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 V2.0

INSTITUCIÓN / SIGLA:	CONSEJO NACIONAL PARA LA IGUALDAD DE GENERO CNIG
NÚMERO DE CONTROLES SELECCIONADOS:	53
NIVEL DE CONFIDENCIALIDAD:	1
RESPONSABLE DEL DOCUMENTO:	ROCIO BALAREZO BUSTAMANTE

ANEXO - EGSI V2.0			Estado actual del Control	Aplica Si/No	Justificación de la selección (Si) o de la exclusión (No)	Observaciones
Ítem	**Sección**	**Descripción**				
	1	**Políticas de Seguridad de la Información**				
	1.1	**Dirección de gestión de seguridad de la información**				
1	1.1.1	Políticas de Seguridad de la Información	Implementado	SI	Obligaciones legales	NA
2	1.1.2	Revisión de las políticas para la seguridad de la información	Por implementar	NO	La politica se aprobó a finales del 2020	NA
	2	**Organización de la Seguridad de la Información**				
	2.1	**Organización interna**				
3	2.1.1	Compromiso de la máxima autoridad de la institución con la seguridad de la información	Implementado	SI	Obligaciones legales	
4	2.1.2	Separación de funciones	Implementado	SI	Obligaciones legales	
5	2.1.3	Contacto con las autoridades	Por implementar	SI	Obligaciones legales	
6	2.1.4	Contacto con los grupos de interés especial	Por implementar	SI	Obligaciones legales	
7	2.1.5	Seguridad de la Información en la gestión de proyectos		NO	El Consejo no tiene priorizados proyectos	
8	2.1.6	Consideraciones de la seguridad cuando se trata con ciudadanos o clientes	Por implementar	SI	Obligaciones legales	
	2.2	**Dispositivos móviles y teletrabajo**				
9	2.2.1	Política de dispositivos móviles	Por implementar	SI	Política en elaboración	
10	2.2.2	Teletrabajo	Por implementar	SI	La modalidad de teletrabajo fue implementada en el CNIG	
	3	**Seguridad de los recursos humanos**				
	3.1	**Antes del empleo**				
11	3.1.1	Investigación de antecedentes	Por implementar	SI	Se realiza desde la UATH, hay que actualizar el procedimiento	
12	3.1.2	Términos y condiciones laborales	Por implementar	SI	Se realiza desde la UATH, hay que actualizar el procedimiento	
	3.2	Durante el empleo				
13	3.2.1	Responsabilidades de la Máxima Autoridad o su delegado	Implementado	SI	Consta en la política de seguridad de la información	
14	3.2.2	Concienciación, educación y formación en seguridad de la información	Por implementar	SI	En definición políticas	
15	3.2.3	Proceso disciplinario	Por implementar	SI	En definición políticas	
	3.3	Finalización o cambio de empleo				
16	3.3.1	Responsabilidades ante la finalización o cambio de empleo	Por implementar	SI	Se encuentra definida y en aplicación la política, se procederá a actualizar la política	
	4	**Gestión de activos**				
	4.1	Responsabilidad de los activos				
17	4.1.1	Inventario de activos	Implementado	SI	Se realiza un inventario anual, el cual esta actualizado	
18	4.1.2	Propiedad de los activos	Implementado	SI	Los activos han sido entregados mediante Acta entrega recepción individualizada	
19	4.1.3	Uso aceptable de los activos	Por implementar	SI	Elaborar política para uso de activos	
20	4.1.4	Devolución de activos	Implementado	SI	Se cuenta con una política para el efecto	
	4.2	Clasificación de la información				
21	4.2.1	Directrices de Clasificación de la información	Por implementar	SI	Se procederá con la clasificación de la información	
22	4.2.2	Etiquetado de la información	Implementado	SI	Los activos se encuentran etiquetados	
23	4.2.3	Manejo de los activos		NO	No aplica	
	4.3	Manejo de los Soportes de almacenamiento - medios				
24	4.3.1	Gestión de medios extraíbles		NO	No aplica	
25	4.3.2	Eliminación de los medios		NO	No aplica	
26	4.3.3	Transferencia de medios físicos		NO	No aplica	
	5	**Control de acceso**				
	5.1	Requisitos institucionales para el control de acceso				
27	5.1.1	Política de control de acceso	Por implementar	SI	Elaboración de política	
