



RESOLUCIÓN DE SESIÓN ORDINARIA- 017-OCS-2024

**ÓRGANO COLEGIADO SUPERIOR DEL INSTITUTO SUPERIOR TECNOLÓGICO
PICHINCHA CON CONDICION DE IUNIVERSITARIO**

CONSIDERANDO

Que, el artículo 5 de la Ley Orgánica de Educación Superior prescribe: Derechos de las y los estudiantes: son derechos de las y los estudiantes los siguientes: A) Acceder, movilizarse, egresar y titularse sin discriminación conforme sus méritos académicos (...)

Que, el artículo 46 del Reglamento a la Ley Orgánica de Educación Superior establece: Órgano Colegiado Superior. - el Órgano Colegiado Superior es la autoridad máxima de los institutos y conservatorios superiores, tengan o no la condición de superior universitario; cuyas resoluciones serán de obligatorio cumplimiento por parte de la institución

Que, el Órgano Colegiado Superior del Instituto Superior Tecnológico Pichincha con condición de Universitario en sesión ordinaria de 14 de junio del 2024, procedió revisar las reformas a la normativa propuesta por La Coordinación de TICs respecto de SISTEMA INFORMATICO DE GESTION – (SIG) HOLON.

En ejercicio de sus atribuciones

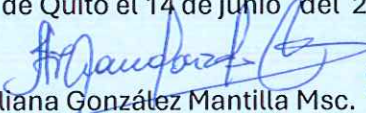
RESUELVE

Art. 1 Aprobar las Reformas del REGLAMENTO DE USO DEL SISTEMA INFORMATICO DE GESTION (SIG) HOLON- ISTP.

Art. 2 Disponen se notifique a la Coordinación de Comunicación y a la Coordinación de TICS para su socialización y aplicación, respectivamente.

NOTIFIQUESE Y CUMPLASE

Dado en el Distrito Metropolitano de Quito el 14 de junio del 2024


Dra. Iliana González Mantilla Msc.
SECRETARIA ABOGADA





EL ÓRGANO COLEGIADO SUPERIOR DEL INSTITUTO SUPERIOR TECNOLÓGICO PICHINCHA
CON CONDICION DE UNIVERSTARIO

CONSIDERANDO:

Que el artículo 18 de la Constitución de la República, en su numeral segundo, establece que es derecho de todas las personas el acceso a la información generada en instituciones públicas o privadas que manejen fondos públicos o realicen funciones públicas. Además del derecho de acceso universal a las tecnologías de información y comunicación;

Que el artículo 52 de la Constitución de la República dispone que las personas tengan derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características;

Que el artículo 10 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, establece que: "Es responsabilidad de las instituciones públicas y personas 2 jurídicas de derecho público, crear y mantener registros públicos de manera profesional, de acuerdo con lo que determine la Ley del Sistema Nacional de Archivos para que el derecho a la información se pueda ejercer de forma integral; y, en ningún caso se justificará la ausencia de normas técnicas y manejo de archivo de la información y documentación tanto física como digital para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción (...)";

Que la Ley del Sistema Nacional de Archivos, en su artículo 1 define que: "Constituye Patrimonio del Estado la documentación básica que actualmente existe o que en adelante se produjere en los archivos de todas las instituciones de los sectores público, y privado, así como la de personas particulares, que sean calificadas como tal (...)";

En uso de sus atribuciones aprueba el siguiente:

REGLAMENTO DE USO DEL SISTEMA INFORMATICO DE GESTION (SIG) HOLON-ISTP

GENERALIDADES

Artículo 1.- Objetivo.- La presente normativa tiene como objetivo establecer las directrices y

procedimientos para el uso adecuado y seguro del Sistema Informático de Gestión HOLON del Instituto Superior Tecnológico Pichincha. Este documento busca asegurar que todos los usuarios comprendan y cumplan con las políticas de uso, garantizando así la integridad, confidencialidad y disponibilidad de la información manejada por el sistema.

Artículo 2 Alcance.- Esta normativa es aplicable a todos los usuarios del Sistema Informático de Gestión HOLON, incluyendo personal administrativo, docente, estudiantes y cualquier otra persona autorizada para acceder y utilizar el sistema. De acuerdo con los roles y permisos asignados cubre los módulos del sistema que se han implementado hasta el momento en esta Fase 1 y que son: Gestión de Recursos Humanos, Gestión Académica y Gestión Contable, en el apartado de Revisión y Actualización de la Normativa se abordará el tema de las acciones a realizar en las implementaciones de nuevos módulos comprendidos en la Fase 2 del Sistema HOLON.

