PROYECTO:

"IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V2)"

UNIDAD RESPONSABLE

Planificación y Gestión Estratégica

PERÍODO DE EJECUCIÓN

2020-2021

1.- PROBLEMA

Los sistemas desarrollados y aplicaciones utilizadas en la institución no cuentan con una política de seguridad, ni requerimientos básicos para su parametrización a nivel de seguridad informática y de la información. Las reglas establecidas espontáneamente por la unidad de Tecnologías de la Información no fueron socializadas y avaladas por la Máxima Autoridad, dejando a la institución inmersa en un proceso improvisado para asignar permisos, accesos y restricciones a la infraestructura, paquetes y sistemas informáticos, así como a la información siendo una gran debilidad para la unidad de Gestión de TI . Actualmente no se cuenta con una política de seguridad de la información aprobada que permita establecer los parámetros apropiados para salvaguardar la confidencialidad, disponibilidad e integridad de la infraestructura tecnológica, aplicaciones e información institucional.

2.- OBJETIVO GENERAL

El presente proyecto tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información del Consejo Nacional para la Igualdad de Género, mediante la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI V2) y el cumplimiento de 127 hitos, conforme se establece en el Acuerdo Ministerial 025-2019 publicado en el registro oficial del 10 de enero de 2020.

3.- JUSTIFICACIÓN

La implementación del EGSI V2.0 reducirá significativamente amenazas, riesgos y vulnerabilidades relacionadas a la gestión de la información, tanto física como

electrónica, que procesa la institución. Así mismo, contribuirá a establecer un proceso de mejora continua de la gestión de la seguridad de la información y crear cultura y conciencia en los/as servidores/as públicos/as en cuanto al manejo de la información que utilizan para cumplir sus funciones, sea esta, institucional o de la ciudadanía.

4.- BENEFICIARIOS/AS

Entidades públicas o privadas, servidores públicos, Gobierno, Ciudadanía.

5.- OBJETIVOS ESPECÍFICOS

a) Identificar, cuantificar y priorizar las amenazas, riesgos y vulnerabilidades que puedan afectar la seguridad de la información de la entidad.
b) Proporcionar a las autoridades herramientas e insumos adecuados que faciliten la toma de decisiones mediante una gestión de seguridad de la información, en concordancia con la constitución, leyes y demás normativas legales vigentes.
c) Contar con estructuras de evaluación y gestión de riesgos en la organización, así como la definición de las responsabilidades individuales de cada miembro a nivel de seguridad, con los respectivos acuerdos de confidencialidad.
d) Crear conocimiento, conciencia y cultura de los servidores públicos en cuanto a la gestión de la seguridad de la información que utilizan. Implementar acciones preventivas para evitar una mala gestión de la seguridad de la información y sus posibles consecuencias.
e) Compartir información y gestionar incidentes de seguridad de la información que afecten a la entidad o al gobierno en su conjunto en coordinación con la MINTEL.

6.- DESCRIPCIÓN DEL PROYECTO

El presente proyecto tiene como objetivo cumplir con los 127 hitos establecidos en GPR que corresponde a los requisitos y controles que comprende la implementación del Esquema Gubernamental de Seguridad de

la Información (EGSI V2) conforme se establece en el Acuerdo Ministerial 025-2019 publicado en el registro oficial del 10 de enero de 2020.

Los requisitos y controles a implementar y que han sido homologadas como hitos del proyecto tienen un plazo de ejecución de 15 meses.

La implementación del EGSI V2.0 reducirá significativamente amenazas, riesgos y vulnerabilidades relacionadas a la gestión de la información, tanto física como electrónica, que procesa la institución. Así mismo, contribuirá a establecer un proceso de mejora continua de la gestión de la seguridad de la información e incrementar la cultura de los servidores públicos en cuanto al manejo de la información que utilizan para cumplir sus funciones sea esta institucional o de la ciudadanía.

7.- ESPECIFICACIONES TÉCNICAS

Aplicar los estándares internacionales (ISO/IEC 27000) adoptados como normas técnicas ecuatorianas para la gestión de la seguridad de la información y cumplir con los 127 hitos que corresponde a los requisitos y controles que comprende la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI V2), aplicables a los procesos relacionados directamente con la prestación de los servicios del CNIG, dentro de la cadena de valor de este Consejo en concordancia con el modelo de gestión vigente.

