INSTITUTO NACIONAL DE BIODIVERSIDAD

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

2021

Dir.: Pje. Rumipamba 341 y Av. De los Shyris **Telf.:** (+593) 22449-825
E-mail: info@biodiversidad.gob.ec - www.inabio.biodiversidad.gob.ec

ÍNDICE

FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

	Nombre / Cargo	Firma	Fecha
Elaborado:	Rosa Bolaños Ibujés **OFICIAL DE SEGURIDAD DE LA INFORMACIÓN**	ROSA ELVIRA BOLANOS IBUJES Firmado digitalmente por ROSA ELVIRA BOLANOS IBUJES Fecha: 2021.07.09 10:33:26 -05'00'	30 junio 2021
Revisado por:	Ma. Belén Montenegro **PRESIDENTA COMITÉ DE SEGURIDAD DE LA INFORMACIÓN**	Firmado electrónicamente por: **MARIA BELEN MONTENEGRO RODRIGUEZ**	30 junio 2021
Aprobado por:	Diego Inclán Luna **DIRECTOR EJECUTIVO**	Firmado electrónicamente por: **DIEGO JAVIER**	30 junio 2021

CONTROL E HISTORIAL DE CAMBIOS

Versión	Descripción del Cambio	Fecha de Actualización
1.0	Versión Inicial	18 junio 2020
2.0	Versión elaborada durante la implementación del EGSI V 2.0	30 junio 2021

1. ANTECEDENTES

Mediante Decreto Ejecutivo No. 245 de 24 de febrero de 2014, se crea el Instituto Nacional de Biodiversidad, adscrito al Ministerio del Ambiente[1], con personalidad jurídica de derecho público, con independencia funcional, administrativa, financiera y presupuestaria, con jurisdicción nacional.

Mediante Registro Oficial No. 228 de 10 de enero de 2020, se expide el Esquema Gubernamental de Seguridad de la Información –EGSI-, el cual es de implementación obligatoria en las instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

2. Política de seguridad de la información

2.1 Descripción de la política

El Instituto Nacional de Biodiversidad –INABIO-, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información con el objetivo de establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y la visión del Instituto.

Para el INABIO, la información es uno de sus principales activos, su protección busca la disminución del impacto generado por los riesgos identificados de manera sistemática, con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde a las necesidades de los diferentes grupos de interés identificados.

Los usuarios, proveedores y todos aquellos que tengan responsabilidad sobre las fuentes, repositorios y recursos de procesamiento de la información del INABIO, deben adoptar los lineamientos contenidos en el presente documento y otros relacionados con él.

2.2 Objetivos

- Fortalecer la cultura de seguridad de la información en los usuarios, proveedores y

[1] Actual Ministerio del Ambiente Agua y Transición Ecológica

personas relacionadas con el Instituto Nacional de Biodiversidad.

- Adoptar y difundir las políticas de seguridad de la información en cumplimiento de la normativa legal vigente.
- Proteger sus activos de información de amenazas y vulnerabilidades internas y externas deliberadas o accidentales.
- Normar el uso adecuado de los equipos y herramientas informáticas que el Instituto Nacional de Biodiversidad provee al usuario.
- Proteger el prestigio y el buen nombre del Instituto Nacional de Biodiversidad.

2.3 Roles y responsabilidades

- La máxima autoridad a través del Comité de Seguridad de la Información –CSI-, conformado por los responsables o delegados de las áreas de Talento Humano, Administrativa, Planificación y Gestión Estratégica, Comunicación Social, Tecnologías de la Información, áreas agregadoras de valor y Asesoría Jurídica que participa como asesor, es la responsable de garantizar que la seguridad de la información se gestiona adecuadamente en todo el Instituto.
- Cada funcionario líder de área es responsable de garantizar que los usuarios que laboran bajo su control protejan la información de acuerdo con las normas establecidas por el Instituto.
- El Oficial de Seguridad de la Información –OSI- asesora al equipo directivo, proporciona apoyo especializado al personal del Instituto y garantiza que los informes sobre la situación de la seguridad de la información estén disponibles.
- Cada uno de los usuarios del Instituto, tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

2.4 Alcance y usuarios

La Política de Seguridad de la Información del INABIO, establece lineamientos de actuación para los usuarios que laboran en la entidad, en relación con los recursos y servicios de información.