Artículo 3.- Definiciones y Términos:

- a. Sistema Informático de Gestión HOLON (SIG-HOLON):** Plataforma ERP utilizada para la gestión de los procesos administrativos y académicos del Instituto.
- b. Usuario:** Persona autorizada para acceder y utilizar el SIG-HOLON.
- c. Roles y Permisos:** Conjunto de privilegios asignados a los usuarios del sistema, que determinan las acciones que pueden realizar.
- d. Datos Personales:** Información relacionada con una persona identificada o identificable.
- e. Coordinador:** Empleado del Instituto responsable de una Unidad.
- f. Unidad:** Área organizacional del Instituto que representa una Gestión o una Carrera
- g. Administrador del Sistema:** Persona o equipo responsable de la gestión técnica y operativa del SIG-HOLON, incluyendo mantenimiento, seguridad y soporte.
- h. Módulo:** Componente funcional del SIG-HOLON que gestiona un área específica del Instituto, como Recursos Humanos, Gestión Académica o Contabilidad.
- i. Autenticación:** Proceso de verificación de la identidad de un usuario antes de otorgarle acceso al sistema.
- j. Contraseña:** Combinación secreta de caracteres utilizada por los usuarios para autenticarse en el SIG-HOLON.





- k. **Base de Datos:** Conjunto organizado de datos almacenados y gestionados por el SIG-HOLON.
- l. **Incidencia:** Evento o problema que afecta el funcionamiento normal del SIG-HOLON y requiere intervención técnica.
- m. **Backup/Respaldo:** Copia de seguridad de los datos del sistema, utilizada para restaurar la información en caso de pérdida o daño.
- n. **Política de Seguridad:** Conjunto de medidas y procedimientos destinados a proteger la información y los recursos del SIG-HOLON.
- o. **Confidencialidad:** Principio que garantiza que la información sea accesible solo para las personas autorizadas.
- p. **Integridad:** Principio que asegura que la información sea precisa y completa, y no haya sido alterada de manera no autorizada.
- q. **Disponibilidad:** Principio que garantiza que la información y los recursos del sistema estén accesibles y utilizables cuando se necesiten.

CAPITULO II Acceso y Autenticación

Artículo 5.- Requisitos de Acceso.- Para acceder al SIG-HOLON, los usuarios deben cumplir con los siguientes requisitos:

1. Ser personal administrativo, docente, estudiante o cualquier otra persona autorizada por la administración del Instituto Superior Tecnológico Pichincha.
2. Contar con una cuenta de usuario activa proporcionada por el administrador técnico/funcional del sistema.
3. Aceptar y cumplir con la normativa de uso del SIG-HOLON.

Artículo 6.- Procedimiento de Autenticación.- el procedimiento para la autenticación será el siguiente:

1. Los usuarios deben autenticarse utilizando su nombre de usuario y contraseña únicos.
2. Las contraseñas deben cumplir con los requisitos de seguridad establecidos por la política de seguridad del Instituto, incluyendo longitud mínima, complejidad y periodicidad de cambio.
3. Las cuentas de acceso al SIG-HOLON son personales e intransferibles.

Artículo 7 .- Gestión de Cuentas de Usuario.- La creación, modificación y eliminación de cuentas de usuario serán gestionadas exclusivamente por el administrador del sistema.

- La creación de cuentas de usuario tiene dos opciones:

- Administrativos y docentes: se crean a partir de la aprobación del señor Rector y son generadas por la Coordinación de Talento Humano.
- Estudiantes: se crean automáticamente al realizar por parte del estudiante un proceso de Admisión a través de un formulario ubicado en la página web.

- Las cuentas de usuario inactivas por un período mayor a seis meses o por pedido de la Coordinación de Talento Humano se deshabilitan manualmente por parte del administrador técnico del SIG-HOLON.

Artículo 8.- Roles y Permisos.-

- Los usuarios serán asignados a roles específicos basados en sus responsabilidades y necesidades de acceso.

- Cada rol tendrá permisos específicos que determinan las acciones que los usuarios pueden realizar dentro del sistema.

- La asignación de roles será revisada periódicamente para asegurar que los permisos otorgados sigan siendo apropiados para las funciones del usuario.

CAPITULO III

DEL USO DEL SISTEMA

Artículo 9.- Políticas Generales de Uso

Política 1. Uso Exclusivo para Fines Institucionales

- El SIG-HOLON debe ser utilizado exclusivamente para actividades laborales y académicas relacionadas con el Instituto Superior Tecnológico Pichincha.

