



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN

SUBSECRETARÍA DE GOBIERNO
ELECTRÓNICO Y REGISTRO CIVIL

DECLARACIÓN DE APLICABILIDAD (Statement of Applicability - SoA)

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN - EGSi V3.0

INSTITUCIÓN / SIGLA:	Empresa Pública de Comunicación del Ecuador EP / COMUNICA EP
NÚMERO DE CONTROLES SELECCIONADOS Y APLICABLES:	91 de 93 controles del EGSi v3.0 (consolidado preliminar)
NIVEL DE CONFIDENCIALIDAD:	Bajo
RESPONSABLE DEL DOCUMENTO:	Mgs. Angel Franco Calixto - Oficial de Seguridad de la Información (OSI)

CRITERIOS PARA IDENTIFICAR LOS CONTROLES APLICABLES (controles necesarios, independientemente que se encuentren implementados o no)

1. Resultado de la evaluación de riesgos, ¿Qué controles necesito para gestionar los riesgos identificados?
2. Cumplimiento de otras normativas legales que corresponda a cada institución, ¿Qué controles me ayudan a cumplir con algún requisito legal o regulación?
3. Necesidad institucional, ¿Qué controles de seguridad son necesarios institucionalmente (buenas prácticas) y no han sido considerados en los dos criterios anteriores?

ANEXO - EGSi V3.0			Estado actual del Control	Aplica Si/No	Justificación de la selección (Si) o de la exclusión (No)	Observaciones
Ítem	Sección	Descripción				
	1	CONTROLES ORGANIZACIONALES				
1	1.1	Políticas de seguridad de la información (específicas)	Implementado	Si	Resultado de la evaluación de riesgos (R1, R3, R4, R6) y obligación normativa del EGSi v3.0. Establece el marco regulatorio base para todo el SGSi.	Política de Seguridad de la Información documentada y aprobada.
2	1.2	Roles y Responsabilidades de Seguridad de la Información	Por implementar	Si	Buena práctica y obligación normativa del EGSi v3.0: sin roles y responsabilidades definidos no es posible operar ni auditar el SGSi.	Se recomienda formalizar mediante resolución o manual de funciones de seguridad de la información.
3	1.3	Separación de Funciones	Por implementar	Si	Necesidad institucional: mitiga el riesgo de abuso de privilegios (relacionado con R6, uso indebido de credenciales) al evitar la concentración de funciones críticas en una sola persona.	Aplica especialmente a roles de administración de sistemas y de comercialización / finanzas.
4	1.4	Responsabilidades de la dirección	Por implementar	Si	Obligación normativa del EGSi v3.0: la alta dirección debe demostrar compromiso explícito y asignar recursos al SGSi.	Se sugiere incluirlo en el Plan Estratégico de Tecnología de la Información (PETI) ya aprobado.
5	1.5	Contacto con las autoridades	Por implementar	Si	Necesidad institucional y obligación legal: como entidad pública, COMUNICA EP requiere canales formales con CSIRT-EGOB, ARCTEL y otras autoridades competentes ante incidentes.	Formalizar punto de contacto institucional con el CSIRT gubernamental.
6	1.6	Contacto con grupos de interés especial	Parcialmente implementado	Si	Buena práctica: mantener contacto con grupos de interés especial mejora la inteligencia de amenazas y la respuesta coordinada del sector.	El OSI participa en un grupo de WhatsApp de OSI a nivel nacional; falta formalizar el canal y sus objetivos.
7	1.7	Inteligencia de amenazas	Por implementar	Si	Resultado de la evaluación de riesgos (R2, R4): necesario para anticipar amenazas de ciberseguridad como ransomware y ataques al portal web.	Puede apoyarse en alertas del CSIRT-EGOB y proveedores de ciberseguridad.
8	1.8	Seguridad de la información en la Gestión de proyectos	Por implementar	Si	Buena práctica: la institución desarrolla proyectos tecnológicos (PETI) que deben incorporar seguridad desde el diseño.	Integrar checklist de seguridad de la información en la metodología de gestión de proyectos institucional.

