

**INFORME DE LA EVALUACIÓN DE LOS RIESGOS
ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA
INFORMACIÓN (EGSI versión 3.0)**

AGOSTO 2026

Contenido

1	Objetivo.....	3
2	Descripción de la institución.....	3
3	Contexto de la evaluación de riesgos	6
4	Metodología de evaluación y tratamiento de riesgos	6
4.1	La metodología	6
4.2	Identificación y valoración de los activos (impacto).....	6
4.3	Identificación de amenazas y vulnerabilidades (probabilidad)	8
4.4	Identificación de controles existentes.....	9
4.5	Evaluación del riesgo	10
4.6	Tratamiento del riesgo.....	10
5	Niveles de riesgo	11
6	Nota aclaratoria	13
7	Firmas de responsabilidad	14
	Control de versiones	15
	Historial de modificaciones.....	15

1 Objetivo

El objetivo del presente documento es presentar los resultados de la evaluación de riesgos de seguridad de la información y definir el tratamiento que se aplicará a los riesgos identificados, en el marco del Esquema Gubernamental de Seguridad de la Información (EGSI versión 3.0).

2 Descripción de la institución

La creación de la Empresa Pública de Comunicación del Ecuador EP se encuentra marcada por varios hechos históricos que han llevado a los medios de comunicación públicos a enfrentar procesos de creación, extinción, absorción, fusión y cambios en su objeto y razón social.

El medio más antiguo que hoy en día es propiedad de la empresa nació en 1884: el diario “El Telégrafo”, que años más tarde se convertiría en el primer diario público del país. En 2007 se constituyó la empresa “Televisión Nacional del Ecuador TEVECUADOR S.A.”, la cual fue cambiando su denominación hasta convertirse en “Empresa Pública Televisión y Radios del Ecuador E.P.”. El crecimiento continuó seguido del proceso de incautación de medios de comunicación por parte de gobiernos anteriores; dicho conglomerado de medios, tras un proceso de absorción, pasó a ser parte de la denominada Empresa Pública Medios Públicos de Comunicación del Ecuador - Medios Públicos EP.

En mayo de 2020, mediante Decreto Ejecutivo No. 1059, se dispuso la extinción de la Empresa Pública Medios Públicos de Comunicación del Ecuador - Medios Públicos EP y, meses después, mediante Decreto Ejecutivo No. 1160 se creó la nueva Empresa Pública de Comunicación del Ecuador EP, que inició operaciones en 2021.

Ilustración 1: Línea de tiempo empresarial



Elaborado por: Oficial de Seguridad de la Información (OSI)

Misión

Prestar el servicio público de comunicación mediante la operación, gestión y desarrollo de medios de radio, televisión y plataformas digitales, produciendo y difundiendo contenidos informativos, educativos, culturales y de interés público que garanticen el acceso ciudadano a una comunicación plural, inclusiva y democrática para contribuir al mejoramiento de la calidad de vida de la población.

Visión

Al 2029, ser la empresa pública de comunicación referente en la generación de contenidos de calidad que aporten valor a la ciudadanía, consolidando un modelo de gestión innovador y eficiente que reduzca progresivamente la dependencia del financiamiento estatal.

Valores Corporativos

- **Pluralismo:** Se reconoce y promueve la participación activa de los diversos sectores sociales en los procesos comunicacionales, dentro de un marco ético, democrático y respetuoso de la diversidad de opiniones, cosmovisiones y expresiones.
- **Participación:** Se garantiza la intervención de todos los actores sociales en el ejercicio del derecho a informar, ser informados y expresar libremente sus opiniones. COMUNICA EP considera a la ciudadanía como un actor fundamental en la construcción de contenidos, incorporando sus criterios en la selección y elaboración de los mensajes, en reconocimiento de que la comunicación es un derecho que da voz a todos los demás derechos.
- **Protección de derechos:** Los medios de comunicación de COMUNICA EP se comprometen a no difundir contenidos discriminatorios, vejatorios, lesivos o que inciten a la violencia, especialmente aquellos que puedan afectar a grupos vulnerables, poblaciones en doble condición de vulnerabilidad, grupos de atención prioritaria y a niños, niñas y adolescentes.
- **Función social:** La gestión comunicacional debe priorizar el abordaje responsable de la realidad nacional y de los asuntos de interés público. Los medios de COMUNICA EP cumplen una función social orientada a informar, reflexionar y aportar a la construcción colectiva de soluciones.
- **Función pública:** Los medios de COMUNICA EP, deben transparentar su quehacer, garantizando espacios equitativos para todos los sectores de la sociedad. Su labor se orienta a producir y difundir contenidos audiovisuales y escritos en el marco del servicio público, aportando al debate democrático mediante mensajes de calidad. Les corresponde fomentar una cultura del diálogo, la participación y el pensamiento crítico y reflexivo.