- El uso para beneficio personal del sistema (base de datos), incluso durante horas laborales, no está permitido y será monitoreado para asegurar el cumplimiento.

Política 2.- Cumplimiento de Normativas y Procedimientos

- Todos los usuarios deben conocer y cumplir con las normativas y procedimientos establecidos





para el uso del SIG-HOLON.

- Las actualizaciones o cambios en las normativas serán comunicados a los usuarios, quienes deberán ajustarse a las nuevas directrices de inmediato.

Política 4.- Confidencialidad de Credenciales

- Las credenciales de acceso (nombre de usuario y contraseña) son personales e intransferibles.
- Está prohibido compartir credenciales con otros usuarios, incluso si pertenecen al mismo departamento.

Política 5 Seguridad en el Acceso

- Los usuarios deben asegurarse de cerrar sesión adecuadamente al finalizar su uso del sistema para prevenir accesos no autorizados.
- Se recomienda no almacenar contraseñas en navegadores o dispositivos compartidos.

Artículo 10 Responsabilidades de los Usuarios.- las responsabilidades de los usuarios son.

1. Precisión y Actualización de Información

- Los usuarios son responsables de la precisión y veracidad de la información ingresada en el sistema.
- Cualquier cambio en los datos debe ser reflejado de manera oportuna para mantener la integridad de la información.

2. Protección de la Confidencialidad

- Los usuarios deben proteger la confidencialidad de la información accesible a través de su cuenta, evitando divulgaciones o filtraciones no autorizadas.
- La información confidencial no debe ser compartida mediante correos electrónicos no seguros o plataformas no aprobadas por el Instituto.

3. Reporte de Incidentes

- Cualquier incidente de seguridad, anomalía o error en el sistema debe ser reportado inmediatamente a la Coordinación de TICs.
- Los usuarios deben colaborar con el equipo de soporte técnico para resolver cualquier problema detectado.

CAPITULO IV DEL CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD

Artículo 11.- Los usuarios deben cumplir todas las políticas de seguridad establecidas, incluyendo el uso de contraseñas fuertes.

Artículo 12.- Las contraseñas deben ser cambiadas regularmente y no deben ser reutilizadas, manteniendoun historial de al menos 4 iteraciones.

Artículo 13.- Uso Responsable del Sistema

- Los usuarios deben utilizar el sistema de manera responsable, evitando actividades que puedan afectar negativamente el rendimiento o la seguridad del mismo.

- Está prohibido intentar eludir las medidas de seguridad implementadas en el SIG-HOLON.

Artículo 14.- Formación y Conocimiento

- Los usuarios deben participar en las sesiones de capacitación proporcionadas por el Instituto para mantenerse actualizados sobre el uso y las mejores prácticas del SIG-HOLON.

- Es responsabilidad del usuario familiarizarse con los manuales y recursos de ayuda disponibles.

CAPITULO V RESTRICCIONES Y PROHIBICIONES

Artículo 15.- Acceso No Autorizado

- a. Los usuarios solo deben acceder a las áreas y módulos del SIG-HOLON para los cuales tienen permisos explícitos.
- b. Intentar acceder a áreas restringidas del sistema sin la autorización correspondiente será considerado una violación grave de esta normativa.

Artículo 16.- Uso del Sistema para Actividades No Relacionadas

- a. El SIG-HOLON está destinado únicamente para actividades laborales y académicas relacionadas con el Instituto Superior Tecnológico Pichincha.
- b. Está prohibido utilizar el sistema para actividades personales, comerciales externas, o cualquier otra actividad no autorizada por el Instituto.

Artículo 17.- Modificación y Manipulación de Información





- a. Solo los usuarios con los permisos necesarios pueden modificar, borrar o actualizar información en el SIG-HOLON.
- b. Las modificaciones deben estar documentadas y justificadas, siguiendo los procedimientos establecidos por cada departamento.
- c. Manipular información con el fin de distorsionar la verdad u obtener beneficios personales está terminantemente prohibido.

Artículo 18.- Introducción de Datos Falsos o Engañosos

- a. Los usuarios deben asegurarse de que todos los datos ingresados en el sistema sean precisos, verificados y reflejen la realidad.
- b. La introducción intencional de información falsa, engañosa o errónea será sancionada de acuerdo con las políticas disciplinarias del Instituto.