28	5.1.2	Acceso a redes y servicios de red	Por implementar	SI	Elaboración de política	
	5.2	Gestión de acceso de los usuarios				
29	5.2.1	Registro y retiro de usuarios	Por implementar	SI	Definir política de registro de usuarios	
30	5.2.2	Provisión de accesos a usuarios	Por implementar	SI	Definir política para otorgar claves de acceso	

31	5.2.3	Gestión de los derechos de acceso con privilegios especiales	Por implementar	SI	Definir política para otorgar claves de acceso con privilegios	
32	5.2.4	Gestión de la información confidencial de autenticación de los usuarios		NO	No contramos con un sistema de acceso a información confidencial	
33	5.2.5	Revisión de los derechos de acceso de usuario	Por implementar	SI	Política de renovación de contraseñas cada cierto tiempo	
34	5.2.6	Retiro o adaptación de los derechos de acceso	Por implementar	SI	Política para revocar acceso a personas que salen de la institución	
	5.3	Responsabilidades del usuario				
35	5.3.1	Uso de la información confidencial para la autenticación	Por implementar	SI	Politica de confidencialidad en el uso y resguardo de claves	
	5.4	Control de acceso a sistemas y aplicaciones				
36	5.4.1	Restricción del acceso a la información		NO		
37	5.4.2	Procedimientos seguros de inicio de sesión	Por implementar	SI	Procedimiento seguro de inicio de sesión	
38	5.4.3	Sistema de gestión de contraseñas	Por implementar	SI	Política de gestión de contraseñas	
39	5.4.4	Uso de herramientas de administración de sistemas	Por implementar	SI	Política de control sobre el uso de programas que puedan anular o evitar controles	
40	5.4.5	Control de acceso al código fuente del programa		NO	El Consejo no tiene programas desarrollados internamente	
	6	**Criptografía**				
	6.1	Controles criptográficos				
41	6.1.1	Política de uso de los controles criptográficos		NO	No se cuenta con el personal ni recursos para el efecto	
42	6.1.2	Gestión de Claves	Por implementar	SI		
	7	**Seguridad física y del entorno**				
	7.1	Áreas seguras				
43	7.1.1	Perímetro de seguridad física	Implementado	SI	Se cuenta con una unidad de Recepción	
44	7.1.2	Controles físicos de entrada	Por implementar	SI	Al retomar la modalidad presencial de trabajo	
45	7.1.3	Seguridad de oficinas, despachos e instalaciones		NO	El edificio en el que funciona el CNIG pertenece a la SNAI y proximanete desocuparemos	
46	7.1.4	Protección contra las amenazas externas y ambientales	Por implementar	SI	Se mnatiene vigente el equipo contraincendios, pero en virtud que las instalaciones no son propias, no contamos con recursos para realizar adecuaciones físicas, el edificio es vetusto	
47	7.1.5	Trabajo en áreas seguras		NO	El edficio no es de propiedad del CNIG, no se pueden realizar adecuaciones	
48	7.1.6	Áreas de carga y entrega	Por implementar	SI	Definir política interna para el efecto	
	7.2	Seguridad de los Equipos				
49	7.2.1	Ubicación y protección de equipos		NO	El edficio no es de propiedad del CNIG, no se pueden realizar adecuaciones	
50	7.2.2	Instalaciones de suministro		NO	La Institución no cuenta con recursos	
51	7.2.3	Seguridad del cableado		NO	El edficio no es de propiedad del CNIG, no se pueden realizar adecuaciones	
52	7.2.4	Mantenimiento de los equipos	Implementado	SI	Se realiza un plan de mantenimiento anual	
53	7.2.5	Salida de los activos fuera de las instalaciones de la institución	Implementado	SI	Se cuenta con unprocedimiento establecido para el efecto	
54	7.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Por implementar	SI	Definir política de uso	
55	7.2.7	Seguridad en la reutilización o eliminación segura de dispositivos de almacenamiento		NO	No se cuenta con dispositivos de almacenamiento externos	
56	7.2.8	Equipo informático de usuario desatendido	Por implementar	SI	Definir política de protección pantalla en reposo	