9	1.9	Inventario de información y otros activos asociados	Parcialmente implementado	Si	Resultado de la evaluación de riesgos (R3, R4): un inventario completo de activos es prerequisite para proteger la información crítica y gestionar copias de seguridad.	Existen inventarios en Dirección Administrativa y Talento Humano; los inventarios de hardware y software de TI están incompletos.
10	1.10	Uso aceptable de la información y otros activos asociados	Por implementar	Si	Resultado de la evaluación de riesgos (R3, R6): reduce la probabilidad de fuga de información y uso indebido de activos institucionales.	Debe articularse con la Política de Seguridad de la Información ya aprobada.
11	1.11	Devolución de activos	Implementado	Si	Obligación normativa institucional y buena práctica para el control de activos físicos asignados al personal.	Existen actas de entrega-recepción y el Manual de Lineamientos para Verificación, Recepción, Registro, Custodia y Traspaso de Bienes.
12	1.12	Clasificación de la información	Por implementar	Si	Resultado de la evaluación de riesgos (R3, R6): permite diferenciar la información pública periodística de la información confidencial/administrativa, reduciendo el riesgo de fuga.	Debe considerar el carácter público de gran parte de la información (medio de comunicación) frente a la información reservada institucional.
13	1.13	Etiquetado de la información	Por implementar	Si	Necesidad institucional derivada del control 1.12: el etiquetado permite aplicar el tratamiento adecuado según la clasificación.	Implementación condicionada a contar primero con esquema de clasificación de la información (1.12).
14	1.14	Transferencia de información	Por implementar	Si	Resultado de la evaluación de riesgos (R3): regula la transferencia segura de información entre direcciones, medios y terceros (agencias de noticias, proveedores).	Incluye transferencia electrónica, física y verbal de información.
15	1.15	Control de Acceso	Por implementar	Si	Resultado de la evaluación de riesgos (R6, uso indebido de credenciales): control de acceso es prioritario ante la ausencia total de gestión de accesos identificada en el diagnóstico.	El PETI contempla la implementación de un sistema de gestión de identidades a corto plazo.
16	1.16	Gestión de Identidad	Por implementar	Si	Resultado de la evaluación de riesgos (R6): necesario para evitar que excolaboradores o terceros mantengan accesos a redes sociales oficiales e infraestructura tecnológica.	Acción contemplada en el PETI como prioridad de corto plazo.
17	1.17	Información de autenticación	Por implementar	Si	Resultado de la evaluación de riesgos (R6): gestión segura de contraseñas y credenciales de autenticación a sistemas y plataformas digitales.	Debe incluir políticas de complejidad, vigencia y resguardo de credenciales.
18	1.18	Derechos de acceso	Por implementar	Si	Resultado de la evaluación de riesgos (R6): formaliza el otorgamiento, revisión y revocación de derechos de acceso, especialmente ante salida de personal.	Vincular con el proceso de desvinculación de Talento Humano.
19	1.19	Seguridad de la información en las relaciones con proveedores	Por implementar	Si	Necesidad institucional: la empresa contrata servicios de proveedores externos (firewall, monitoreo Zabbix, desarrollo del portal web), lo que exige gestionar el riesgo en la cadena de suministro.	Prioritario dado que ya existen relaciones contractuales activas con proveedores de TI.
20	1.20	Abordar la seguridad de la información en los acuerdos con proveedores	Por implementar	Si	Necesidad institucional: los contratos vigentes (firewall, monitoreo) no incorporan cláusulas formales de seguridad de la información.	Revisar y actualizar contratos vigentes y futuros con cláusulas de confidencialidad y seguridad.

