

PLAN DE TRATAMIENTO DE RIESGOS
(ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN - EGSÍ V3.0)

INSTITUCIÓN / SIGLAS:	Empresa Pública de Comunicación del Ecuador EP / COMUNICA EP
NIVEL DE CONFIDENCIALIDAD:	Bajo
FECHA DE ÚLTIMA MODIFICACIÓN:	27/08/2026
RESPONSABLE DEL DOCUMENTO:	Mgs. Angel Franco Calixto - Oficial de Seguridad de la Información (OSI)

ID riesgo	Tipo de Activo	Nivel del Riesgo	Opción de tratamiento	Controles a implementar EGSÍ V3	Descripción de actividades (acciones)	Responsable de implementación	Área funcional	Plazo de implementación		Recursos		
								C/M/L	Fecha de inicio	Fecha de fin	h/H x Día	(\$ USD)
[R1] Amenaza = Pérdida del suministro de energía / Falla del equipo de telecomunicaciones Vulnerabilidad = Red energética inestable; ausencia de planes de continuidad (Catálogo de Amenazas/Vulnerabilidades EGSÍ V3, fuente ISO/IEC 27005)	- Hardware - Sitio - Organización	Alto	Modificar/Reducir el riesgo	- [3.5] Protección contra las amenazas externas y ambientales - [3.11] Servicios de Soporte - [1.29] Seguridad de la información durante la interrupción - [1.30] Preparación de la TIC para la continuidad del negocio	Se debe formalizar mediante política y procedimiento documentado el uso del generador eléctrico a diésel existente, definiendo responsables de operación, frecuencia de pruebas de encendido y niveles mínimos de combustible. El Oficial de Seguridad de la Información, en conjunto con la Jefatura de Operaciones, debe elaborar un plan de continuidad de las TIC orientado a los servicios de radiodifusión y TV, que incluya un procedimiento de respuesta ante interrupción del servicio de emisión y los tiempos máximos tolerables de indisponibilidad. Se debe ejecutar al menos una prueba piloto controlada de corte de energía para validar la efectividad del plan de contingencia antes de su aprobación final.	- Director de Planificación, Procesos y Tecnología - Jefatura de Operaciones - Oficial de Seguridad de la Información	Dirección de Planificación, Procesos y Tecnología / Jefatura de Operaciones	C	01/09/2026	31/12/2026	6	\$ 5,000.00
[R2] Amenaza = Espionaje remoto / Falsificación de derechos Vulnerabilidad = Arquitectura insegura de la red; ausencia de identificación y autenticación de emisor y receptor (Catálogo de Amenazas/Vulnerabilidades EGSÍ V3, fuente ISO/IEC 27005)	- Software - Red - Información	Medio / Alto	Modificar/Reducir el riesgo	- [4.5] Autenticación Segura - [4.20] Seguridad de redes - [4.26] Requisitos de seguridad de la aplicación - [4.29] Pruebas de seguridad en el desarrollo y la aceptación	La Dirección de Planificación, Procesos y Tecnología, con apoyo del Oficial de Seguridad de la Información, implementará autenticación multifactor (MFA) para los administradores de las plataformas Joomla! (El Telégrafo), Laravel (Ecuador TV y Pública FM) y WordPress (Comunica EP). El cumplimiento de esta disposición se estructurará de la siguiente manera: Gestión Contractual y Proveedores Externos (Ecuador TV, Pública FM) Cláusulas de seguridad: Incluir de forma obligatoria requisitos de protección de datos y pruebas de pentesting en contratos vigentes y futuros. MFA obligatorio: Exigir al proveedor la configuración de doble factor mediante paquetes seguros en Laravel Análisis y remediación: El contratista ejecutará un escaneo de vulnerabilidades antes de cada despliegue mayor y corregir los hallazgos previo al paso a producción. Gestión de Desarrollo Interno (El Telégrafo y Comunica EP) MFA técnico: El área técnica activará la funcionalidad nativa de doble factor directamente en el núcleo de Joomla! y complementos corporativos en WordPress. Control previo: El equipo interno realizará el análisis de vulnerabilidades antes de liberar cualquier cambio mayor en el sitio. Solución de fallas: El personal institucional subsanará los riesgos detectados antes de la puesta en producción. Protección Perimetral Común Reglas WAF: Configurar reglas específicas a nivel de aplicación web en el firewall contratado para mitigar ataques dirigidos a las vulnerabilidades propias de Joomla!, WordPress y Laravel.	- Dirección de Planificación, Procesos y Tecnología - Proveedor de desarrollo/mantenimiento del portal web - Oficial de Seguridad de la Información	Dirección de Planificación, Procesos y Tecnología / Jefatura de contenidos / Dirección de comunicación	C	01/09/2026	31/12/2026	4	\$ 14,400.00