Artículo 19.- Uso de Software No Autorizado

- a. Está prohibido instalar o ejecutar cualquier software no autorizado que interactúe con el SIG-HOLON.
- b. Los scripts automatizados o cualquier otro tipo de software que manipule o extraiga información del sistema sin aprobación previa están prohibidos.

Artículo 20.- Compartición de Credenciales

- a. Las credenciales de acceso son personales e intransferibles. Compartir nombre de usuario y contraseña con otras personas está totalmente prohibido.
- b. Los usuarios deben mantener sus credenciales seguras y no divulgarlas en ninguna circunstancia.

Artículo 21.- Protección Contra Malware y Otros Amenazas

- a. Los usuarios deben evitar la descarga de archivos sospechosos o la visita a sitios web inseguros desde dispositivos que accedan al SIG-HOLON.
- b. Cualquier sospecha de malware u otras amenazas debe ser reportada inmediatamente a la Coordinación de TICs.

**CAPITULO VI
MÓDULOS DEL SISTEMA**

Artículo 22.- Recursos Humanos:

DE LOS CONTRATOS:

- a. Gestión y almacenamiento digital de los contratos de los empleados.
- b. Registro de fechas de inicio y finalización, renovaciones y condiciones contractuales.
- c. Registro de aviso de entrada y salida del IESS.

DE LA NOMINA

- a. Procesamiento de la nómina mensual, incluyendo cálculo de sueldos, deducciones y bonificaciones.
- b. Generación de reportes de nómina y entrega de roles de pago a los empleados.

Artículo 23.- Gestión Académica

Notas

- a. Registro de calificaciones de los estudiantes en todas las materias.
- b. Generación de informes de desempeño académico.

Admisiones

- Gestión del proceso de admisión de nuevos estudiantes.
 - Pregrado
 - Postgrado
- Registro de información de los postulantes y seguimiento del proceso de selección.

Matrículas

- Administración del proceso de matrícula de los estudiantes.
 - Pregrado
 - Postgrado
- Registro de inscripciones en materias y gestión de horarios.

Lectivos

- Gestión de los períodos lectivos, incluyendo fechas de inicio y fin de cada ciclo.





- Planificación de actividades académicas para cada período.

Materias

- Administración del catálogo de materias ofrecidas por el Instituto.
- Actualización de contenidos y requisitos de cada materia.

Planificaciones

- Elaboración de planes de estudio y asignación de materias a cada carrera.
- Coordinación de recursos necesarios para la ejecución de los planes de estudio.

Distributivos

- Asignación de profesores a materias y horarios.
- Gestión de carga horaria y distribución de recursos docentes.

Pagos en Línea

- Facilitar el pago de matrículas y otros servicios académicos a través de plataformas en línea.
- Integración con sistemas de pago seguros y generación de comprobantes.

Artículo 24.- Contabilidad

Proveedores

- Gestión de información de proveedores y contratos.
- Control de cuentas por pagar y seguimiento de pagos.

Contabilidad General

- Registro de transacciones contables y mantenimiento de libros mayores.
- Generación de estados financieros y reportes contables.
- Conciliaciones bancarias y auditorías internas.

CAPITULO VI SECCION PRIMERA

Artículo 25.- Seguridad y Confidencialidad

Matriz – Quito

Dir.: Buenos Aires OE1-16 y Av. 10 de Agosto
(02) 2 238 291
www.tecnologicopichincha.edu.ec



Protección de Datos Personales (Ley Orgánica de protección de datos personales)

a. Recolección y Almacenamiento

- Solo se recolectarán los datos personales que sean estrictamente necesarios para cumplir con las funciones del Instituto, minimizando la recopilación de datos sensibles.
- Los datos personales serán almacenados en servidores seguros con acceso limitado y protegido. Se utilizarán métodos de cifrado para proteger la información almacenada.

b. Uso y Divulgación

- Los datos personales se utilizarán exclusivamente para los fines para los cuales fueron recolectados, tales como gestión académica, recursos humanos y contabilidad (y en las futuras fases del sistema)
- La divulgación de datos personales a terceros se realizará únicamente con el consentimiento explícito del titular de los datos, a menos que una ley, una orden judicial o una entidad oficial requiera lo contrario.

c. Derechos de los Titulares

- Los titulares de los datos tienen derecho a acceder a su información personal almacenada en el SIG-HOLON.
- Los titulares pueden solicitar la corrección de datos inexactos o desactualizados.
- Los titulares tienen derecho a solicitar la eliminación de sus datos cuando estos ya no sean necesarios para los fines para los cuales fueron recolectados.
- El Instituto proporcionará procedimientos claros y accesibles para que los titulares ejerzan estos derechos, incluyendo formularios de solicitud y tiempos de respuesta establecidos.

