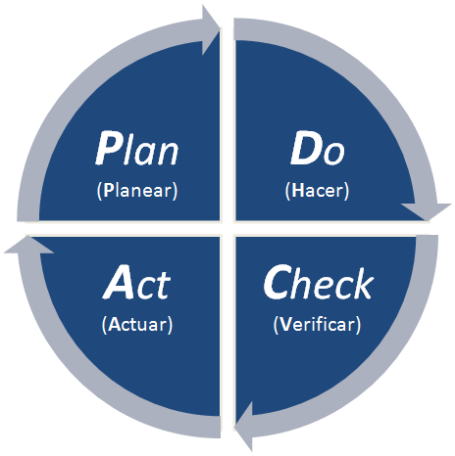

Figura No.2 MODELO PDCA,

Fuente: https://www.jacquelinebetancourt.com/single-post/2019/03/04/Mejora-Continua-Excelencia-a-nuestro-alcance

La relación que existe entre el modelo PDCA Y La ISO 27001:2013 se presenta a continuación:

ISO 27001:2013 & EL CICLO PDCA (Estructura General)						
PLAN/PLANEAR				DO/HACER	CHECK/VERIFICAR	ACT/ACTUAR
4. Contexto de la Organización	**5. Liderazgo**	**6. Planificación**	**7. Soporte**	**8. Operación**	**9. Evaluación del desempeño**	**10. Mejora**
Entendiendo la organización y su contexto	Liderazgo y Compromiso	Acciones para abordar riesgos y oportunidades	Recursos	Control y Planificación Operacional	Monitoreo, medición, análisis y evaluación.	Acciones correctivas y no conformidades
Expectativa de las partes interesadas	Política		Competencias			
Alcance del SGSI		Objetivos de S.I. y planes para alcanzarlos.	Concienciación	Evaluación de riesgos de seguridad de la Información	Auditoría interna	Mejora continua
SGSI	Organización, roles, responsabilidades y autoridades		Comunicación		Revisión de gestión	
				Tratamiento de riesgos de seguridad de la Información		
			Información Documentada			

Figura No.3, ESTRUCTURA PDCA-ISO27001,
Fuente: elaboración propia.

PROCESO PDCA ASOCIADO AL ESTANDAR INTERNACIONAL ISO 27001

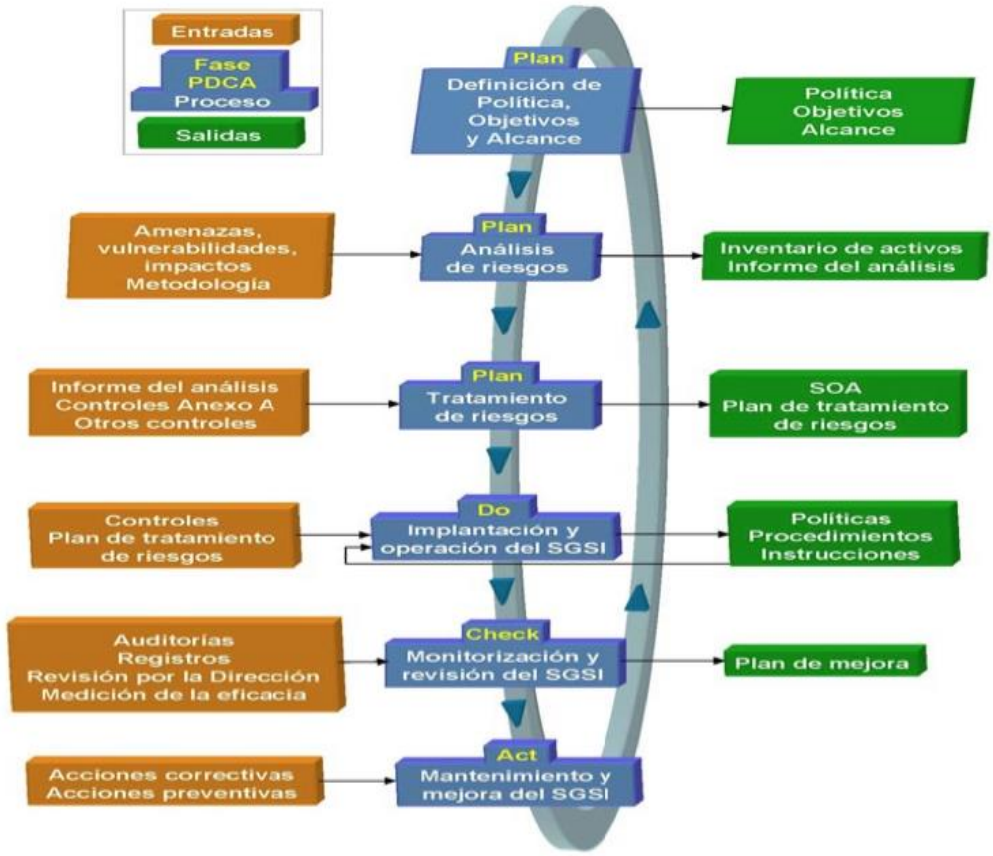

Figura No.4, PROCESO PDCA-ISO27001,

Fuente: http://www.iso27000.es/sgsi.html

"La adecuada Gestión de los Riesgos en Seguridad de la Información, conllevará a una efectiva implantación de un Sistema de Gestión de Seguridad de la Información. Sólo una vez identificado los riesgos existentes, permitirá aplicar los controles necesarios para su tratamiento".