[R3] Amenaza = Hurto de medios o documentos Vulnerabilidad = Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla; falta de conciencia acerca de la seguridad (Catálogo de Amenazas/Vulnerabilidades EGSÍ V3, fuente ISO/IEC 27005)	- Información - Personal - Organización	Bajo / Medio	Modificar/Reducir el riesgo	- [1.12] Clasificación de la información - [2.3] Concienciación, educación y formación en seguridad de la información - [2.6] Acuerdo de confidencialidad o no divulgación	El Oficial de Seguridad de la Información debe elaborar y someter a aprobación del CSI un esquema de clasificación de la información institucional (pública, uso interno, confidencial), que diferencie el contenido periodístico de carácter público de la información administrativa reservada. Todos los funcionarios de la institución, y en donde sea pertinente los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la institución pertinentes para su cargo; se deben realizar campañas de concientización orientadas por el OSI y el CSI, para realizar el seguimiento pertinente, garantizando que el personal esté capacitado en temas de seguridad de la información, convirtiendo esa falta de conciencia en fortaleza para la institución. En paralelo, la Jefatura de Asesoría Jurídica y el OSI deben revisar y formalizar la validación de los acuerdos de confidencialidad o no divulgación ya existentes, y la Política de Seguridad de la Información debe difundirse formalmente a todo el personal.	- Oficial de Seguridad de la Información - Dirección Administrativa y Talento Humano - Jefatura de Asesoría Jurídica	Dirección Administrativa y Talento Humano	M	31/12/2026	31/05/2027	3	\$ 0.00
[R4] Amenaza = Manipulación con software (envío o distribución de malware) Vulnerabilidad = Ausencia de copias de respaldo; descarga y uso no controlados de software (Catálogo de Amenazas/Vulnerabilidades EGSÍ V3, fuente ISO/IEC 27005)	- Software - Hardware - Información	Alto	Modificar/Reducir el riesgo	- [4.13] Copia de seguridad de la información - [4.7] Protección contra malware - [4.8] Gestión de vulnerabilidades técnicas - [4.16] Actividades de monitoreo	La Dirección de Planificación, Procesos y Tecnología debe implementar una solución de respaldo (backup) automático y periódico para los sistemas y bases de datos críticas de la institución, asegurando al menos una copia fuera de sitio o en un repositorio aislado de la red administrativa, conforme a la prioridad ya establecida en el PETI. Debe formalizarse documentalmente, mediante política y procedimiento, el uso del firewall y las herramientas antimalware ya contratadas, incluyendo la revisión periódica de su eficacia. Se debe definir un cronograma de escaneo de vulnerabilidades técnicas sobre los servidores y bases de datos centrales, con remediación de hallazgos críticos en plazos definidos. Finalmente, se debe concluir la implementación del sistema de monitoreo Zabbix y configurar alertas automáticas ante eventos de seguridad críticos, con notificación inmediata al OSI.	- Dirección de Planificación, Procesos y Tecnología - Oficial de Seguridad de la Información	Dirección de Planificación, Procesos y Tecnología	C	01/09/2026	31/12/2026	6	\$ 15,000.00
[R5] Amenaza = Inundación / Fenómeno sísmico Vulnerabilidad = Ubicación en un área susceptible de inundación (Catálogo de Amenazas/Vulnerabilidades EGSÍ V3, fuente ISO/IEC 27005); riesgo mitigado por el Plan de Mantenimiento de Equipos ya aprobado	- Sitio - Hardware	Bajo	Aceptar el riesgo	- [3.13] Mantenimiento de equipo (control ya implementado) - [3.5] Protección contra las amenazas externas y ambientales (monitoreo periódico)	Conforme a la Tabla 5 del Informe de Evaluación de Riesgos, los riesgos de nivel bajo (resultado de 1 a 3) son riesgos aceptables y serán asumidos por la institución; por lo tanto, no se requieren acciones adicionales de tratamiento más allá de las ya existentes. Se debe mantener vigente el Plan de Mantenimiento de Equipos Tecnológicos ya aprobado por Gerencia General, y realizar una revisión anual de la ubicación y condiciones físicas de las instalaciones técnicas centrales frente a riesgos naturales, dejando constancia escrita de dicha revisión como evidencia de monitoreo periódico del riesgo aceptado.	- Dirección de Planificación, Procesos y Tecnología - Oficial de Seguridad de la Información	Dirección de Planificación, Procesos y Tecnología	L	01/09/2026	28/02/2028	1	\$ 0.00