8.- RIESGOS

a) El no cumplimiento de los hitos de control del proyecto causaría la no aplicación del acuerdo Ministerial 025-2019.

b) La falta de asignación de recursos requeridos para la implementación del EGSI causaría la ejecución parcial o no ejecución del proyecto.

9.- PLAZOS

El MINTEL socializóla versión 2 del EGSI y el Consejo inició la ejecución de algunas actividades, con la finalidad de dar cumplimiento a las estipulaciones del ente de control, por lo que se han llevado a cabo varias acciones durante los meses de febrero a septiembre de 2021.

Se planifica la ejecución del presente proyecto desde septiembre de 2020 a julio de 2021, el cronograma de principales hitos detalla la fecha de cumplimiento, el entregable y medio de verificación

10.- CRONOGRAMA DE HITOS

#	Fase/Hito[1]	Tiempo Estimado	Unidad/Cargo	Entregable[2]	Medio de Verificación
FASE 1 (5 MESES)					
1	Perfil de proyecto	30/09/2020	UP/OSI	Acta de proyecto	Acta
2	Definición del Alcance del EGSI versión 2.0	30/09/2020	OSI	Alcance EGSI en el CNIG	Documento alcance
3	Política de Seguridad de la Información	08/10/2020	SECRETARIA TÉCNICA	Política de Seguridad de la Información	Resolución
4	Metodología de evaluación y tratamiento del riesgo	23/10/2020	OSI	Metodología	Instrumentos técnicos
5	Plan de Comunicación y Sensibilización del EGSI versión 2.0	29/10/2020	UCS	Plan	Acta de socialización del plan
6	Informe de la Evaluación de los Riesgos	01/12/2020	OSI	Informe de evaluación de riegos	Quipux de envío de informe al MINTEL
FASE 2 (7 MESES)					
7	Declaración de Aplicabilidad (SoA)	15/12/2020	OSI	SOA	Plan de aplicabilidad
8	Plan de Tratamiento de los riesgos	15/12/2020	OSI	Plan de riesgos	Plan aprobado
9	Procedimiento de comprobación del cumplimiento técnico	26/05/2021	UTI/OSI	Reporte mensual de comprobación	Reporte
10	Plan de auditoría Interna	01/06/2021	UP/OSI	Plan de auditoría	Plan
11	Informe de los resultados de la revisión del EGSI	15/06/2021	CSI	Informe resultados revisión CSI	Informe
12	Informe de los resultados de las medidas correctivas aplicadas	22/06/2021	OSI	EGSI implementado	Informe

[1] Hito: es una tarea que simboliza el haber conseguido un logro importante en el proyecto.
[2] Entregable: Es un producto tangible o intangible producido como resultado del proyecto. Un entregable es cualquier producto, resultado o capacidad de prestar un servicio, único y verificable, que debe producirse para terminar un proceso, una fase o un proyecto. Un entregable puede ser un informe, un documento, una parte del programa.

13	Informe de cierre	15/07/2021	OSI	Informe de Cierre	Informe de cierre

SIGLAS[3]

11.- PRESUPUESTO

Grado	Número	Cargo	Remuneración Mensual	# meses	Remuneración total
SP2	1	Analista de Tecnologías de la Información	901 USD	25% del tiempo por 11 meses	2.477,75 USD
SP7	1	Analista de Planificación	1.676 USD	25% del tiempo por 11 meses	4.609,00 USD
SP5	1	Analista de Comunicación	1.212 USD	25% del tiempo por 1 mes	303,00 USD
				TOTAL	7.389,75 USD

12.- APROBACIÓN

INSTANCIA	SERVIDORA	CARGO	FIRMA
Aprobado por:	NELLY JACOME VILLALVA	SECRETARIA TÉCNICA CNIG	
Validado por:	INTEGRANTES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Según Acta No. 4, del 30 de septiembre de 2020
Elaborado por:	ROCÍO BALAREZO B.	RESPONSABLE DE PLANIFICACIÓN	

[3] UP Unidad de Planificación; OSI Oficial de Seguridad de la información; UCS, Unidad de Comunicación Social; UTI, Unidad de Tecnologías de la Información; y, CSI Comité de Seguridad de la Información