Esta política debe ser acatada por todos los usuarios y personas relacionadas con el INABIO que hagan uso de los recursos tecnológicos provistos por el Instituto, o que dispongan de sistemas o redes conectadas directa o indirectamente a su red, así como proveedores que desempeñen labores o proporcionen algún tipo de servicio al Instituto.

La aplicación de esta política tiene el carácter de obligatorio para todos los usuarios que en cualquier modalidad contractual presten servicios a la institución, su incumplimiento será objeto del régimen disciplinario correspondiente.

2.5 Comunicación de la política

El Instituto Nacional de Biodiversidad, garantizará que los usuarios y ciudadanía en general, conozcan la política de seguridad utilizando los mecanismos de comunicación disponibles, como sistema de gestión documental, correo electrónico institucional, portales web y otros.

3. Políticas

3.1 Política general de la información

- El Instituto Nacional de Biodiversidad es el propietario de los datos e información que se deriven de cualquier actividad o trabajo de investigación que realicen los usuarios o personas con quienes el INABIO mantenga una relación o dependencia.
- Con la finalidad de asegurar que la información del INABIO sea administrada de manera adecuada y segura de acuerdo con sus intereses. Los usuarios, proveedores o personas con quienes se establezca algún tipo de relación o dependencia, deben firmar un documento o acuerdo, en el que se determine claramente la propiedad y confidencialidad, que sobre esta información mantiene el Instituto.
- Se prohíbe la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información, propiedad del INABIO.

3.2 Seguridad física y del entorno

- El acceso físico a las instalaciones del INABIO, no es libre, es controlado las 24 horas del día, los 365 días del año.
- Las ventanas y puertas de acceso a las oficinas deben permanecer cerradas, especialmente cuando no haya vigilancia.
- Para los usuarios que mantienen relación de dependencia con el Instituto, es obligatorio el uso de la credencial de identificación cuando se encuentren en las instalaciones del INABIO. En caso de pérdida de la identificación, se debe notificar inmediatamente a la Unidad Administrativa de Talento Humano.
- Está prohibido el ingreso de personas ajenas a la institución sin la autorización de la

Dirección Ejecutiva o subdirector, en coordinación con el Jefe de la Dirección correspondiente. A las personas autorizadas, se les otorgará una identificación temporal que permita identificar las áreas físicas en las cuales puede permanecer durante su estadía, deben estar acompañadas por un responsable del INABIO y será registrada su hora de ingreso y salida.

- Se prohíbe el ingreso y/o instalación de hardware personal o dispositivos externos, sin la debida autorización del jefe inmediato y sin conocimiento de TIC's.
- No se permite ninguna acción que pueda causar daño físico en los equipos informáticos o infraestructura de datos.
- La protección de los sistemas informáticos no es sólo responsabilidad de TIC's, sino también de los usuarios finales.
- Está prohibido fumar, ingerir alimentos y/o bebidas en los sitios donde están ubicados los equipos informáticos, almacenamiento de datos, copiadoras/impresoras y de comunicaciones.
- La pérdida o robo de cualquier componente de hardware o software debe ser reportado a la Dirección Administrativa Financiera - DAF y TIC's inmediatamente detectado el incidente.
- Ningún equipo tecnológico que pertenece al Instituto puede moverse o ser reubicado, sin la respectiva autorización del jefe inmediato y en coordinación con TIC's. Para movilizar un equipo fuera del Instituto se requiere autorización de la Dirección Ejecutiva.
- Está prohibido conectar cafeteras, microondas, calefactores o algún equipo similar sin la respectiva autorización de la DAF.
- El mobiliario donde se guardan los activos de información contará con las seguridades del caso para evitar la pérdida, robo o destrucción de la información.
- El personal del INABIO podrá permanecer en las instalaciones del Instituto durante el horario autorizado. Quien deba permanecer fuera del horario habitual, deberá contar con la respectiva autorización de los jefes inmediatos.
- Establecer un sistema de suministro de energía sin interrupción (UPS) o al menos permitir el cierre/apagado ordenado de los servicios y equipos que soportan las operaciones de los servicios informáticos de la Institución.
- Se deberá mantener barreras físicas y de procedimientos que impidan el acceso a las áreas restringidas, pudiendo ingresar solamente el personal autorizado a ellas respetando el debido proceso de identificación.

