	PROTOCOLO	Versión	01
	PTO-TSI-001/11-2024	Fecha	07/11/2024
	PROTOCOLO DE ACTUACIÓN ANTE VULNERABILIDAD E INCIDENTES EN LA SEGURIDAD DE DATOS PERSONALES	**APROBADO POR:**	
		Firmado electrónicamente por: LENIN EDUARDO FREIRE COBO	
		Mgtr. Lenín Freire Cobo	
		GERENTE DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN	

1. OBJETIVO

Establecer directrices y asignar responsabilidades para asegurar la protección de los datos personales tratados por la ESPOL, frente a posibles vulnerabilidades e incidentes de seguridad.

2. ALCANCE

Este protocolo se aplica a todo el personal administrativo, académico, de servicio, profesionales contratados, proveedores, terceros vinculados a la ESPOL, así como a cualquier persona que tenga acceso a los datos personales proporcionados por la institución, utilice los sistemas informáticos que facilitan dicho acceso o participe en cualquier etapa del tratamiento de estos datos.

3. NORMATIVA

- Constitución de la República del Ecuador.
- Ley Orgánica de Protección de Datos Personales.
- Reglamento de la Ley Orgánica de Protección de Datos Personales.
- Política de Privacidad, Términos y Condiciones de la Política de Privacidad de la ESPOL.

4. UNIDAD RESPONSABLE

Gerencia de Tecnologías y Sistemas de Información (GTSI)

5. UNIDADES COLABORADORAS

Toda unidad académica y administrativa que forme parte de la comunidad politécnica y que por la ejecución de sus funciones realice un tratamiento de los datos personales que son suministrados por la ESPOL.

6. DEFINICIONES

Dato personal. - Dato que identifica o hace identificable a una persona natural, directa o indirectamente.

Datos sensibles: Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

- **Comunidad politécnica**: Son los aspirantes, estudiantes, graduados, personal administrativo, académico, de servicio, profesionales contratados (en adelante colaboradores), proveedores, y en general cualquier persona que en algún momento tenga relación con la ESPOL.

  Colaboradores: Es todo el personal administrativo, académico, de servicio, profesionales contratados, proveedores y terceros relacionados con la ESPOL.

  Tratamiento: Conjunto de operaciones realizadas sobre datos personales, que comprende la obtención, registro, organización, conservación, modificación, eliminación, extracción, consulta, elaboración, utilización, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, y uso de datos personales.

7. ETAPA DE PREVENCIÓN

Esta etapa tiene como objetivo identificar las acciones y medidas preventivas que deben tomar las personas que realicen un tratamiento de datos para reducir la probabilidad de que ocurran incidentes en la seguridad y operación de los datos.

INSTANCIA	FUNCIÓN
GTSI (UNIDAD RESPONSABLE)	• Analizar los riesgos y vulnerabilidades tecnológicas y los impactos y medidas de seguridad que los distintos sistemas pudieran tener. • Asegurar la actualización y corrección regular de software para solucionar posibles errores o vulnerabilidades de seguridad y mejorar el rendimiento de programas y sistemas operativos. • Implementar y gestionar soluciones de seguridad integrales, incluyendo firewalls y software antivirus/antimalware, para proteger la red y los dispositivos contra accesos no autorizados, ataques maliciosos y amenazas de software. • Asegurar que solo las personas autorizadas tengan acceso a los sistemas y datos personales; esto incluye la gestión de credenciales, autenticación multifactor y permisos de acceso basados en roles. • Utilizar cifrado para proteger los datos en tránsito. • Implementar dentro de las bases de información y datos personales, medidas técnicas y organizativas. • Asegurar que los respaldos de datos se realicen de manera regular y se guarden en ubicaciones seguras, además de eliminar de manera segura la información que ya no sea necesaria, utilizando técnicas de borrado seguro.