21	1.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	Por implementar	Si	Resultado de la evaluación de riesgos (R2, R4): mitiga riesgos derivados de proveedores de TIC que dan soporte a sistemas críticos y al portal web institucional.	Aplica a proveedores de hosting, desarrollo web y soluciones de ciberseguridad.
22	1.22	Monitoreo, revisión y gestión de cambios de servicios de proveedores.	Por implementar	Si	Necesidad institucional: se requiere supervisar el desempeño y cambios en los servicios contratados (firewall, Zabbix).	Definir indicadores de cumplimiento (SLA) para los servicios de TI contratados.
23	1.23	Seguridad de la información para el uso de servicios en la nube	Por implementar	No	No aplica actualmente: la institución no ha identificado el uso de servicios en la nube como parte de su infraestructura crítica a la fecha de este informe.	Reevaluar la aplicabilidad si se contratan servicios cloud (correo, almacenamiento, hosting) en el futuro.
24	1.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Por implementar	Si	Resultado de la evaluación de riesgos (R1, R4 - riesgo ALTO): la ausencia de planificación de incidentes agrava el impacto de interrupciones de transmisión y ataques de ransomware.	Prioridad alta; debe articularse con el plan de continuidad de negocio (1.30).
25	1.25	Evaluación y decisión sobre eventos de seguridad de la información	Por implementar	Si	Resultado de la evaluación de riesgos (R1, R4): permite clasificar y escalar adecuadamente los eventos de seguridad detectados por el monitoreo (Zabbix).	Definir criterios de escalamiento según severidad del evento.
26	1.26	Respuesta a incidentes de seguridad de la información	Por implementar	Si	Resultado de la evaluación de riesgos (R1, R4 - riesgo ALTO): procedimiento crítico para contener y responder ante un eventual ataque de ransomware o interrupción de servicio.	Prioridad alta; vincular con el plan de respuesta a incidentes y notificación al CSIRT-EGOB.
27	1.27	Aprendiendo de los incidentes de seguridad de la información	Por implementar	Si	Buena práctica: cierra el ciclo de mejora continua del SGSI, exigido por el EGSi v3.0.	Implementar lecciones aprendidas posteriores a cada incidente gestionado.
28	1.28	Recopilación de evidencias	Por implementar	Si	Obligación legal: necesario para preservar evidencia digital ante eventuales procesos legales o investigaciones derivadas de incidentes de seguridad.	Coordinar con Jefatura de Asesoría Jurídica para la cadena de custodia de evidencias.
29	1.29	Seguridad de la Información durante la interrupción	Por implementar	Si	Resultado de la evaluación de riesgos (R1 - riesgo ALTO): crítico para mantener la seguridad de la información durante interrupciones de los servicios de radiodifusión o TV.	Prioridad alta; relacionado directamente con el riesgo R1 del informe de evaluación.
30	1.30	Preparación de la TIC para la continuidad del Negocio	Por implementar	Si	Resultado de la evaluación de riesgos (R1, R4 - riesgo ALTO): la continuidad del servicio público de comunicación depende de la preparación de las TIC ante eventos disruptivos.	Prioridad alta; el PETI debe incorporar este componente como eje de continuidad operativa.
31	1.31	Requisitos legales, estatutarios, reglamentarios y contractuales	Por implementar	Si	Obligación legal: como empresa pública, COMUNICA EP debe cumplir la Ley Orgánica de Transparencia, la Ley Orgánica de Protección de Datos Personales y normativa EGSi emitida por el ente rector.	Elaborar matriz de requisitos legales, estatutarios, reglamentarios y contractuales aplicables.
32	1.32	Derechos de propiedad intelectual	Por implementar	Si	Obligación legal: la institución produce y administra contenidos periodísticos y audiovisuales protegidos por derechos de autor y propiedad intelectual.	Relevante para el diario El Telégrafo y la producción audiovisual de los medios de COMUNICA EP.
33	1.33	Protección de los registros	Por implementar	Si	Obligación legal y resultado de la evaluación de riesgos (R3): protege registros administrativos, contables y periodísticos contra pérdida, destrucción o alteración.	Debe alinearse con la normativa de archivo público vigente en Ecuador.