13.- ANEXOS

HITOS DE CONTROL

DEFINICIÓN: 0.0.1 Perfil de proyecto "Implementación EGSI versión 2.0", aprobado
PLANEACIÓN: 0.0.2 Definición del Alcance del EGSI, aprobado.
PLANEACIÓN: 0.0.3 Política de Seguridad de la información, aprobado.
PLANEACIÓN: 0.0.4 Metodología de evaluación y tratamiento del riesgo, aprobado.
PLANEACIÓN: 0.0.5 Plan de Comunicación y Sensibilización del EGSI versión 2.0, aprobado.
EJECUCIÓN: 0.0.6 Informe de la Evaluación de los Riesgos, aprobado.
EJECUCIÓN: 0.0.7 Declaración de Aplicabilidad (SoA), aprobado.
EJECUCIÓN: 0.0.8 Plan de Tratamiento de los riesgos, aprobado.
EJECUCIÓN: 1.1.1 Políticas de Seguridad de la Información, documentadas
EJECUCIÓN: 1.1.2 Revisión de las políticas para la seguridad de la información, actualizada.
EJECUCIÓN: 2.1.1 Compromiso de la máxima autoridad de la institución con la seguridad de la información, documentado e implementado.
EJECUCIÓN: 2.1.2 Separación de funciones, documentado e implementado.
EJECUCIÓN: 2.1.3 Contacto con las autoridades, documentado e implementado.
EJECUCIÓN: 2.1.4 Contacto con los grupos de interés especial, documentado e implementado.
EJECUCIÓN: 2.1.5 Seguridad de la Información en la gestión de proyectos, verificado.
EJECUCIÓN: 2.1.6 Consideraciones de la seguridad cuando se trata con ciudadanos o clientes, identificados.
EJECUCIÓN: 2.2.1 Política de dispositivos móviles, documentada e implementada.
EJECUCIÓN: 2.2.2 Política de Teletrabajo y medidas de seguridad, documentada implementada.
EJECUCIÓN: 3.1.1 Procedimiento para verificar antecedentes, documentado e implementado.
EJECUCIÓN: 3.1.2 Términos y condiciones laborales, firmados.
EJECUCIÓN: 3.2.1 Responsabilidades de la Máxima Autoridad o su delegado, socializadas.
EJECUCIÓN: 3.2.2 Plan de Concienciación, educación y formación en seguridad de la información, documentado e implementado.
EJECUCIÓN: 3.2.3 Proceso disciplinario, garantizado y socializado.
EJECUCIÓN: 3.3.1 Responsabilidades ante la finalización o cambio de empleo, definidas y comunicadas.
EJECUCIÓN: 4.1.1 Inventario de activos, actualizado.
EJECUCIÓN: 4.1.2 Propiedad de los activos, asignado.
EJECUCIÓN: 4.1.3 Uso aceptable de los activos, documentado e implementado.
EJECUCIÓN: 4.1.4 Devolución de activos, documentado e implementado.
EJECUCIÓN: 4.2.1 Clasificación de la información, documentada.
EJECUCIÓN: 4.2.2 Etiquetado de la información, documentado e implementado.
EJECUCIÓN: 4.2.3 Manejo de los activos, documentado e implementado.
EJECUCIÓN: 4.3.1 Gestión de medios extraíbles, documentado e implementado.
EJECUCIÓN: 4.3.2 Procedimiento de eliminación de los medios, documentado e implementado.
EJECUCIÓN: 4.3.3 Transferencia de medios físicos, documentado e implementado.
EJECUCIÓN: 5.1.1 Política de control de acceso, documentada e implementada.