SECCIÓN SEGUNDA

CAPÍTULO I

Artículo 26.- Medidas de Seguridad

a. Seguridad Lógica

- Los usuarios deberán autenticarse mediante credenciales seguras, que incluirán contraseñas fuertes y, cuando sea posible.
- El sistema será monitoreado continuamente para detectar accesos no autorizados, actividades





sospechosas y otras amenazas. Se utilizarán sistemas de detección de intrusiones (IDS) y otros mecanismos de seguridad.

- Se implementarán políticas de control de acceso basadas en roles (RBAC) para asegurar que los usuarios solo puedan acceder a la información y funcionalidades necesarias para sus funciones.

b. Cifrado de Datos

- Los datos sensibles serán cifrados durante su transmisión utilizando protocolos seguros como HTTPS y SSL/TLS.

- Los datos almacenados en servidores y bases de datos serán cifrados para protegerlos contra accesos no autorizados y robos de información.

c. Respaldo y Recuperación

- Se realizarán respaldos regulares de todos los datos críticos del sistema, que serán almacenados en ubicaciones seguras y fuera de las instalaciones principales.

- Se establecerán y probarán regularmente planes de recuperación de desastres para asegurar la rápida restauración de datos y la continuidad de las operaciones en caso de fallos del sistema o desastres.

CAPITULO II

PROCEDIMIENTOS EN CASO DE BRECHA DE SEGURIDAD

Artículo 27.- Detección y Respuesta

- Se implementarán sistemas de detección de intrusiones y monitoreo continuo para identificar brechas de seguridad en tiempo real.

- Se desarrollará un plan de respuesta a incidentes que detalle los pasos a seguir en caso de una brecha de seguridad, incluyendo la contención, erradicación y recuperación.

Artículo 28.- Investigación y Remediación

- Todos los incidentes de seguridad serán investigados a fondo para determinar la causa raíz, el alcance del daño y las vulnerabilidades explotadas.

- Se tomarán medidas correctivas para abordar las vulnerabilidades identificadas y prevenir la reaparición de incidentes similares en el futuro. Esto incluirá la actualización de sistemas, parches de seguridad y mejoras en las políticas de seguridad.

Artículo 29.- Notificación de Brechas

- En caso de una brecha de seguridad que afecte datos personales, se notificará a los titulares de los datos afectados de manera oportuna, proporcionando información sobre la naturaleza de la brecha y las medidas que pueden tomar para protegerse.

- Se notificará a las autoridades correspondientes conforme a la legislación aplicable, proporcionando todos los detalles requeridos sobre la brecha de seguridad y las acciones tomadas.

CAPITULO III

Artículo 30.- Mantenimiento y Soporte Técnico

a. Actualizaciones del Sistema

Planificación de Actualizaciones

- Las actualizaciones del SIG-HOLON serán planificadas y programadas con anticipación para minimizar el impacto en las operaciones diarias del Instituto.

- Los usuarios serán notificados con al menos tres días de antelación sobre las actualizaciones programadas.

Tipos de Actualizaciones

- Las actualizaciones de seguridad se aplicarán inmediatamente para proteger el sistema contra vulnerabilidades conocidas.

- Las actualizaciones funcionales serán implementadas periódicamente para optimizar el rendimiento y la utilidad del sistema.

Procedimiento de Actualización

- Las actualizaciones serán realizadas por el equipo de soporte técnico del proveedor siguiendo un procedimiento documentado que incluya pruebas en un entorno de desarrollo antes de la implementación en el entorno de producción.

- Se realizarán copias de seguridad completas antes de cualquier actualización importante para asegurar la posibilidad de revertir cambios en caso de problemas.





b. Soporte Técnico y Resolución de Problemas

Canales de Soporte

- Los usuarios pueden solicitar soporte técnico a través de diferentes canales, incluyendo correo electrónico, teléfono y un sistema de tickets en línea.
- (<https://ayudatic.tecnologicopichincha.edu.ec/helpdesk/>)

Niveles de Soporte

- Primer Nivel: Asistencia inicial para problemas comunes y consultas generales. Este nivel incluye la solución de problemas básicos y la orientación sobre el uso del sistema, lo realiza el personal de la Coordinación de TICs del Instituto.
- Segundo Nivel: Resolución de problemas más complejos que requieren intervención técnica especializada. Este nivel incluye diagnósticos detallados y reparaciones técnicas, lo realiza el primer nivel de Open Alliance.
- Tercer Nivel: Intervención avanzada y desarrollo de soluciones personalizadas. Este nivel incluye la colaboración con los desarrolladores del SIG-HOLON para solucionar problemas críticos y realizar mejoras específicas, de igual forma lo realiza Open Alliance.