34	1.34	Privacidad y protección de PII	Por implementar	Si	Obligación legal: cumplimiento de la Ley Orgánica de Protección de Datos Personales del Ecuador, dado que la institución trata datos de empleados, usuarios y ciudadanos.	La institución ya cuenta con un Delegado de Protección de Datos Personales designado.
35	1.35	Revisión independiente de seguridad de la información	Por implementar	Si	Buena práctica y obligación normativa del EGSi v3.0: garantiza objetividad en la verificación del cumplimiento del SGSi.	Puede ejecutarse mediante auditoría interna o externa independiente del área de TI.
36	1.36	Cumplimiento de políticas, reglas y normas de seguridad de la información	Por implementar	Si	Obligación normativa del EGSi v3.0: verifica que las políticas y normas internas de seguridad se cumplan efectivamente.	Vincular con el control 1.35 (revisión independiente).
37	1.37	Procedimientos operativos documentados	Por implementar	Si	Buena práctica: la documentación de procedimientos operativos reduce errores humanos y facilita la continuidad ante rotación de personal.	Priorizar la documentación de los procesos de TI críticos (backup, monitoreo, soporte).
2 CONTROLES DE PERSONAS						
38	2.1	Selección de personas, documentado e implementado	Parcialmente implementado	Si	Buena práctica y obligación legal: un proceso formal de selección de personal reduce el riesgo de vinculación de personas no idóneas a roles sensibles.	Se realizan procedimientos de selección, pero no existen procesos ni documentación formalizada.
39	2.2	Términos y condiciones de empleo, documentado e implementado	Por implementar	Si	Obligación legal y buena práctica: los términos y condiciones de empleo deben incluir cláusulas explícitas de seguridad de la información.	Coordinar con Dirección Administrativa y Talento Humano para incluir cláusulas en contratos.
40	2.3	Concienciación, educación y formación en seguridad de la información, documentado e implementado	Por implementar	Si	Resultado de la evaluación de riesgos (R3, R6): el personal es el activo más sensible identificado en el informe; la concientización reduce la fuga de información y el uso indebido de credenciales.	El PETI ya contempla acciones de capacitación y concientización en seguridad de la información.
41	2.4	Proceso disciplinario, documentado e implementado	Implementado	Si	Obligación legal: la institución cuenta con normativa vigente sobre prevención y sanción de faltas disciplinarias.	Existe el Instructivo de Protocolo de Prevención, Protección y Sanción de Faltas Disciplinarias Graves por Discriminación, Violencia y Acoso Laboral.
42	2.5	Responsabilidades después de la terminación o cambio de empleo, documentado e implementado	Por implementar	Si	Resultado de la evaluación de riesgos (R6): crítico para revocar accesos y proteger activos de información tras la salida o cambio de puesto del personal.	Vincular con los controles 1.16, 1.18 y el proceso de desvinculación de Talento Humano.
43	2.6	Acuerdo de confidencialidad o no divulgación, documentado e implementado	Parcialmente implementado	Si	Resultado de la evaluación de riesgos (R3): reduce la probabilidad de fuga de información confidencial por parte de servidores públicos.	Existen documentos de acuerdo de confidencialidad, pero no han sido validados por el Comité de Seguridad de la Información ni por el OSI.
44	2.7	Trabajo remoto, documentado e implementado	Implementado	Si	Obligación normativa y necesidad institucional: regula las condiciones de seguridad de la información para el personal bajo modalidad de teletrabajo.	Instructivo para la Aplicación y Desarrollo de Teletrabajo aprobado e implementado.
45	2.8	Reporte de eventos de seguridad de la información, documentado e implementado	Por implementar	Si	Resultado de la evaluación de riesgos (R1, R4): habilita la detección temprana de incidentes por parte de todo el personal, no solo del área de TI.	Definir canal y formulario simple de reporte accesible a todos los colaboradores.
3 CONTROLES FÍSICOS						
46	3.1	Perímetros de seguridad física	Por implementar	Si	Resultado de la evaluación de riesgos (R1 - riesgo ALTO): protege la infraestructura física de transmisión y los equipos centrales ante accesos no autorizados.	Prioridad alta; relacionado con la continuidad del servicio público de radiodifusión y TV.