57	7.2.9	Política de puesto de trabajo despejado y pantalla limpia	Por implementar	SI	Elaboración de política	
	8	**Seguridad de las operaciones**				
	8.1	Procedimientos y responsabilidades operacionales				
58	8.1.1	Documentación de procedimientos de operación	Por implementar	SI	Definición de política	
59	8.1.2	Gestión de cambios		NO	No aplica	
60	8.1.3	Gestión de capacidades	Por implementar	SI	Definir cronograma	
61	8.1.4	Separación de ambientes de desarrollo, pruebas y producción		NO	No se cuenta con programas propios	
	8.2	Protección contra un malware				
62	8.2.1	Controles contra malware	Por implementar	SI	Elaborar política	
	8.3	Copias de seguridad				
63	8.3.1	Copias de seguridad de la información	Por implementar	SI	Elaborar política	
	8.4	Registro y monitoreo				
64	8.4.1	Registro de eventos		NO	No se cuenta con personal	
65	8.4.2	Protección de los registros de información		NO	No aplica	
66	8.4.3	Registros de administración y operación		NO	No aplica	
67	8.4.4	Sincronización de relojes	Por implementar	SI		
	8.5	Control del software en producción				
68	8.5.1	Instalación del software en sistemas en producción		NO	El CNIG no desarrolla sistemas	
	8.6	Gestión de la vulnerabilidad técnica				
69	8.6.1	Gestión de las vulnerabilidades técnicas		NO	El CNIG no desarrolla sistemas	

70	8.6.2	Restricciones en la instalación de software	Por implementar	SI	Definir política	
	8.7	Consideraciones sobre la auditoría de sistemas de información				
71	8.7.1	Controles de auditoría de sistemas de información		NO	El CNIG no desarrolla sistemas	
	9	**Seguridad en las comunicaciones**				
	9.1	Gestión de la seguridad de redes				
72	9.1.1	Controles de red	Por implementar	SI	Definir política	
73	9.1.2	Seguridad de los servicios de red	Por implementar	SI	Definir procedimientos	
74	9.1.3	Separación en las redes		no	El equipo del CNIG es limitado	
	9.2	Transferencia de información				
75	9.2.1	Políticas y procedimientos de transferencia de información	Por implementar	SI	Revisión acuerdo de confidencialidad	
76	9.2.2	Acuerdos de transferencia de información		NO	La institución no transfiere información	
77	9.2.3	Mensajería electrónica	Por implementar	SI	Política de manejo de Redes	
78	9.2.4	Acuerdos de confidencialidad o no revelación	Implementado	SI		
	10	**Adquisición, desarrollo y mantenimiento de los sistemas**				
	10.1	Requisitos de seguridad de los sistemas de información				
79	10.1.1	Análisis de requisitos y especificaciones de seguridad de la información		NO	El CNIG no maneja sistemas de información	
80	10.1.2	Asegurar los servicios de aplicaciones en redes públicas		NO	No aplica	
81	10.1.3	Controles de transacciones en línea		NO	No aplica	
	10.2	Seguridad en el desarrollo y en los procesos de soporte				
82	10.2.1	Política de desarrollo seguro		NO	El CNIG no desarrolla sistemas	
83	10.2.2	Procedimientos de control de cambios en sistemas		NO	El CNIG no desarrolla sistemas	
84	10.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo		NO	El CNIG no desarrolla sistemas	
85	10.2.4	Restricciones a los cambios en los paquetes de software		NO	El CNIG no desarrolla sistemas	
86	10.2.5	Principios de ingeniería de sistemas seguros		NO	El CNIG no desarrolla sistemas	
87	10.2.6	Ambiente de desarrollo seguro		NO	El CNIG no desarrolla sistemas	
88	10.2.7	Desarrollo externalizado		NO	El CNIG no desarrolla sistemas	
89	10.2.8	Pruebas de seguridad del sistema		NO	El CNIG no desarrolla sistemas	
90	10.2.9	Pruebas de aceptación de sistemas		NO	El CNIG no desarrolla sistemas	
	10.3	Datos de prueba				
91	10.3.1	Protección de los datos de prueba		NO	El CNIG no desarrolla sistemas	
	11	**Relaciones con proveedores**				
	11.1	Seguridad de la información en relación con los proveedores				