Tiempo de Respuesta

- Se establecerán tiempos de respuesta y resolución según la gravedad del problema. Los problemas críticos serán atendidos de inmediato, mientras que los problemas menores se resolverán en un plazo acordado.

Registro de Incidencias

- Todas las solicitudes de soporte y problemas reportados serán registrados en un sistema de seguimiento de incidencias, permitiendo la documentación completa y la trazabilidad de cada caso.
- Se generarán informes periódicos sobre las incidencias y las soluciones implementadas para identificar patrones y mejorar continuamente el servicio de soporte.

Artículo 31.- Procedimientos de Respaldo y Recuperación

Política de Respaldo

- Se realizará un respaldo completo de los datos del SIG-HOLON al menos una vez al día. Los respaldos incrementales se realizarán con mayor frecuencia según la criticidad de los datos.

- Los respaldos serán almacenados en ubicaciones seguras y fuera del sitio principal para protegerlos contra desastres locales.





Verificación de Respaldo

- Se realizarán pruebas periódicas para verificar la integridad y la funcionalidad de los respaldos, asegurando que los datos puedan ser restaurados en caso de necesidad.

Plan de Recuperación

- Se establecerá un plan de recuperación ante desastres que detalle los pasos a seguir para restaurar el sistema y los datos en caso de fallo crítico.
- El plan incluirá procedimientos para la recuperación rápida y la comunicación con los usuarios durante el proceso de recuperación.

TITULO II

Formación y Capacitación

Artículo 32.- Capacitación Inicial

a. Objetivo de la Capacitación

- Proveer a los nuevos usuarios del SIG-HOLON los conocimientos necesarios para utilizar el sistema de manera eficiente y segura.

c. Contenido de la Capacitación

1. Introducción al SIG-HOLON y sus módulos.
2. Procedimientos básicos de uso y navegación.
3. Políticas de seguridad y buenas prácticas.
4. Resolución de problemas comunes y uso del soporte técnico.

d. Métodos de Capacitación

- Sesiones presenciales y virtuales dirigidas por instructores de OpenAlliance y de la Coordinación de TICs.
- Ejercicios prácticos para asegurar la comprensión de los temas tratados.

e. Evaluación:

1. Los usuarios deberán completar una evaluación práctica al finalizar la capacitación para

certificar su competencia en el uso del sistema.

2. Los resultados de la evaluación serán utilizados para identificar áreas que requieran refuerzo adicional.

Artículo 33.- Actualizaciones y Nuevas Funcionalidades

a. Notificación de Actualizaciones

- Los usuarios serán notificados sobre las actualizaciones del sistema y las nuevas funcionalidades a través de correos electrónicos y anuncios a través del SIG-HOLON.

b. Capacitación Continua

- Se organizarán sesiones de capacitación adicionales para introducir nuevas funcionalidades y cambios en el sistema.

- Se proporcionarán recursos de autoaprendizaje, como tutoriales en video y documentación actualizada, para que los usuarios puedan familiarizarse con las novedades a su propio ritmo.

c. Soporte Post-Actualización

- El equipo de soporte técnico estará disponible para asistir a los usuarios con preguntas y problemas relacionados con las nuevas funcionalidades.

- Se establecerán canales de retroalimentación para que los usuarios puedan reportar sus experiencias y sugerencias sobre las actualizaciones.

Artículo 34.- Recursos de Capacitación

a. Portal de Capacitación

- Un portal en línea estará disponible con acceso a todos los materiales de capacitación, incluyendo manuales de usuario, tutoriales en video, preguntas frecuentes y foros de discusión.

b. Sesiones de Capacitación Regular

- Se programarán sesiones de capacitación regular para todos los usuarios, con énfasis en áreas específicas según las necesidades identificadas.

c. Apoyo de Instructores

- Instructores especializados estarán disponibles para proporcionar asistencia y tutoría personalizada a los usuarios que requieran ayuda adicional.





Artículo 35.- Evaluaciones y Retroalimentación

- Se realizarán evaluaciones periódicas para medir la efectividad de la capacitación y ajustar los programas según sea necesario.
- Los usuarios podrán proporcionar retroalimentación sobre los programas de capacitación, lo cual será utilizado para mejorar continuamente el contenido y la metodología.