47	3.2	Entrada física	Por implementar	Si	Resultado de la evaluación de riesgos (R1): controla el ingreso físico a las áreas técnicas y de transmisión.	Evaluar implementación de control de acceso biométrico o por tarjeta en salas técnicas.
48	3.3	Seguridad de oficinas, despachos e instalaciones	Por implementar	Si	Necesidad institucional: la institución opera salas de transmisión, redacción y servidores que requieren protección física diferenciada.	Aplica a oficinas administrativas, salas de transmisión y cuarto de servidores.
49	3.4	Monitoreo de seguridad física	Por implementar	Si	Resultado de la evaluación de riesgos (R1): el monitoreo físico complementa el monitoreo tecnológico (Zabbix) ya en implementación.	Evaluar la viabilidad de cámaras de videovigilancia en áreas críticas (cuarto de servidores, transmisión).
50	3.5	Protección contra las amenazas externas y ambientales	Por implementar	Si	Resultado de la evaluación de riesgos (R1 - riesgo ALTO, R5): mitiga fallos eléctricos y daños ambientales que pueden suspender el servicio de forma inmediata.	El generador eléctrico a diésel existe pero sin política o procedimiento formal que respalde el control.
51	3.6	Trabajo en áreas seguras	Por implementar	Si	Necesidad institucional: existen áreas que requieren controles adicionales de seguridad (cuarto de servidores, archivo).	Definir el listado de áreas seguras y sus controles de acceso restringido.
52	3.7	Puesto de trabajo despejado y pantalla limpia	Por implementar	Si	Buena práctica: reduce el riesgo de exposición de información sensible en puestos de trabajo desatendidos.	Política de escritorio limpio y bloqueo automático de pantalla, de bajo costo de implementación.
53	3.8	Ubicación y protección de equipos	Por implementar	Si	Resultado de la evaluación de riesgos (R1 - riesgo ALTO): protege los equipos de procesamiento y comunicación críticos para la emisión.	Prioridad alta; incluye protección contra cortes eléctricos, sobrecalentamiento y manipulación no autorizada.
54	3.9	Seguridad de los activos fuera de las instalaciones	Por implementar	Si	Necesidad institucional: el personal de prensa y producción utiliza equipos móviles (cámaras, laptops) fuera de las instalaciones.	Definir lineamientos para equipos usados en coberturas externas.
55	3.10	Medios de almacenamiento	Por implementar	Si	Resultado de la evaluación de riesgos (R3, R4): protege medios de almacenamiento que contienen archivos periodísticos, respaldos e información institucional.	Incluye discos externos, cintas de respaldo y medios extraíbles.
56	3.11	Servicios de Soporte	Parcialmente implementado	Si	Resultado de la evaluación de riesgos (R1 - riesgo ALTO): el respaldo eléctrico es esencial para la continuidad de la transmisión.	Se cuenta con generador eléctrico a diésel, pero no existen políticas ni procedimientos formales al respecto; requiere formalización prioritaria.
57	3.12	Seguridad del cableado	Por implementar	Si	Buena práctica: protege el cableado de red y eléctrico contra interceptación, daño o interrupción.	Aplica especialmente al cableado de los cuartos de comunicaciones y transmisión.
58	3.13	Mantenimiento de equipo	Implementado	Si	Resultado de la evaluación de riesgos (R5): el mantenimiento preventivo reduce la probabilidad de fallos de hardware.	Plan de Mantenimiento de Equipos Tecnológicos aprobado por Gerencia General.
59	3.14	Eliminación segura o reutilización de equipos	Por implementar	Si	Resultado de la evaluación de riesgos (R3): previene la fuga de información a través de equipos dados de baja o reutilizados sin borrado seguro.	Definir procedimiento de borrado seguro o destrucción física de medios de almacenamiento.
4	CONTROLES TECNOLÓGICOS					
60	4.1	Dispositivos de usuario final	Por implementar	Si	Resultado de la evaluación de riesgos (R2, R6): regula el uso seguro de laptops, equipos móviles y estaciones de trabajo del personal.	Incluye lineamientos de antivirus, cifrado y uso de dispositivos personales (BYOD) si aplica.