EJECUCIÓN: 5.1.2 Acceso a redes y servicios de red, difundido.
EJECUCIÓN: 5.2.1 Registro y retiro de usuarios, documentado e implementado.
EJECUCIÓN: 5.2.2 Provisión de accesos a usuarios, documentado e implementado.
EJECUCIÓN: 5.2.3 Gestión de los derechos de acceso con privilegios especiales, documentado e implementado.
EJECUCIÓN: 5.2.4 Gestión de la información confidencial de autenticación de los usuarios, documentado e implementado.
EJECUCIÓN: 5.2.5 Derechos de acceso de usuario, revisado.
EJECUCIÓN: 5.2.6 Retiro o adaptación de los derechos de acceso, documentado e implementado.
EJECUCIÓN: 5.3.1 Uso de la información confidencial para la autenticación, documentado e implementado.
EJECUCIÓN: 5.4.1 Restricción del acceso a la información, implementado.
EJECUCIÓN: 5.4.2 Procedimientos seguros de inicio de sesión, documentados e implementados.
EJECUCIÓN: 5.4.3 Política para la gestión de contraseñas, documentada e implementada.
EJECUCIÓN: 5.4.4 Uso de herramientas de administración de sistemas, documentado e implementado.
EJECUCIÓN: 5.4.5 Control de acceso al código fuente del programa, implementado.
EJECUCIÓN: 6.1.1 Política de uso de los controles criptográficos, documentada e implementada.
EJECUCIÓN: 6.1.2 Política para la Gestión de Claves, documentada e implementada.
EJECUCIÓN: 7.1.1 Perímetro de seguridad física, definido y documentado e implementado.
EJECUCIÓN: 7.1.2 Controles físicos de entrada, implementados.
EJECUCIÓN: 7.1.3 Seguridad de oficinas, despachos e instalaciones, implementado.
EJECUCIÓN: 7.1.4 Protección contra las amenazas externas y ambientales, implementado.
EJECUCIÓN: 7.1.5 Procedimiento para trabajo en áreas seguras, documentado e implementado.
EJECUCIÓN: 7.1.6 Áreas de carga y entrega, implementado.
EJECUCIÓN: 7.2.1 Ubicación y protección de equipos, implementado.
EJECUCIÓN: 7.2.2 Instalaciones de suministro de energía sin interrupción, implementado.
EJECUCIÓN: 7.2.3 Seguridad del cableado (eléctrico y telecomunicaciones), implementado.
EJECUCIÓN: 7.2.4 Plan de Mantenimiento de los equipos, documentado e implementado.
EJECUCIÓN: 7.2.5 Salida de los activos fuera de las instalaciones de la institución, documentado e implementado.
EJECUCIÓN: 7.2.6 Seguridad de los equipos y activos fuera de las instalaciones, implementado.
EJECUCIÓN: 7.2.7 Seguridad en la reutilización o eliminación segura de dispositivos de almacenamiento, implementado.
EJECUCIÓN: 7.2.8 Equipo informático de usuario desatendido, protección implementada.
EJECUCIÓN: 7.2.9 Política de puesto de trabajo despejado y pantalla limpia, documentado e implementado.
EJECUCIÓN: 8.1.1 Procedimientos de operación, documentados e implementados.
EJECUCIÓN: 8.1.2 Procedimiento para la Gestión de cambios, documentado e implementado.
EJECUCIÓN: 8.1.3 Monitoreo y ajuste de capacidades, documentado e implementado.
EJECUCIÓN: 8.1.4 Separación de ambientes de desarrollo, pruebas y producción, documentado e implementado.
EJECUCIÓN: 8.2.1 Controles contra malware, documentado e implementado.
EJECUCIÓN: 8.3.1 Política de respaldos y copias de seguridad de la información, documentada e implementada.
EJECUCIÓN: 8.4.1 Registro de eventos, documentado e implementado.
EJECUCIÓN: 8.4.2 Procedimiento para la protección de los registros de información, documentado e implementado.