[R6] Amenaza = Abuso de los derechos Vulnerabilidad = Desconocimiento en seguridad de la información; ausencia de proceso formal para la revisión de los derechos de acceso (Catálogo de Amenazas/Vulnerabilidades EGIS V3, fuente ISO/IEC 27005)	- Personal - Software - Organización	Medio	Modificar/Reducir el riesgo	- [1.16] Gestión de Identidad - [1.18] Derechos de acceso - [4.2] Derechos de acceso privilegiado - [2.5] Responsabilidades después de la terminación o cambio de empleo	La Dirección de Planificación, Procesos y Tecnología debe implementar un sistema de gestión de identidades y accesos (IAM), conforme a lo ya contemplado en el PETI como acción de corto plazo, y definir junto con la Unidad de Comunicación una política de contraseñas seguras para las redes sociales oficiales e infraestructura tecnológica institucional. Se debe realizar una revisión y depuración de los accesos vigentes a redes sociales y plataformas digitales, retirando de forma inmediata las cuentas de excolaboradores o terceros que ya no deban tener acceso. Este proceso debe quedar formalmente vinculado al procedimiento de desvinculación de personal de la Dirección Administrativa y Talento Humano, de modo que la revocación de accesos y credenciales sea automática e inmediata ante la salida o cambio de puesto de un colaborador.	- Dirección de Planificación, Procesos y Tecnología - Dirección de Comunicación - Dirección Administrativa y Talento Humano	Dirección de Comunicación / Dirección de Planificación, Procesos y Tecnología	M	31/12/2026	31/05/2027	4	\$ 0.00

\$ 34,400.00

FIRMAS DE RESPONSABILIDAD	
NOMBRES/CARGO	FIRMA
Mgs. Angel Franco Calixto OFICIAL DE SEGURIDAD DE LA INFORMACIÓN Especialista de Infraestructura, Soporte Técnico y Seguridad de la Información	 Validar únicamente en FirmaEC. Firmado electrónicamente por: ANGEL DIONICIO FRANCO CALIXTO
Ing. Oscar Miranda PRESIDENTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Director de Planificación, Procesos y Tecnología	 Validar únicamente en FirmaEC. Firmado electrónicamente por: OSCAR EFRAIN MIRANDA PATIN
Ing. Oscar Miranda INTEGRANTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Director Administrativo y de Talento Humano (subrogante)	 Validar únicamente en FirmaEC. Firmado electrónicamente por: OSCAR EFRAIN MIRANDA PATIN
Mgs. Grace Cordero Loor INTEGRANTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Coordinadora General de Medios	 Validar únicamente en FirmaEC. Firmado electrónicamente por: GRACE VANESSA CORDERO LOOR
Espc. José Estrella López INTEGRANTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Jefe de Asesoría Jurídica	 Validar únicamente en FirmaEC. Firmado electrónicamente por: JOSE GABRIEL ESTRELLA LOPEZ
Mgs. Omar Barrera Romero INTEGRANTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Especialista de Planificación y Desarrollo Tecnológico	 Validar únicamente en FirmaEC. Firmado electrónicamente por: OMAR GUILLERMO BARRERA ROMERO