92	11.1.1	Política de seguridad de la información en las relaciones con los proveedores	Por implementar	SI	Desarrollo de política de acceso de proveedores y terceras personas a los activos de la institución	
93	11.1.2	Requisitos de seguridad en contratos con terceros	Por implementar	SI	Identificación y evaluación de riesgos para la información	
94	11.1.3	Cadena de suministro de tecnologías de la información y de las comunicaciones	Implementado	SI	Constan en los contratos	
	11.2	Gestión de la provisión de servicios del proveedor				
95	11.2.1	Monitoreo y revisión de los servicios de proveedores	Implementado	si	Seguimiento realizado por los administradores/as de contrato	
96	11.2.2	Gestión de cambios en los servicios de proveedores	Por implementar	SI	Actualización de políticas	
	12	**Gestión de incidentes de seguridad de la información**				
	12.1	Gestión de los incidentes de seguridad de la información y mejoras				
97	12.1.1	Responsabilidades y procedimientos	Por implementar	SI	Definición de política	
98	12.1.2	Reporte de los eventos de seguridad de la información	Por implementar	SI	Definición de política	
99	12.1.3	Reporte de debilidades de seguridad de la información	Por implementar	SI	Definición de procedimiento	
100	12.1.4	Apreciación y decisión sobre los eventos de seguridad de la información	Por implementar	SI	Definición de procedimiento	
101	12.1.5	Respuesta a incidentes de seguridad de la información	Por implementar	SI	Definición de procedimiento	
102	12.1.6	Aprendizaje de los incidentes de seguridad de la información		NO	El CNIG no reporta incidentes	
103	12.1.7	Recopilación de evidencias	Por implementar	SI	Definición del procedimiento	
	13	**Aspectos de seguridad de la información para la gestión de la continuidad del negocio**				
	13.1	Continuidad de seguridad de la información				
104	13.1.1	Planificación de la continuidad de seguridad de la información	Por implementar	SI	Definición de procedimiento	
105	13.1.2	Implementación de la continuidad de seguridad de la información	Por implementar	SI	Definición de procedimiento	
106	13.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información		NO	No se cuenta con el personal ni recursos para el efecto	
	13.2	Redundancias				
107	13.2.1	Disponibilidad de las instalaciones de procesamiento de la información		NO	El CNIG no procesa información	
	14	**Cumplimiento**				
	14.1	Cumplimiento de los requisitos legales y contractuales				
108	14.1.1	Identificación de la legislación aplicable y de los requisitos contractuales		NO	El CNIG no tiene sistemas de información	
109	14.1.2	Derechos de propiedad intelectual	Por implementar	si	Definir política	
110	14.1.3	Protección de los registros		NO	No aplica	
111	14.1.4	Protección y privacidad de la información de carácter personal		NO	El CNIG no tiene sistemas de información	
112	14.1.5	Reglamentos de controles criptográficos		NO	No aplica	
	14.2	Revisiones de seguridad de la información				
113	14.2.1	Revisión independiente de seguridad de la información	Por implementar	SI	Establecer proceso	
114	14.2.2	Cumplimiento de las políticas y normas de seguridad		NO	El CNIG no tiene sistemas de información	

115	14.2.3	Comprobación del cumplimiento técnico		NO	El CNIG no tiene sistemas de información	

FIRMAS DE RESPONSABILIDAD	
FECHA DE ELABORACIÓN:	
NOMBRE DEL OFICIAL DE SEGURIDAD: **ROCÍO DEL PILAR BALAREZO BUSTAMANTE**	**FIRMA:** Firmado digitalmente porROCIO DEL PILAR BALAREZO BUSTAMANTE DN: cn=ROCIO DEL PILAR BALAREZO BUSTAMANTE c=EC o=SECURITY DATA S.A. ou=ENTIDAD DE CERTIFICACION DE INFORMACION
NOMBRE DEL REPRESENTANTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN: **ROCIO DEL PILAR BALAREZO BUSTAMANTE**	**FIRMA:**
NOMBRE DEL PROPIETARIO DE LA INFORMACIÓN: **ROCIO DEL PILAR BALAREZO BUSTAMANTE**	**FIRMA:**