	• Llevar un registro de Actividades de Tratamiento (RAT) de los datos personales mantenidas en las bases de información. • Capacitar a los colaboradores del área de GTSI en prácticas seguras relacionadas con el manejo de datos y el uso de sistemas tecnológicos para reducir el riesgo de errores humanos y ataques dirigidos. • Enviar correos periódicos a la comunidad politécnica con información clara y puntual sobre los posibles ataques digitales que podrían enfrentar, incluyendo phishing y otros métodos de engaño, explicando en qué consisten estos ataques, cómo identificar correos y enlaces sospechosos, y/o compartir las mejores prácticas para protegerse.
DELEGADO DE PROTECCIÓN DE DATOS PERSONALES	• Asesorar y supervisar al responsable del tratamiento de datos personales, así como a todo el personal que tenga acceso a datos sobre las disposiciones legales, resoluciones oficiales, procesos y/o normativa interna referente a la protección de datos personales. • Elaborar políticas institucionales para guiar el proceso de tratamiento de datos personales, supervisando continuamente el cumplimiento a las disposiciones aprobadas por las autoridades. • Asesorar en los análisis que se realicen con relación a los riesgos, impactos y medidas de seguridad y supervisar que sean aplicadas. • Cooperar con la autoridad de protección de datos personales y actuar como punto de contacto con dicha entidad, con relación a las cuestiones referentes al tratamiento de datos personales.
UNIDADES COLABORADORAS	• Tratar de manera confidencial los datos personales de los titulares, y no compartirlos con terceros a menos que sea necesario para cumplir con el fin que se otorgó consentimiento o se encuentre permitido en la ley. • Crear contraseñas robustas y no reutilizarlas para diferentes cuentas. • Cerrar sesión en aplicaciones y sistemas cuando no estén en uso, especialmente en dispositivos compartidos o públicos. • Identificar y reportar posibles amenazas, como correos de phishing, enlaces sospechosos, y comportamientos inusuales en los sistemas. • Utilizar únicamente los medios oficiales institucionales (como el correo electrónico institucional) para compartir información relacionada con sus labores.

	• Verificar que los destinatarios de datos personales sean correctos y que la información autorizada para comunicar sea remitida a través de canales oficiales y seguros. • No compartir datos personales sin autorización. • Conocer y seguir estrictamente todas las políticas de seguridad de la información y tratamiento de datos personales de la institución.

8. ETAPA DE RESPUESTA

Las situaciones previstas en esta etapa, constituyen incidentes y riesgos de seguridad a los datos personales, aquí se define la ruta de actuación y las unidades responsables de responder ante estas situaciones:

8.1. SITUACIÓN A: AVERÍA/DESTRUCCIÓN/PERDIDA DE EQUIPOS DEL DATA CENTER QUE ALMACENAN INFORMACIÓN Y DATOS PERSONALES DE LA ESPOL.

RUTA DE ACTUACIÓN		RESPONSABLE
1	Determina qué equipos o dispositivos han sido afectados, para evaluar el alcance del incidente que pueda afectar a las bases de datos personales e información.	Responsable de seguridad de datos personales de GTSI
2	Inicia la recuperación de datos desde las cintas magnéticas de respaldo, siguiendo los procedimientos establecidos para restaurar la información en nuevos equipos o en la infraestructura disponible.	
3	Configura los nuevos equipos o utiliza la infraestructura alternativa donde los datos recuperados puedan ser restaurados de manera segura, garantizando que los sistemas estén operativos lo antes posible.	
4	Comprobar que los datos restaurados desde las cintas magnéticas son completos y no presentan errores.	
5	Realizar pruebas de funcionalidad y consistencia para asegurar que la información esté correctamente restaurada.	

8.2. SITUACIÓN B: ERRORES OPERACIONALES EN LA GESTIÓN DE DATOS PERSONALES E INFORMACIÓN

RUTA DE ACTUACIÓN		RESPONSABLE
1	Notifica a GTSI, de manera inmediata a partir del momento en la que tuvo conocimiento de la divulgación accidental de información.	Colaborador
2	Documenta los detalles del incidente, incluyendo la naturaleza de la información divulgada, los destinatarios no autorizados, y el momento en que ocurrió la divulgación.	Responsable de seguridad de datos personales de GTSI
3	Toma medidas inmediatas para recuperar o eliminar la información divulgada accidentalmente, como la revocación de acceso a archivos o la eliminación de correos electrónicos, en los casos que sea posible.	