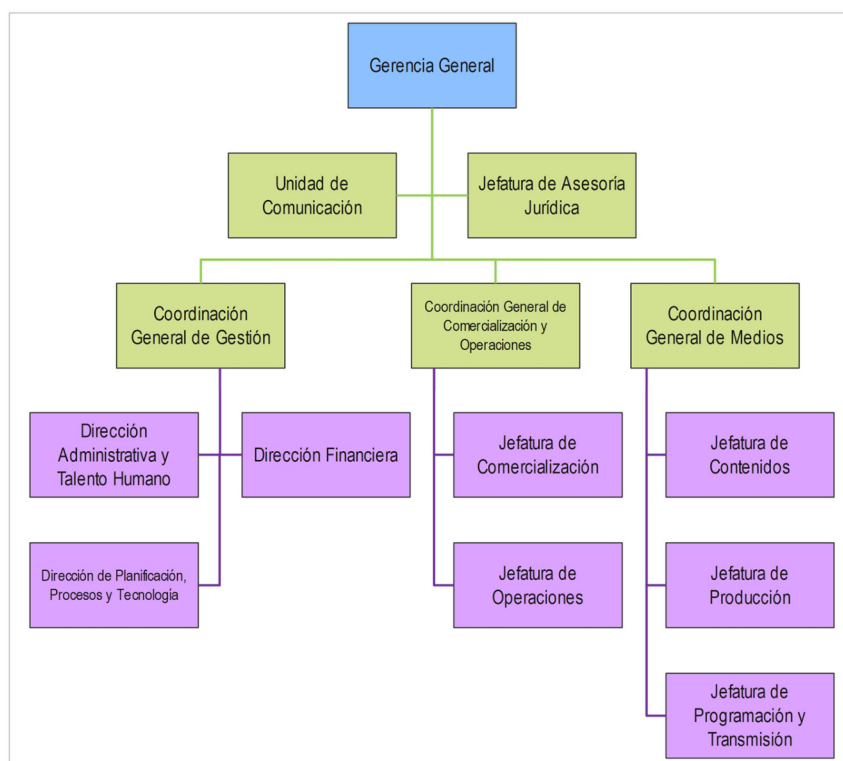
Objetivos Estratégicos

- **FINANCIERO:** Incrementar la sostenibilidad financiera con enfoque en la diversificación de las fuentes de ingresos.

- **COMERCIAL:** Incrementar el posicionamiento y la relevancia de los medios públicos de comunicación priorizando el acceso ciudadano a contenidos informativos, educativos y culturales.
- **OPERACIONAL:** Incrementar la eficiencia operacional aplicando procesos técnicos que garanticen la sostenibilidad del servicio comunicacional.
- **APREDIZAJE:** Fortalecer las capacidades empresariales.

Organigrama de la empresa

Ilustración 2: Organigrama Empresa Pública de Comunicación del Ecuador EP.



Elaborado por: Oficial de Seguridad de la Información (OSI)

Objetivos de la Seguridad de la Información

- Salvaguardar la integridad, confidencialidad y disponibilidad de la información albergada o generada en la Empresa Pública de Comunicación del Ecuador EP en cualquiera de sus estados, durante todo el ciclo de vida de la información: desde la creación, recepción y/o modificación, distribución, archivo, conservación y custodia, hasta la transferencia o destrucción de la información.
- Garantizar que las operaciones de la empresa se realicen de forma ininterrumpida, segura y confiable.