- Los extintores, deben mantenerse en lugares estratégicos para su uso en caso de una emergencia, considerar el respectivo mantenimiento, recarga o adquisición según corresponda cada año.

3.3 Gestión de los activos de información

3.3.1 Uso del computador y equipos informáticos

- Es responsabilidad del usuario, el cuidado externo, buen uso y limpieza de los equipos tecnológicos que le han sido asignados como herramientas de trabajo.
- Los equipos del Instituto deben usarse únicamente para actividades de trabajo y no para otros fines como juegos, pasatiempos o personales.
- Los equipos que se encuentren desatendidos deben ser bloqueados para evitar su uso no autorizado.
- Es obligación de los usuarios apagar los equipos (monitor y computadora) asignados, una vez que termina su jornada de trabajo.
- Está restringido el uso de dispositivos extraíbles, discos externos, cámaras, equipos de video y audio, dispositivos móviles, etc. Para su uso debe existir la respectiva aprobación por parte de los jefes inmediatos.
- Se debe utilizar únicamente el software autorizado e instalado por TIC´s, para lo cual se respetarán los procedimientos establecidos de soporte técnico.
- El uso de equipos informáticos de propiedad privada debe ser autorizado por el jefe inmediato del área a donde ingresan, notificado al OSI y, controlado y monitoreado por TIC´s.
- Los usuarios no pueden abrir los equipos tecnológicos y hacer cambios no autorizados en el hardware y/o software. Si el usuario estima que su equipo requiere algún tipo de arreglo o cambio, debe solicitar soporte técnico de TIC’s.
- Es responsabilidad de los usuarios el uso apropiado del servicio telefónico, se debe utilizar este sistema sólo para llamadas de carácter laboral. El Instituto, a través del OSI, verificará periódicamente el buen uso de este recurso.
- Es responsabilidad de los usuarios, el uso apropiado de los recursos de impresión, scanner, plotter y copiadoras únicamente para actividades institucionales.