61	4.2	Derechos de acceso privilegiado	Por implementar	Si	Resultado de la evaluación de riesgos (R6 - riesgo MEDIO): restringe y audita las cuentas con privilegios administrativos sobre sistemas y redes sociales oficiales.	Crítico para mitigar el uso indebido de credenciales identificado en el riesgo R6.
62	4.3	Restricción de acceso a la información	Por implementar	Si	Resultado de la evaluación de riesgos (R2, R6): limita el acceso a la información según el principio de necesidad de conocer.	Aplica a los sistemas de gestión de contenidos del portal web y bases de datos institucionales.
63	4.4	Acceso al código fuente	Por implementar	Si	Resultado de la evaluación de riesgos (R2): protege el código fuente del portal web institucional contra accesos o modificaciones no autorizadas.	Aplica si existe desarrollo propio o repositorios gestionados internamente.
64	4.5	Autenticación Segura	Por implementar	Si	Resultado de la evaluación de riesgos (R2, R6 - riesgo MEDIO): la autenticación robusta es la principal barrera contra el acceso no autorizado al portal web y otros sistemas.	Evaluar la implementación de autenticación multifactor (MFA) en sistemas críticos.
65	4.6	Gestión de la capacidad	Por implementar	Si	Buena práctica: garantiza que la infraestructura tecnológica soporte la demanda de los servicios de streaming, portal web y sistemas administrativos.	Relevante para evitar degradación del servicio en eventos de alta audiencia.
66	4.7	Proteccion contra malware	Parcialmente implementado	Si	Resultado de la evaluación de riesgos (R4 - riesgo ALTO): control directo contra el riesgo de ransomware identificado como crítico en el informe.	Se cuenta con firewall y herramientas antimalware contratadas; requiere formalización documental y revisión periódica de eficacia.
67	4.8	Gestión de vulnerabilidades técnicas	Por implementar	Si	Resultado de la evaluación de riesgos (R2, R4 - riesgo ALTO): identifica y corrige vulnerabilidades antes de que sean explotadas por amenazas como ransomware o accesos no autorizados.	Prioridad alta; considerar escaneos periódicos de vulnerabilidades en el portal web y sistemas centrales.
68	4.9	Gestión de la Configuración	Por implementar	Si	Buena práctica: una configuración estandarizada reduce la superficie de ataque de servidores y equipos de red.	Definir líneas base de configuración segura (hardening) para servidores y equipos críticos.
69	4.10	Eliminación de información	Por implementar	Si	Resultado de la evaluación de riesgos (R3): garantiza la eliminación segura de información cuando ya no es necesaria, evitando fuga de datos.	Vincular con el control 3.14 (eliminación segura de equipos).
70	4.11	Enmascaramiento de datos	Por implementar	No	No aplica actualmente: la institución no maneja bases de datos con información sensible que requiera enmascaramiento (no es una entidad financiera ni de salud).	Reevaluar si se implementan sistemas con datos personales sensibles de gran escala.
71	4.12	Prevención de fuga de datos	Por implementar	Si	Resultado de la evaluación de riesgos (R3): previene la fuga de información confidencial o sensible por parte de servidores públicos.	Puede iniciarse con controles básicos (restricción de USB, monitoreo de transferencias) antes de soluciones DLP avanzadas.
72	4.13	Copia de seguridad de la información	Por implementar	Si	Resultado de la evaluación de riesgos (R4 - riesgo ALTO): control prioritario ante el riesgo de ransomware; sin respaldos, un ataque paralizaría las operaciones administrativas y de emisión.	El PETI contempla la implementación de soluciones de backup como acción prioritaria. Máxima prioridad de implementación.