- Enfocar a las personas como el activo más sensible de la empresa en materia de seguridad de la información, generando una cultura de seguridad que minimice los riesgos.
- Realizar un correcto análisis de los activos fundamentales para el cumplimiento de la misión, visión y objetivos de la empresa, con la finalidad de aplicar los controles adecuados para mitigar los riesgos identificados.

3 Contexto de la evaluación de riesgos

La Empresa Pública de Comunicación del Ecuador EP tiene por objeto operar y mantener los servicios públicos de radiodifusión y televisión pública, incluido el diario El Telégrafo como un medio en internet.

En el marco de la aplicación del Esquema Gubernamental de Seguridad de la Información EGSI v3.0, la Empresa Pública de Comunicación del Ecuador EP implementó la metodología para la Evaluación de Riesgos, en la cual se detallan los pasos a seguir para dicha evaluación.

A la fecha de emisión de este informe, la Empresa Pública de Comunicación del Ecuador EP se encuentra en fase de transición y estructuración empresarial, por lo que el Estatuto Orgánico de Gestión Organizacional por Procesos está en desarrollo. En consecuencia, y para garantizar el cumplimiento del EGSI v3.0, la presente evaluación toma como alcance transversal los activos de información críticos que soportan la continuidad de la operación tecnológica de los medios digitales y tradicionales de la empresa.

4 Metodología de evaluación y tratamiento de riesgos

4.1 La metodología

La evaluación de riesgos se realizó con base en el estándar ISO 27005 y la metodología Magerit, con el uso de la matriz de evaluación de riesgos definida en el Anexo del Acuerdo Ministerial No. MINTEL-MINTEL-2024-0003. El proceso de evaluación de riesgos fue coordinado por el Oficial de Seguridad de la Información al interior de la empresa, conjuntamente con el Comité de Seguridad de la Información.

4.2 Identificación y valoración de los activos (impacto)

Tipo de activos identificados:

Tabla 1: Categorías y tipos de activos

Categoría	Tipo de activo
Información	Información electrónica
	Información escrita
	información hablada
	Otro tipo de información

Categoría	Tipo de activo
Software	Software comercial o herramientas, utilitarios
	Software desarrollado por terceros
	Software desarrollado internamente
	Software de administración de base de datos
	Otro software
Físicos (hardware, comunicaciones e infraestructura)	Equipo de procesamiento
	Equipo de comunicación
	Medio de almacenamiento
	Mobiliario y equipamiento
	Otros equipos
Servicios	Procesamiento y comunicación
	Servicios generales
	Otros servicios
Personal	Clientes (usuarios)
	Empleados
	Personal externo
Instalaciones	Control de acceso físico a las edificaciones y los recintos
Organización	Procedimientos y procesos
	Auditorías
Imagen y reputación	Imagen y reputación

Elaborado por: Oficial de Seguridad de la Información (OSI)

Criterios seleccionados:

Para la evaluación del impacto se consideraron los principios de seguridad de la información, analizando la pérdida de confidencialidad, disponibilidad e integridad, y en qué medida cada pérdida afecta las finanzas, las obligaciones legales y contractuales o el prestigio de la empresa. Para ello se establecieron los siguientes criterios:

Tabla 2: Escala de valor de los activos.

Valoración del impacto	en términos de la pérdida de la <u>confidencialidad</u> (Criterio)	en términos de la pérdida de la <u>integridad</u> (Criterio)	en términos de la pérdida de la <u>disponibilidad</u> (Criterio)
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la empresa. (Ej. Divulgación de información confidencial o sensible)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la empresa	El no acceso para aquellos que estén autorizados a la información o los sistemas tienen un efecto severo para la empresa

Valoración del impacto	en términos de la pérdida de la <u>confidencialidad</u> (Criterio)	en términos de la pérdida de la <u>integridad</u> (Criterio)	en términos de la pérdida de la <u>disponibilidad</u> (Criterio)
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la empresa. (Ej. Divulgación de información de uso interno)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la empresa	El no acceso para aquellos que estén autorizados a la información o los sistemas tienen un efecto considerable para la empresa
Bajo (1)	La divulgación de la información no tiene ningún efecto para la empresa. (Ej. Divulgación de información pública)	La destrucción o modificación de la información tiene un efecto leve para la empresa	El no acceso para aquellos que estén autorizados a la información o los sistemas tienen un efecto mínimo para la empresa

Elaborado por: Oficial de Seguridad de la Información (OSI)

La valoración del impacto de un activo (VA) resulta del promedio de los valores de las tres dimensiones de la Gestión de la Seguridad de la Información asociadas a cada activo de información identificado:

$$VA = \frac{C + I + D}{3}$$

4.3 Identificación de amenazas y vulnerabilidades (probabilidad)

Luego de la evaluación del impacto se procedió a evaluar la probabilidad de que se materialice el riesgo; es decir, la probabilidad de que una amenaza se aproveche de la vulnerabilidad del activo en cuestión.