GLOSARIO DE TÉRMINOS

Lista de términos relacionados en el contexto del Esquema Gubernamental de la Seguridad de la Información:

A.

Activo de información. - En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la institución.

Amenaza. - causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.

Análisis de riesgos. - proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Aplicación. – solución de TI, incluyendo programas de aplicación, datos de aplicaciones y procedimientos diseñados para ayudar a los usuarios de las organizaciones a realizar tareas específicas o manejar tipos específicos de problemas de TI, automatizando un proceso o función del negocio

Ataque. - intento de destruir, exponer, alterar, deshabilitar, robar o lograr acceso no autorizado o hacer uso no autorizado de un activo.

Autenticación. - Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad. - Propiedad de que una entidad es lo que afirma ser.

C.

Comité de Seguridad de la información (CSI). – se encarga de gestionar la implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información.

Confidencialidad. - Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados.

Contenidos maliciosos. - Aplicaciones, documentos, archivos, datos u otros recursos que tienen características o capacidades maliciosas incrustadas, disfrazadas o escondidas en ellos.

Control. - Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Control contramedida. - los medios de gestión de riesgos, que incluyen las políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o de carácter legal.

D.

Directiva o directriz. - Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad. - Propiedad de estar disponible y utilizable en el momento que sea requerido por una entidad autorizada.

E.

EGSI. - Esquema Gubernamental de Seguridad de la Información para las instituciones de la APCID para preservar la integridad, disponibilidad y confidencialidad de la información.

Evaluación de riesgos. - Proceso global de identificación, análisis y estimación de riesgos.

G.

Gestión de claves. - Controles referidos a la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información. - Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos. - Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

I.

Identificación de riesgos. - Proceso de encontrar, reconocer y describir riesgos.

Impacto. - El costo para la institución de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros (ejem.: pérdida de reputación, implicaciones legales, entre otros).

Incidente de seguridad de la información. - Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información.- Es uno de los activos más importantes de las instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.

Institución. - Grupo de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones.

Integridad. - Propiedad de proteger la precisión y completitud de los activos.

Internet (red interconectada), interconexión de redes. - una colección de redes interconectadas.
“La internet. - sistema global de redes interconectadas de dominio público”

Inventario de activos. - Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.)

dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

N.

No repudio. - Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

M.

Malware, software malicioso. - Software diseñado con malas intenciones que contiene características o capacidades que potencialmente pueden causar daño directamente o indirectamente al usuario y/o al sistema informático del usuario.

O.

Objetivo. - Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

Oficial de Seguridad de la Información (OSI). - Es el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema

P.

Parte interesada. - <gestión de riesgos> persona u organización que puede afectar, verse afectada por, o percibirse a sí misma como afectada por una decisión o actividad.

Phishing (engaño técnico). - proceso fraudulento o intento de adquirir información privada o confidencial de manera enmascarada haciéndose pasar por una entidad confiable en una comunicación electrónica.

Plan de continuidad del negocio. - Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos. - Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de escritorio despejado. - La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

Proceso. - Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario del activo. - puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la institución.

Propietario de la Información. - es el responsable de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

Propietario del riesgo. - persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Proveedor de servicios de Internet. - organización que presta servicios de Internet a un usuario y permite a sus clientes acceder a Internet.

R.

Resiliencia. - Capacidad de los activos institucionales, para regresar a su forma original.

Riesgo. - Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual. - El riesgo que permanece tras el tratamiento del riesgo.

S.

Seguridad de la información. - conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de información. - Aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento

Software engañoso (spyware). - que recopila información privada o confidencial de un usuario de computador.

Software potencialmente no deseado. - software engañoso, incluyendo el malware y no malicioso, que exhibe las características de software engañoso.

Spam (correo basura). - abuso de los sistemas de mensajería electrónica para enviar indiscriminadamente mensajes masivos no solicitados.

T.

Tratamiento de riesgos. - Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad. - Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Troyano, caballo de Troya. - software malintencionado que aparece para realizar una función deseable.

V.

Vulnerabilidad. - Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Dirección Nacional - Interoperabilidad, Seguridad de la Información e Infraestructura

2020-Subsecretaría de Estado-Gobierno Electrónico

www.gobiernoelectronico.gob.ec