Artículo 36.- Cumplimiento y Auditoría

Supervisión del Cumplimiento

a. Monitoreo Continuo

- Se implementarán mecanismos de monitoreo continuo para asegurar que los usuarios cumplan con las políticas y procedimientos establecidos en esta normativa.
- Las actividades de los usuarios dentro del SIG-HOLON serán registradas y revisadas periódicamente para detectar y corregir cualquier incumplimiento.

b. Evaluaciones Periódicas

- Se realizarán evaluaciones periódicas del cumplimiento normativo para identificar áreas de mejora y asegurar la pertinencia con las políticas de seguridad y uso del sistema.
- Los resultados de estas evaluaciones serán documentados y comunicados a los responsables de cada área.

Artículo 37.- Auditorías Internas y Externas

a. Auditorías Internas

- El Coordinación de TICs realizará auditorías internas regulares para revisar la efectividad de los controles y procedimientos del SIG-HOLON.
- Estas auditorías incluirán la revisión de accesos, el cumplimiento de las políticas de seguridad y la gestión de datos.

b. Auditorías Externas

- Se contratarán auditores externos para llevar a cabo auditorías independientes del SIG-HOLON al menos una vez al año.
- Los auditores externos revisarán los controles de seguridad, la protección de datos y el cumplimiento normativo, proporcionando recomendaciones para mejoras.

c. Informes de Auditoría

- Los resultados de las auditorías serán documentados en informes detallados, los cuales serán revisados por el Órgano Colegiado Superior.
- Se desarrollarán planes de acción para abordar cualquier hallazgo o recomendación, y se realizará un seguimiento de la implementación de estos planes.

Artículo 38.- Consecuencias del Incumplimiento

a. Medidas Disciplinarias

- El incumplimiento de las políticas y procedimientos establecidos en esta normativa resultará en medidas disciplinarias, que pueden incluir advertencias, suspensión de acceso al sistema, y acciones legales si corresponde.
- Las medidas disciplinarias serán proporcionales a la gravedad de la infracción.

b. Proceso de Investigación

- Cualquier incidente de incumplimiento será investigado a fondo para determinar las causas y responsables y estará a cargo del Comité de Ética y un Técnico independiente.
- Los usuarios implicados tendrán la oportunidad de presentar su versión de los hechos antes de que se tomen decisiones finales sobre las medidas disciplinarias.

c. Reporte de Incidentes

- Los usuarios están obligados a reportar cualquier incidente de incumplimiento o sospecha de violación de esta normativa a la Coordinación de TICs.
- Se garantizará la confidencialidad de los reportes y la protección contra represalias para quienes reporten incidentes de buena fe.

Artículo 39.- Revisión y Actualización de la Normativa

1. Procedimiento de Revisión

a. Responsabilidad

- La responsabilidad de la revisión de esta normativa recae en la Coordinación de TICs, en colaboración de Asesoría Jurídica del Instituto Superior Tecnológico Pichincha.
- Se formará un comité de revisión compuesto por el Coordinador de TICs, la Secretaria Abogada del





Instituto y la Coordinación de Aseguramiento de la Calidad.

b. Proceso de Revisión

- Se recogerán comentarios y sugerencias de los usuarios y se evaluará el cumplimiento y la efectividad de la normativa actual.
- El comité de revisión analizará las propuestas de cambios y realizará las modificaciones necesarias.
- Las versiones revisadas de la normativa serán aprobadas por la alta dirección y comunicadas a todos los usuarios.

c. Frecuencia de Revisión:

1. Revisiones Anuales

- La normativa será revisada y, si es necesario, actualizada cada año para reflejar los cambios en el entorno tecnológico y regulatorio.
- Las revisiones anuales asegurarán que la normativa siga siendo adecuada para la protección del sistema y los datos que maneja.

2. Revisiones Adicionales

- Se realizarán revisiones adicionales cuando se identifiquen nuevas amenazas, se produzcan incidentes de seguridad significativos o se implementen nuevas funcionalidades en el SIG-HOLON.
- Las revisiones adicionales pueden ser producto de recomendaciones de auditorías internas o externas.

Artículo 40.- Aprobación de Modificaciones

a. Proceso de Aprobación

- Todas las modificaciones a esta normativa deberán ser aprobadas por la alta dirección del instituto.
- Las propuestas de modificación serán presentadas por el comité de revisión junto con una justificación detallada de los cambios.

b. Comunicación de Cambios

- Los cambios aprobados serán comunicados a todos los usuarios del SIG-HOLON mediante correos electrónicos y sesiones de capacitación específicas.