Se analizó si los controles de seguridad existentes son adecuados y si han suministrado un nivel de protección suficiente. Para ello se establecieron los siguientes criterios:

Tabla 3: Nivel de amenaza y vulnerabilidad.

Valoración de la probabilidad	Estimación de la <u>amenaza</u> (criterio)	Ejemplo de amenaza (TI)	Estimación de la <u>vulnerabilidad</u> (criterio)	Ejemplo de vulnerabilidad (TI)
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Código malicioso	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza	No se utilizan contraseñas para que los usuarios ingresen a los sistemas
Medio (2)	La ocurrencia es probable (probabilidad = 50%)	Falla de hardware	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable	Existen normas para la utilización de contraseñas, pero no se implementa

Valoración de la probabilidad	Estimación de la <u>amenaza</u> (criterio)	Ejemplo de amenaza (TI)	Estimación de la <u>vulnerabilidad</u> (criterio)	Ejemplo de vulnerabilidad (TI)
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%)	desastres naturales	La medida de seguridad es adecuada	Existen normas para la utilización de contraseñas y es aplicada

Elaborado por: Oficial de Seguridad de la Información (OSI)

4.4 Identificación de controles existentes

A continuación, se presenta el resumen del estado de madurez de los controles del EGSi v3.0 por categoría, según la evaluación realizada:

Tabla 4: Resumen de controles implementados por categoría.

ítem	Categoría	Controles EGSi V3	Controles implementados	Estado de Madurez
1	Controles organizacionales	37	3	Política de Seguridad de la Información documentada. Instructivo de Teletrabajo aprobado. Plan Estratégico de Tecnología de la Información (PETI) aprobado por Gerencia General.
2	Controles de personas	8	1	Instructivo para la Aplicación y Desarrollo de Teletrabajo implementado.
3	Controles físicos	14	1	Plan de Mantenimiento de Equipos Tecnológicos aprobado por Gerencia General. Se cuenta con generador eléctrico a diésel y plan de mantenimiento de equipos de TI, sin documentación normativa que los respalde.
4	Controles tecnológicos	34	0	No implementado formalmente. Se cuenta con firewall con herramientas antimalware contratado y sistema de monitoreo Zabbix en proceso de implementación.
TOTAL		93	5	

Elaborado por: Oficial de Seguridad de la Información (OSI)

Nota: Se contabilizan como controles implementados únicamente aquellos que cuentan con documentación formal aprobada. Los elementos identificados en las categorías físico y tecnológico (generador eléctrico, plan de mantenimiento, firewall y Zabbix) se registran como controles en proceso de formalización y serán incorporados en la declaración de aplicabilidad (SoA).

4.5 Evaluación del riesgo

El nivel del riesgo se identificó como el resultado del producto de la probabilidad de ocurrencia de la amenaza, la probabilidad de ocurrencia de la vulnerabilidad y el valor del impacto del activo de la información (CID):

$$\text{Nivel de riesgo} = \text{Nivel de amenaza} * \text{Nivel de vulnerabilidad} * \text{VA(CID)}$$

Con este resultado se estableció una semaforización que permite seleccionar la opción de tratamiento de los riesgos:

Tabla 5: Nivel de aceptación de riesgos.

El Riesgo es:	NIVEL DE RIESGO (VA * nivel de amenaza * nivel de vulnerabilidad)
ALTO	de 9 a 27
MEDIO	de 4 a 8
BAJO	de 1 a 3

Elaborado por: Oficial de Seguridad de la Información (OSI)

Los riesgos identificados en nivel MEDIO y ALTO (resultado de 4 a 27) son riesgos NO aceptables y serán tratados. Los riesgos de nivel BAJO (resultado de 1 a 3) son riesgos aceptables y serán asumidos por la empresa.