EJECUCIÓN: 8.4.3 Registros de administración y operación, documentado e implementado.
EJECUCIÓN: 8.4.4 Sincronización de relojes, implementado.
EJECUCIÓN: 8.5.1 Procedimiento para la instalación de software en sistemas en producción, documentado e implementado.
EJECUCIÓN: 8.6.1 Política de monitoreo continuo, gestión de las vulnerabilidades técnicas, documentada e implementada.
EJECUCIÓN: 8.6.2 Política para la restricción en la instalación de software, documentada e implementada.
EJECUCIÓN: 8.7.1 Controles de auditoría de sistemas de información, documentado e implementado.
EJECUCIÓN: 9.1.1 Administración y control de las redes para proteger la información, implementado.
EJECUCIÓN: 9.1.2 Seguridad de los servicios de red, implementado.
EJECUCIÓN: 9.1.3 Separación en las redes, documentado e implementado.
EJECUCIÓN: 9.2.1 Políticas y procedimientos de transferencia de información, documentado e implementado.
EJECUCIÓN: 9.2.2 Acuerdos de transferencia de información, documentados e implementados.
EJECUCIÓN: 9.2.3 Políticas y Procedimientos para mensajería electrónica, documentados e implementados.
EJECUCIÓN: 9.2.4 Acuerdos de confidencialidad o no revelación, elaborados y firmados.
EJECUCIÓN: 10.1.1 Análisis de requisitos y especificaciones de seguridad de la información, documentado e implementado.
EJECUCIÓN: 10.1.2 Servicios de aplicaciones en redes públicas, asegurados e implementados.
EJECUCIÓN: 10.1.3 Controles de transacciones en línea, implementados.
EJECUCIÓN: 10.2.1 Política de desarrollo seguro, documentada e implementada.
EJECUCIÓN: 10.2.2 Procedimientos de control de cambios en sistemas, documentados e implementados.
EJECUCIÓN: 10.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo, implementada.
EJECUCIÓN: 10.2.4 Restricciones a los cambios en los paquetes de software, documentado e implementado.
EJECUCIÓN: 10.2.5 Principios de ingeniería de sistemas seguros, documentado e implementado.
EJECUCIÓN: 10.2.6 Ambiente de desarrollo seguro, implementado.
EJECUCIÓN: 10.2.7 Desarrollo externalizado, supervisado y monitoreado.
EJECUCIÓN: 10.2.8 Pruebas de seguridad del sistema, documentado e implementado.
EJECUCIÓN: 10.2.9 Pruebas de aceptación de sistemas, documentado e implementado.
EJECUCIÓN: 10.3.1 Protección de los datos de prueba, implementado.
EJECUCIÓN: 11.1.1 Política de seguridad de la información en las relaciones con los proveedores, documentada e implementada.
EJECUCIÓN: 11.1.2 Requisitos de seguridad en contratos con terceros, documentados e implementados.
EJECUCIÓN: 11.1.3 Requisitos de Seguridad en la cadena de suministro de tecnologías de la información y de las comunicaciones, documentados e implementados.
EJECUCIÓN: 11.2.1 Monitoreo y revisión de los servicios de proveedores, documentado e implementado.
EJECUCIÓN: 11.2.2 Proceso de Gestión de cambios en los servicios de proveedores, documentado e implementado.
EJECUCIÓN: 12.1.1 Responsabilidades y procedimientos en la Gestión de Incidentes de Seguridad de la Información, documentado e implementado.
EJECUCIÓN: 12.1.2 Reporte de los eventos de seguridad de la información, documentado e implementado.
EJECUCIÓN: 12.1.3 Reporte de debilidades de seguridad de la información, documentado e implementado.
EJECUCIÓN: 12.1.4 Apreciación y decisión sobre los eventos de seguridad de la información, documentado e implementado.
EJECUCIÓN: 12.1.5 Procedimiento de respuesta a incidentes de seguridad de la información, documentado e implementado.

EJECUCIÓN: 12.1.6 Aprendizaje de los incidentes de seguridad de la información, implementado.
EJECUCIÓN: 12.1.7 Procedimiento para la recopilación de evidencias, documentado e implementado.
EJECUCIÓN: 13.1.1 Planificación de la continuidad de seguridad de la información, documentado e implementado.
EJECUCIÓN: 13.1.2 Continuidad de seguridad de la información, implementado.
EJECUCIÓN: 13.1.3 Controles de continuidad de seguridad de la información, verificado, revisado y evaluado.
EJECUCIÓN: 13.2.1 Disponibilidad de las instalaciones de procesamiento de la información, implementado.
EJECUCIÓN: 14.1.1 Identificación de la legislación aplicable y de los requisitos contractuales, documentado e implementado.
EJECUCIÓN: 14.1.2 Procedimiento para el cumplimiento de derechos de propiedad intelectual, documentado e implementado.
EJECUCIÓN: 14.1.3 Procedimiento para la protección de los registros, documentado e implementado.
EJECUCIÓN: 14.1.4 Política de protección y privacidad de la información de carácter personal, documentado e implementado.
EJECUCIÓN: 14.1.5 Reglamento de controles criptográficos, documentado e implementado.
EJECUCIÓN: 14.2.1 Revisión independiente de seguridad de la información, documentado e implementado.
EJECUCIÓN: 14.2.2 Cumplimiento de las políticas y normas de seguridad, documentado e implementado.
EJECUCIÓN: 14.2.3 Procedimiento de comprobación del cumplimiento técnico, documentado e implementado.
EJECUCIÓN: 0.0.9 Plan de auditoría Interna, documentado.
EJECUCIÓN: 0.0.10 Informe de los resultados de la revisión del EGSI por parte del CSI, documentado.
EJECUCIÓN: 0.0.11 Informe de los resultados de las medidas correctivas aplicadas, documentado.
CIERRE: 0.0.12 Informe de cierre del proyecto "Implementación EGSI versión 2.0", aprobado.