3.3.2 Acceso y uso de la información

- El ingreso a la red informática del INABIO, se realizará utilizando un login de usuario asignado por TIC's, y una clave personal definida por cada usuario, cuya custodia y uso es de su exclusiva responsabilidad.
- Las contraseñas creadas por los usuarios, para los accesos a los servicios informáticos, deben contener letras mayúsculas, minúsculas, caracteres especiales y números, de una longitud mínima de 8 caracteres.
- El usuario debe guardar su contraseña, no debe escribirla en papel y dejarla en sitios donde pueda ser encontrada.
- TIC's debe cambiar las contraseñas predefinidas que traen los equipos nuevos tales como ruteadores, cortafuegos, etc., inmediatamente al ponerlos en operación.
- TIC's debe definir mecanismos que aseguren la confidencialidad de la información transmitida por los canales de conexión remota, mediante técnicas como encriptación de datos, redes virtuales privadas y otros.
- El buen uso de los accesos y contraseñas otorgadas para los sistemas institucionales y de gobierno electrónico (correo electrónico institucional, Quipux, entre otros), es de exclusiva responsabilidad de los usuarios a quienes han sido otorgadas.
- La custodia de la información almacenada y requerida para ejecutar sus actividades diarias, es responsabilidad de cada usuario, por lo tanto, a través de su jefe inmediato se debe coordinar con TIC´S, la obtención periódica de respaldos de los datos críticos.
- Previo al uso de dispositivos extraíbles o software que provenga de fuera del INABIO, debe ejecutarse un análisis con el antivirus corporativo.
- La solicitud de acceso a información que no es competencia del usuario debe ser autorizada por el custodio de esta.
- Los usuarios que utilicen equipos de impresión deben tener el cuidado de retirar inmediatamente los documentos para evitar que alguna persona no autorizada tenga acceso a esta información.
- Es responsabilidad de los directores, la concientización de los usuarios, sobre la seguridad de la información que es parte de sus funciones y responsabilidades dentro del INABIO.
- Una vez finalizada la relación de dependencia laboral entre el usuario y el INABIO, es responsabilidad de cada director, aplicar los debidos procesos para garantizar que toda la información generada y procesada por el exusuario, sea respaldada y

verificada, con su respectiva acta de entrega y recepción.

- No está permitido realizar de forma intencionada acciones cuya finalidad sea la obtención de contraseñas, la obtención de información ajena o sobrepasar los sistemas de protección de datos y de seguridad informática. Esto incluye, el uso de sniffers, software de escaneo de puertos y búsqueda de vulnerabilidades, entre otros.
- Los usuarios serán creados en los Sistemas de Gobierno Electrónico de acuerdo con las necesidades y perfiles requeridos, previa autorización de Talento Humano.
- La Unidad de Administración de Talento Humano deberá brindar una inducción a los nuevos usuarios que se integran a la Institución, donde expliquen con el apoyo del OSI, las funciones, responsabilidades respecto a la seguridad de la información, acceso a la información, uso de contraseñas con sistemas de información confidencial.
- El control de acceso a la información se realizará a través de roles que administren los privilegios de los usuarios de cada sistema, aplicativo o servicio, mismos que deben contar en un registro incluido con acceso solo a personal de tecnología autorizado.
- El INABIO con el apoyo del OSI, implementará un procedimiento formal para el reporte de eventos de seguridad informáticos junto al procedimiento de escalada y respuesta al incidente que amenace la seguridad informática.

3.3.3 Uso del correo institucional

- Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en el Instituto y no debe utilizarse para fines particulares.
- Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.
- Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.
- Todo usuario es responsable de la eliminación de los mensajes con origen desconocido. En estos casos, no se deben contestar dichos mensajes y enviar una copia a TIC’s para que efectúe el seguimiento necesario.
- Todo usuario es responsable de la cantidad y tamaño de documentos adjuntos que envíe por correo.

- Está restringido el envío de correos masivos, sin la previa autorización de TIC's.
- No se debe ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, porque el archivo adjunto puede contener virus.
- Es responsabilidad del usuario el contenido o los criterios emitidos en el correo institucional.
- Todo usuario es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos. En estos casos, no se deben contestar dichos mensajes y deben enviar una copia al Oficial de Seguridad de la Información para que efectúe el seguimiento y la investigación necesaria.
- Es responsabilidad del usuario la depuración, administración de su cuenta de correo y, en coordinación con TIC's la obtención de respaldos.