4.6 Tratamiento del riesgo

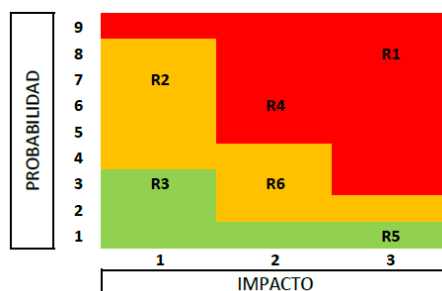
El tratamiento de los riesgos se aplicará a todos los riesgos identificados como NO aceptables. Para este proceso se han definido cuatro opciones de tratamiento:

1. **Reducción del riesgo:** elección de control o controles de seguridad del Anexo del Acuerdo Ministerial No. 0003-2024.
2. **Transferencia de los riesgos a terceros:** por ejemplo, suscribiendo una póliza de seguros o un contrato con proveedores o socios.
3. **Evitar los riesgos:** discontinuando una actividad comercial que ocasiona ese riesgo.
4. **Aceptación del riesgo:** esta opción está permitida solamente si la selección de otras opciones de tratamiento del riesgo costaría más que el potencial impacto en el caso de que se materializara dicho riesgo.

5 Niveles de riesgo

Una vez realizado el proceso de análisis y evaluación de los riesgos, a continuación, se presenta gráficamente, a través de un mapa de calor, los niveles de riesgo identificados. El eje X representa la probabilidad de ocurrencia del riesgo y el eje Y representa el impacto potencial del mismo.

Tabla 6: Mapa de calor del riesgo.



Elaborado por: Oficial de Seguridad de la Información (OSI)

Del mapa de calor se desprende la siguiente distribución de riesgos:

- **Zona ROJA (riesgo alto):** R1 (interrupción de transmisión) y R4 (ransomware/pérdida de datos críticos). Requieren tratamiento inmediato.
- **Zona AMARILLA (riesgo medio):** R2 (acceso no autorizado al portal web) y R6 (uso indebido de credenciales). Requieren tratamiento planificado.
- **Zona VERDE (riesgo bajo):** R3 (fuga de información interna) y R5 (desastres naturales). Son riesgos aceptables, sujetos a monitoreo periódico.

Tabla 7: Tabla de Descripción de Riesgos Identificados

Cód.	Amenaza	Vulnerabilidad	Riesgo/Escenario de Amenaza	Activo Afectado	Impacto Inicial	Justificación Técnica del Consultor
R1	Pérdida del suministro de energía / Falla del equipo de telecomunicaciones	Red energética inestable; ausencia de planes de continuidad	Interrupción de la transmisión y servicios de radiodifusión o TV por eventos de fuerza mayor o fallos técnicos.	Infraestructura física y servicios de emisión	ALTO	Nivel crítico: al no existir controles físicos ni de continuidad operativa documentados (Tabla 4), los fallos eléctricos o de hardware pueden suspender el servicio público de comunicación de forma inmediata.

Cód.	Amenaza	Vulnerabilidad	Riesgo/Escenario de Amenaza	Activo Afectado	Impacto Inicial	Justificación Técnica del Consultor
R2	Espionaje remoto / Falsificación de derechos	Arquitectura insegura de la red; ausencia de identificación y autenticación de emisor y receptor	Acceso no autorizado o alteración de contenidos del portal web del Diario El Telégrafo.	Software e información electrónica	MEDIO / ALTO	La ausencia de controles tecnológicos (cortafuegos a nivel aplicativo, auditorías de código) expone el sitio web a ciberataques que pueden dañar la imagen y reputación empresarial.
R3	Hurto de medios o documentos	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla; falta de conciencia acerca de la seguridad	Fuga de información confidencial o sensible por parte de servidores públicos.	Información digital o escrita	BAJO / MEDIO	Mitigación parcial: la existencia de la Política de Seguridad de la Información otorga al personal una base regulatoria de confidencialidad, reduciendo la probabilidad de ocurrencia. El PETI incorpora acciones de capacitación y concientización.
R4	Manipulación con software (envío o distribución de malware)	Ausencia de copias de respaldo; descarga y usos no controlados de software	Pérdida de integridad o disponibilidad de activos de información crítica debido a ataques de código malicioso (Ransomware).	Sistemas informáticos centrales y bases de datos.	ALTO	Nivel crítico: al no existir controles de respaldo automático (backups) ni herramientas de protección activa formalizadas, un ataque de secuestro de datos paralizaría las operaciones administrativas y de emisión. El PETI contempla la implementación de soluciones de backup como acción prioritaria.