73	4.14	Redundancia de las instalaciones de tratamiento de información	Por implementar	Si	Resultado de la evaluación de riesgos (R1, R4 - riesgo ALTO): la redundancia reduce el impacto de fallos en las instalaciones de procesamiento de información crítica.	Evaluar sitio alternativo o redundancia en la nube para sistemas críticos de emisión y portal web.
74	4.15	Registros de eventos	Por implementar	Si	Resultado de la evaluación de riesgos (R2, R4): los registros de eventos permiten detectar y reconstruir incidentes de seguridad.	Debe integrarse con el sistema de monitoreo Zabbix en implementación.
75	4.16	Actividades de monitoreo	Parcialmente implementado	Si	Resultado de la evaluación de riesgos (R1, R4): el monitoreo activo permite detectar tempranamente fallos técnicos y comportamientos anómalos.	Se está implementando el sistema de monitoreo Zabbix; requiere formalización documental y definición de alertas.
76	4.17	Sincronización de reloj	Por implementar	Si	Buena práctica: la sincronización de reloj es esencial para la correlación confiable de registros de eventos durante una investigación de incidentes.	Bajo costo de implementación (NTP); recomendable junto con 4.15.
77	4.18	Uso de programas de utilidad privilegiados	Por implementar	Si	Necesidad institucional: restringe el uso de herramientas administrativas que podrían usarse para eludir controles de seguridad.	Aplica a herramientas de administración de servidores y redes.
78	4.19	Instalación de software en sistemas operativos	Por implementar	Si	Resultado de la evaluación de riesgos (R4): previene la instalación de software no autorizado que pueda introducir código malicioso.	Restringir privilegios de instalación en estaciones de trabajo del personal.
79	4.20	Seguridad de redes	Por implementar	Si	Resultado de la evaluación de riesgos (R2 - riesgo MEDIO/ALTO): protege la red institucional que soporta el portal web y los sistemas de emisión.	Complementa el firewall ya contratado con controles adicionales de seguridad perimetral.
80	4.21	Seguridad de los servicios de red.	Por implementar	Si	Resultado de la evaluación de riesgos (R2): asegura los servicios de red expuestos, en especial los asociados al portal web del diario El Telégrafo.	Incluye revisión de puertos y servicios expuestos a internet.
81	4.22	Separación en las redes	Por implementar	Si	Resultado de la evaluación de riesgos (R2, R4): limita la propagación de un eventual ataque (ransomware) al segmentar las redes administrativas, de producción y de transmisión.	Considerar segmentación VLAN entre red administrativa, de transmisión y de invitados.
82	4.23	Filtrado web	Por implementar	Si	Buena práctica: reduce la exposición del personal a sitios maliciosos, principal vector de entrada de código malicioso.	Puede integrarse con el firewall ya contratado.
83	4.24	Uso de criptografía	Por implementar	Si	Obligación legal y buena práctica: protege la confidencialidad de información sensible en tránsito y en reposo, en cumplimiento de la normativa de protección de datos.	Priorizar cifrado de respaldos y comunicaciones con el portal web (HTTPS/TLS).
84	4.25	Ciclo de vida de desarrollo seguro	Por implementar	Si	Resultado de la evaluación de riesgos (R2): el portal web del diario El Telégrafo requiere un ciclo de vida de desarrollo que incorpore seguridad desde el diseño.	Aplica si existe desarrollo propio o gestión interna de cambios sobre el portal web.