8.3. SITUACIÓN C: INTENTO DE ACCESO NO AUTORIZADO A SISTEMAS INFORMÁTICOS Y/O BASES DE DATOS PERSONALES MEDIANTE INTRUSIONES CIBERNÉTICAS O FRAUDES DIGITALES (HACKING, PHISHING, MALWARE)

RUTA DE ACTUACIÓN		RESPONSABLE
1	Notifica a GTSI de manera inmediata al detectar cualquier incidente sospechoso relacionado con la seguridad de los sistemas o datos personales, si aplica.	Colaborador
2	Identifica el tipo de incidente, su alcance y los posibles riesgos asociados.	Responsable de seguridad de datos personales de GTSI
4	Detecta y revoca inmediatamente las credenciales sospechosas de haber sido comprometidas, bloqueando o retirando los permisos asociados.	
	Implementa medidas correctivas según el tipo de amenaza: • Bloquea los enlaces maliciosos y elimina los correos electrónicos sospechosos, en casos de phishing • Utiliza herramientas especializadas dependiendo de la situación para eliminar el software malicioso y restaurar la integridad del sistema afectado, en casos de malware. • Cierra las brechas de seguridad identificadas, y aplica parches o actualizaciones de seguridad pertinentes, en casos de hacking.	
4	Solicita de ser necesario la actualización de sus credenciales a los individuos afectados.	
5	De considerarse necesario, notifica a la Comunidad Politécnica explicando brevemente lo ocurrido, sin entrar en detalles	

	técnicos complejos, pero aclarando la naturaleza del ataque (hacking, phishing, malware, etc.) y las recomendaciones a considerar.	

8.4. SITUACIÓN D: DESTRUCCIÓN DE DATOS, ALTERACIÓN, PERDIDA DE CONTROL DE ACCESO, ACCESOS ILICITOS DE TERCEROS, INTRUSIONES CIBERNÉTICAS Y FRAUDES DIGITALES (HACKING, PHISHING, MALWARE, O SIMILARES) QUE RESULTEN EN LA EXPOSICIÓN Y/O PÉRDIDA IRREVERSIBLE DE BASES DE DATOS PERSONALES

En los casos en los que la vulneración de la seguridad de los datos personales implique una violación de la seguridad y represente un riesgo para los derechos y las libertades de las personas naturales, se actuará de acuerdo con lo establecido en el artículo 43 de la Ley Orgánica de Protección de Datos Personales y el artículo 24 de su Reglamento.

RUTA DE ACTUACIÓN		RESPONSABLE
1	Notifica al Gerente de GTSI que la intrusión cibernética no ha podido ser controlada, detallando el alcance de la exposición o pérdida de los datos, incluyendo información sobre el tipo de datos comprometidos, la magnitud del impacto, y las medidas de contención implementadas hasta el momento.	Responsable de seguridad de datos personales de GTSI
2	Documenta y notifica el incidente, enviando al Delegado de protección de datos personales de la institución el "*Formulario de notificación y comunicación de una violación de la seguridad de datos personales*" detallando el incidente ocurrido y el estado del mismo.	Gerente de GTSI
3	Notifica a la máxima autoridad de la institución sobre la intrusión cibernética y los riesgos asociados, proporcionando un informe detallado con toda la información recopilada hasta el momento, incluyendo las medidas de contención implementadas y su efectividad.	Delegado de protección de datos personales
4	Notifica en un plazo máximo de 5 días a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de las Telecomunicaciones sobre la vulneración a la seguridad de los datos personales y su potencial riesgo para los derechos y las libertades de las personas naturales.	Responsable de Datos Personales y Delegado de Protección de Datos Personales
5	Notifica de la vulneración de los datos personales a los titulares de conformidad con lo establecido en el artículo 28 del Reglamento de la Ley Orgánica de Protección de Datos Personales.	Responsable de Datos Personales y Delegado de Protección de Datos Personales

9. ETAPA DE MITIGACIÓN

	RUTA DE ACTUACIÓN	RESPONSABLE
1	Evaluar el incidente de seguridad y coordinar la actualización del presente protocolo, en caso de requerirse nuevas medidas o ajustes.	Delegado de protección de datos personales
2	Seguir las indicaciones de las autoridades correspondientes de la institución y del Delegado de protección de datos personales, si aplica.	Responsable de seguridad de GTSI
3	Realizar una auditoría exhaustiva de los sistemas afectados y de las acciones de respuesta para identificar vulnerabilidades remanentes y asegurar que se ha eliminado cualquier acceso no autorizado.	
4	Mantener un monitoreo continuo de los sistemas y la infraestructura afectada para prevenir nuevos incidentes y asegurar que se implementen las medidas correctivas y preventivas necesarias que no se hayan considerado previo al desarrollo de la situación.	
5	Seguir las recomendaciones planteadas por la Gerencia de Tecnologías y Sistemas de información (GTSI) de la ESPOL.	Colaborador/Comunidad Politécnica

10. ANEXOS

ANEXO 1.