Cód.	Amenaza	Vulnerabilidad	Riesgo/Escenario de Amenaza	Activo Afectado	Impacto Inicial	Justificación Técnica del Consultor
R5	Inundación / Fenómeno sísmico	Ubicación en un área susceptible de inundación (riesgo mitigado por el Plan de Mantenimiento de Equipos ya aprobado)	Daño colateral por desastres naturales en instalaciones técnicas centrales.	Edificaciones e Infraestructura física.	BAJO	El Plan de Mantenimiento de Equipos Tecnológicos contribuye a la resiliencia de los activos físicos. La probabilidad estadística de ocurrencia, combinada con la ubicación de las instalaciones, le otorga una valoración baja.
R6	Abuso de los derechos	Desconocimiento o en seguridad de la información; ausencia de proceso formal para la revisión de los derechos de acceso	Uso indebido de credenciales de acceso a redes sociales oficiales e infraestructura tecnológica por falta de control de usuarios.	Imagen empresarial y plataformas digitales.	MEDIO	Al no existir controles de gestión de accesos ni políticas aplicadas para contraseñas seguras, excolaboradores o terceros podrían comprometer los canales oficiales de difusión. El PETI incorpora la implementación de un sistema de gestión de identidades como acción a corto plazo.

Elaborado por: Oficial de Seguridad de la Información (OSI)

6 Nota aclaratoria

Las instituciones de la Administración Pública Central elaborarán el contenido de este documento basándose en la metodología y/o estándar seleccionado internamente en su institución para el cumplimiento de la evaluación de los riesgos, que es parte de la primera etapa de la implementación del Esquema Gubernamental de Seguridad de la Información.

7 Firmas de responsabilidad

	Nombre/Cargo	Firma
Elaborado por:	Mgs. Angel Franco Calixto Oficial de Seguridad de la Información	 Validar únicamente en FirmaEC. Firmado electrónicamente por: ANGEL DIONICIO FRANCO CALIXTO
Revisado y aprobado por:	Ing. Oscar Miranda Director de Planificación, Procesos y Tecnología, presidente del CSI	 Validar únicamente en FirmaEC. Firmado electrónicamente por: OSCAR EFRAIN MIRANDA PATIN
Aprobado por:	Ing. Oscar Miranda Director Administrativo y de Talento Humano (subrogante), vicepresidente del CSI	 Validar únicamente en FirmaEC. Firmado electrónicamente por: OSCAR EFRAIN MIRANDA PATIN
Aprobado por:	Mgs. Grace Cordero Loo Coordinadora General de Medios	 Validar únicamente en FirmaEC. Firmado electrónicamente por: GRACE VANESSA CORDERO LOOR
Aprobado por:	Espc. José Estrella López Jefe de Asesoría Jurídica	 Validar únicamente en FirmaEC. Firmado electrónicamente por: JOSE GABRIEL ESTRELLA LOPEZ
Aprobado por:	Mgs. Omar Barrera Romero Delegado de Protección de Datos Personales	 Validar únicamente en FirmaEC. Firmado electrónicamente por: OMAR GUILLERMO BARRERA ROMERO

Control de versiones

Versión:	1.0
Fecha de la versión:	27-08-2026
Creado por:	Oficial de Seguridad de la Información de la Empresa Pública de Comunicación del Ecuador EP
Revisado por:	Comité de Seguridad de la Información de la Empresa Pública de Comunicación del Ecuador
Aprobado por:	Empresa Pública de Comunicación del Ecuador EP
Nivel de confidencialidad:	Bajo

Historial de modificaciones

Versión	Fecha	Detalle del cambio
1.0	27/08/2026	Emisión inicial del documento