- Se actualizarán todos los documentos y recursos relacionados, incluyendo manuales de usuarios y materiales de capacitación, para reflejar las modificaciones.

c. Implementación

- Las modificaciones aprobadas serán implementadas de inmediato o según el plan de actualización establecido por el comité de revisión.

- Se realizará un seguimiento para asegurar que todos los usuarios comprendan y cumplan con las nuevas disposiciones de la normativa.

Artículo 41.- Responsabilidad de Coordinación y Gestión del SIG-HOLON.- La Coordinación de TICs es responsable de la administración y supervisión general del Sistema Informático de Gestión HOLON; con las siguientes actividades:

1. Gestión General del SIG-HOLON

- a. Incluye la planificación, implementación, mantenimiento y mejora continua del sistema con la asistencia especializada del proveedor

Artículo 42.- Estructura de la Coordinación

- a. Coordinador de TICs
- Responsable de la dirección y supervisión del equipo de TICs.-
- Asegurar el cumplimiento de las políticas y procedimientos establecidos para el SIG-HOLON.
- b. Equipo de Soporte Técnico.- Compuesto por técnicos especializados en la gestión y mantenimiento del SIG-HOLON. Y tiene como función proveer soporte de primer y segundo nivel a los usuarios.
 - c. Equipo de Seguridad Informática.- Encargado de la implementación y monitoreo de las medidas de seguridad del sistema; realiza auditorías de seguridad y gestionar incidentes de seguridad.
 - d. Equipo de Desarrollo y Actualización.- Responsable de la implementación de nuevas funcionalidades y actualizaciones del sistema (Proveedor).





Artículo 43.- Comunicación y Reportes

1. Comunicación Interna.- La Coordinación de TICs mantendrá una comunicación constante con las diferentes áreas del instituto para asegurar el alineamiento de las necesidades y expectativas con las capacidades del sistema.

- a. Informes Periódicos .- Se generarán informes periódicos sobre el estado del SIG-HOLON, incluyendo el desempeño, las incidencias y las actualizaciones realizadas. Estos informes serán presentados a la alta dirección del Instituto y utilizados para la toma de decisiones estratégicas.

Artículo 44.- Planificación y Estrategia.-

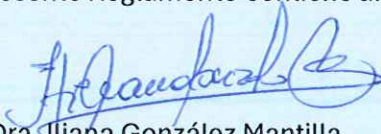
- b. Desarrollo de Estrategias a Largo Plazo.- la Coordinación de TICs desarrollará y actualizará continuamente una estrategia a largo plazo para la evolución del SIG HOLON, asegurando que el sistema siga cumpliendo con las necesidades del instituto.
- c. Evaluación de Nuevas Tecnologías.- Evaluar e incorporar nuevas tecnologías y prácticas que puedan mejorar la eficiencia y seguridad del SIG HOLON.

Artículo 45.- Gestión de Proyectos.- Planificar y gestionar proyectos relacionados con el desarrollo, mejora y expansión del SIG HOLON.

CERTIFICACION

En mi calidad de Secretaria Abogada del Instituto Superior Tecnológico Pichincha con condición de universitario, certifico que el presente reglamento de USO DEL SISTEMA INFORMATICO DE GESTION (SIG) HOLON-ISTP fue discutido y aprobado por el Órgano Colegiado Superior en sesión ordinaria de 30 de mayo del 2024, y sus reformas el 14 de junio del 2024

Se hace constar que el Presente Reglamento contiene anexos.


Dra. Iliana González Mantilla
SECRETARIA ABOGADA



ANEXO:

Formularios y Documentos Relevantes

- d. Formulario de Reporte de Incidentes
- e. Plantilla de Evaluación de Capacitación

Contactos Importantes

f. Soporte Técnico:

- a. Cristian López – clopez@tecnologicopichincha.edu.ec / 0987147686
- b. Mauricio Santillán – gsantillan@tecnologicopichincha.edu.ec / 0998523470
- c. Soporte – soporte@tecnologicopichincha.edu.ec

g. Administrador del Sistema:

- a. Cristian López – clopez@tecnologicopichincha.edu.ec / 0987147686

h. Coordinación de TICs:

- a. Mauricio Santillán – gsantillan@tecnologicopichincha.edu.ec / 0998523470