85	4.26	Requisitos de seguridad de la aplicación	Por implementar	Si	Resultado de la evaluación de riesgos (R2 - riesgo MEDIO/ALTO): define requisitos mínimos de seguridad para el portal web y aplicativos institucionales.	Incluir en términos de referencia de futuros contratos de desarrollo o mantenimiento web.
86	4.27	Arquitectura del sistema seguro y principios de ingeniería	Por implementar	Si	Buena práctica: principios de arquitectura segura reducen vulnerabilidades estructurales en los sistemas institucionales.	Aplicar principalmente a nuevos desarrollos o rediseños de infraestructura.
87	4.28	Codificación Segura	Por implementar	Si	Resultado de la evaluación de riesgos (R2): reduce vulnerabilidades de código explotables en el portal web institucional.	Aplica si existe desarrollo propio; de lo contrario, exigir al proveedor estándares de codificación segura.
88	4.29	Pruebas de seguridad en el desarrollo y la aceptación	Por implementar	Si	Resultado de la evaluación de riesgos (R2 - riesgo MEDIO/ALTO): las pruebas de seguridad antes de poner en producción cambios en el portal web previenen vulnerabilidades explotables.	Incluir pruebas de seguridad como requisito de aceptación en contratos de desarrollo web.
89	4.30	Desarrollo subcontratado	Por implementar	Si	Necesidad institucional: el desarrollo y mantenimiento del portal web está subcontratado, lo que requiere gestionar el riesgo asociado a terceros.	Incluir cláusulas de seguridad y auditoría en los contratos de desarrollo subcontratado.
90	4.31	Separación de los entornos de desarrollo, prueba y producción	Por implementar	Si	Buena práctica: evita que cambios no probados afecten directamente los sistemas en producción (portal web, sistemas administrativos).	Aplica si existe desarrollo propio o ambientes de prueba gestionados internamente.
91	4.32	Gestión de cambios	Por implementar	Si	Resultado de la evaluación de riesgos (R1, R2, R4): un proceso formal de gestión de cambios reduce el riesgo de interrupciones no planificadas en sistemas críticos.	Aplica a cambios en infraestructura, sistemas y portal web.
92	4.33	Información de pruebas	Por implementar	Si	Buena práctica: evita el uso de datos reales sensibles en ambientes de prueba, reduciendo el riesgo de fuga de información.	Aplica si existen ambientes de prueba o desarrollo separados de producción.
93	4.34	Protección de los sistemas de información durante las pruebas de auditoría	Por implementar	Si	Buena práctica: protege los sistemas de información durante la ejecución de auditorías técnicas para evitar afectaciones a la operación.	Definir ventanas de mantenimiento y respaldo previos a auditorías técnicas.

FIRMAS DE RESPONSABILIDAD

FECHA DE ELABORACIÓN:		27/8/2026	
Mgs. Angel Franco Calixto OFICIAL DE SEGURIDAD DE LA INFORMACIÓN Especialista de Infraestructura, Soporte Técnico y Seguridad de la Información		FIRMA:	 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		FIRMA:	 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)		FIRMA:	 Validar únicamente en FirmaEC. Firmado electrónicamente por: OSCAR EFRAIN MIRANDA PATIN
Mgs. Grace Cordero Looor INTEGRANTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Coordinadora General de Medios		FIRMA:	 Validar únicamente en FirmaEC. Firmado electrónicamente por: GRACE VANESSA CORDERO LOOR
Espc. José Estrella Lopez INTEGRANTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Jefe de Asesoría Jurídica		FIRMA:	 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		FIRMA:	 Validar únicamente en FirmaEC. Firmado electrónicamente por: OMAR GUILLERMO BARRERA ROMERO