3.3.4 Acceso y uso de internet y sus aplicaciones/servicios

- Se prohíbe el uso de los sistemas de comunicación para actividades comerciales, privadas o para propósitos de entretenimiento y diversión.
- Cada usuario es responsable de la información y contenidos a los que accede y de aquella que copia para conservación en los equipos del Instituto.
- Está bloqueado el acceso por medio de dispositivos fijos y/o móviles a aquellos portales, aplicaciones o servicios de internet relacionados a pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses y valores del Instituto o que impacten negativamente en la productividad y trabajo de sus servidores públicos y trabajadores.
- Las conexiones no seguras a los servicios de red pueden afectar a toda la Institución, por lo tanto, se debe controlar el acceso a los servicios de red tanto internos como externos.
- El acceso de los usuarios a aplicaciones y/o servicios de internet, puede ser sujeto de monitoreo y registro por parte del Instituto.
- El OSI, puede acceder a los contenidos monitoreados, con el fin de asegurar el cumplimiento de las medidas de seguridad.
- El Instituto podrá en cualquier momento, bloquear o limitar el acceso y uso de la Internet a los usuarios o a terceros que accedan tanto por medio alámbrico como inalámbrico.

4. Documentos de referencia

- Acuerdo Ministerial 025-2019.
- Esquema Gubernamental de Seguridad de la Información (EGSI v2.0).
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001.
- Alcance del Esquema Gubernamental de Seguridad de la Información.

5. Glosario de términos

Activo de información	Es todo recurso que genera, procesa, transporta y/o resguarda información necesaria para la operación y el cumplimiento de la misión del Instituto Nacional de Biodiversidad, por lo tanto, se requiere proteger su confidencialidad, integridad y disponibilidad de las amenazas propias de su naturaleza y características.
Amenaza	Evento previsible o no, que puede afectar a las personas, bienes o información.
Confidencialidad	Es el atributo de la información que garantiza que ésta es accesible únicamente al personal autorizado a tener acceso a ella.
Dato	Término que se refiere a hechos, eventos, transacciones, etc., que han sido registrados. Un dato no dice nada sobre el porqué de las cosas, y por sí mismo tiene poca o ninguna relevancia o propósito
Disponibilidad	Es el atributo de la información que garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, en cualquier momento que la requieran.
Información	Conjunto de datos que han sido procesados en un documento o algún tipo de comunicación audible o visible de tal manera que pueden ser entendidos e interpretados por un receptor (informes, reportes, fichas, artículos, presentaciones, etc.)
Integridad	Es el atributo de la información que garantiza la precisión, fiabilidad, exactitud y totalidad de los datos a lo largo de su ciclo de vida (generación, procesamiento y transmisión).
Investigador asociado	Es aquel investigador que sin ser parte directa del INABIO participa en proyectos y/o programas ejecutados por el Instituto, posterior a un proceso de calificación y registro.
Líder de área	Director, Coordinador, Jefe de proyecto o cualquier servidor

	público que por circunstancias de trabajo, tiene la responsabilidad de guiar o liderar a un equipo de trabajo que maneja información en el Instituto.
Pasante / Practicante	Alumno o estudiante matriculado en el segundo año o en años superiores de un centro de estudios de educación Superior y que concurre normalmente a los correspondientes períodos lectivos
Servidor público	Todas las personas que con cualquier título trabajen, presten servicios o ejerzan un cargo, función o dignidad dentro del sector público y que estén regidos por la Ley Orgánica de Servicio Público – LOSEP
Sniffer	Aplicación de software diseñada específicamente para redes informáticas, que permiten capturar y analizar los paquetes de datos que se envían y reciben a través de la red.
Tesista	Estudiante del último año o egresado de un centro de estudios de educación superior que está ejecutando un proyecto previo a la obtención de su título de grado.
TIC's	Tecnologías de Información y Comunicación, área administrativa que orgánicamente pertenece a la Dirección de Planificación y Gestión Estratégica del INABIO.
Trabajador	Todas las personas que trabajen dentro del sector público y que estén regidos por el Código de Trabajo.
Usuario	Es una persona que utiliza un equipo tecnológico o servicio informático otorgado por el INABIO. Los usuarios pueden ser servidores públicos, trabajadores, investigadores asociados, pasantes o practicantes u otros, que hagan uso de la tecnología del Instituto.