Formulario de notificación y comunicación de una violación de la seguridad de datos personales

NOTIFICACIÓN Y COMUNICACIÓN DE UNA VIOLACIÓN DE LA SEGURIDAD DE DATOS PERSONALES (De conformidad con lo establecido en el artículo 24 del RLOPDP y en concordancia con la situación D del punto 8.4 de este protocolo, se deberá notificar la vulneración a la seguridad de datos personales, debiendo completar el siguiente esquema de notificación con la siguiente información:		
Información antecedente: **Persona que identifica la Presunta de la vulneración:**		**Fecha:** **Hora:**
1	**Descripción de la violación de la seguridad (naturaleza).**	
2	**Interesados y categorías de datos afectados.**	
3	**Detalle de los Sistemas Vulnerados**	
4	**Causa de la Presunta de la vulneración**	
5	**Volumen y tipos de datos comprometidos.**	*-La naturaleza de la violación de la seguridad de los datos personales.* *-Nombre y datos de contacto del delegado de protección de datos de la ESPOL.*
6	**Medidas adoptadas al momento de la detección de la presunta vulneración.**	
7	**Nombre y cédula de persona que llena el formulario.**	**Firma**

ANEXO 2.

Definiciones

VULNERABILIDAD: Debilidad en un sistema que puede ser explotada por atacantes para obtener acceso no autorizado a datos o funciones del sistema.

PHISHING: Es una técnica de ingeniería social que busca obtener información confidencial mediante la manipulación de personas, comúnmente llevado a cabo a través de correos electrónicos.

HACKING: Explotación de vulnerabilidades en sistemas o redes para obtener acceso no autorizado, a menudo con intenciones maliciosas como el robo de datos o la interrupción de servicios.
MALWARE: Es un software malicioso diseñado para dañar, controlar o explotar sistemas informáticos sin el consentimiento del usuario.

FIREWALL: Es un sistema de seguridad de red que supervisa y controla el tráfico de red entrante y saliente basado en reglas de seguridad predefinidas y su principal función es actuar como una barrera protectora entre una red interna confiable y otras redes externas, como internet, bloqueando el acceso no autorizado mientras permite las comunicaciones legítimas.

CREDENCIALES: Son un conjunto de información, típicamente un nombre de usuario y una contraseña, usados para verificar la identidad y autorizar el acceso a sistemas o datos.

ANONIMIZACIÓN: Proceso que modifica los datos personales para que no puedan usarse para identificar a una persona, de manera irreversible.

SEUDOANONIMIZACIÓN: Es una técnica de protección de datos en la que la información identificativa de una persona se sustituye por un seudónimo o un identificador artificial. a diferencia de la anonimización completa, los datos seudoanonimizados pueden ser revertidos al estado original mediante el uso de información adicional (como una clave de cifrado).

CIFRADO DE DATOS: Proceso que convierte información en un formato codificado, accesible solo mediante una clave de descifrado.

BASE DE DATOS: Es un sistema organizado que permite el almacenamiento, la gestión y la recuperación eficiente de grandes volúmenes de información estructurada.

INTRUSIÓN CIBERNÉTICA: Se refiere al acceso no autorizado a sistemas informáticos, redes, o dispositivos con la intención de robar, manipular, o destruir datos.

FRAUDE DIGITAL: Es una actividad criminal que utiliza medios tecnológicos para engañar a personas o entidades con el objetivo de obtener beneficios financieros, datos confidenciales, o información personal.
parches o actualizaciones de seguridad: modificaciones aplicadas a software o sistemas para corregir vulnerabilidades y mejorar la protección contra amenazas.