UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

RESOLUCIÓN OCS-SO-007-No.086-2020

EL ÓRGANO COLEGIADO ACADÉMICO SUPERIOR

CONSIDERANDO:

Que, la Constitución de la República del Ecuador en el artículo 18, numerales 1 y 2 establece que, todas las personas, en forma individual o colectiva, tienen derecho a: 1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior. 2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. (…);

Que, el artículo 233 del Texto Mayor de la República establece que: Ninguna servidora ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones, o por sus omisiones, y serán responsables administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos. (…);

Que, el artículo 355 de la Carta Suprema, entre otros principios, establece que el Estado reconocerá a las universidades y escuelas politécnicas autonomía académica administrativa, financiera y orgánica, acorde con los objetivos del régimen de desarrollo y los principios establecidos en la Constitución. Se reconoce a las universidades y escuelas politécnicas el derecho a la autonomía, ejercida y comprendida de manera solidaria y responsable. Dicha autonomía garantiza el ejercicio de la libertad académica y el derecho a la búsqueda de la verdad, sin restricciones; el gobierno y gestión de sí mismas, en consonancia con los principios de alternancia, transparencia y los derechos políticos; y la producción de ciencia, tecnología, cultura y arte;

Que, en el artículo 17 de la Ley Orgánica de Educación Superior se detalla que el Estado reconoce a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los principios establecidos en la Constitución de la República;

Que, el artículo 18 literal e) de la Ley Orgánica de Educación Superior respecto al ejercicio de la autonomía responsable establece que las universidades y escuelas politécnicas tendrán libertad para gestionar sus procesos internos;

Que, la Ley Orgánica de Servicio Público en su artículo 4 prescribe**. -** Serán servidoras o servidores públicos todas las personas que en cualquier forma o a cualquier título trabajen, presten servicios o ejerzan un cargo, función o dignidad dentro del sector público. (…);

Que, los literales a, b, h e inciso segundo del artículo 22 de la Ley Orgánica de Servicio Público prescribe: Son deberes de las y los servidores públicos; a) Respetar, cumplir y hacer cumplir la Constitución de la República, leyes, reglamentos y más disposiciones expedidas de acuerdo con la Ley; b) Cumplir personalmente con las obligaciones de su puesto, con solicitud, eficiencia, calidez, solidaridad y en función del bien colectivo, con la diligencia que emplean generalmente en la administración de sus propias actividades; h) Ejercer sus funciones con lealtad institucional, rectitud y buena fe. Sus actos deberán ajustarse a los objetivos propios de la institución en la que se desempeñe y administrar los recursos públicos con apego a los principios de legalidad, eficacia, economía y eficiencia, rindiendo cuentas de su gestión. - Custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o comisión tenga bajo su responsabilidad e impedir o evitar su uso indebido, sustracción, ocultamiento o inutilización;

Que, el mismo cuerpo legal en el Capítulo 4 del Régimen Disciplinario artículo 41 establece que; la servidora o servidor público que incumpliere sus obligaciones o contraviniere las disposiciones de esta Ley, sus reglamentos, así como las leyes y normativa conexa, incurrirá en responsabilidad administrativa que será sancionada disciplinariamente, sin perjuicio de la acción civil o penal que pudiere originar el mismo hecho. (…);

Que, el artículo 42 de la Ley Orgánica de Servicio Público determina que: Se considera faltas disciplinarias aquellas acciones u omisiones de las servidoras o servidores públicos que contravengan las disposiciones del ordenamiento jurídico vigente en la República y esta ley, en lo atinente a derechos y prohibiciones constitucionales o legales. Serán sancionadas por la autoridad nominadora o su delegado. (…);

Que, el artículo 1 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos establece que esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas;

Que, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en el Capítulo I de los Principios Generales artículo 5.- Confidencialidad y reserva**. -** Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia;

Que, el artículo **7** de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, sostiene que: Cuando la ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la ley, puede comprobarse que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos;

Que, el artículo 9 del mismo cuerpo legal, en la Protección de datos, sostiene que: Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.- La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. (…);

Que, el Título V de las Infracciones Informáticas, Capítulo I artículo 57 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, sostiene que: Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley;

Que, la Ley de Transparencia y Acceso a la Información Pública en el artículo 1 establece que: El acceso a la información pública es un derecho de las personas que garantiza el Estado;

Que, el artículo 5 de la Ley de Transparencia y Acceso a la Información Pública prescribe: Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado;

Que, el artículo. 6 del mismo cuerpo legal preceptúa: Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, (…). - El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. (…);

Que, la Ley de Transparencia y Acceso a la Información Pública en el artículo 10 establece: Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción.- Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, pérdida y/o desmembración de documentación e información pública. Los

documentos originales deberán permanecer en las dependencias a las que pertenezcan, hasta que sean transferidas a los archivos generales o Archivo Nacional;

Que, el Código Orgánico Integral Penal en el Art. 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.- Con igual pena será sancionada la persona que: 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. - 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general;

Que, el Código Orgánico Integral Penal en el Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años;

Que, el Reglamento General de la Ley Orgánica de Servicio Público Capítulo V del Régimen Disciplinario Sección I artículo 78 establece que: En el ejercicio de la potestad administrativa disciplinaria y sin perjuicio de las responsabilidades administrativas, civiles, o indicios de responsabilidad penal en las que pudiere incurrir la o el servidor público que incumpliere sus obligaciones o contraviniere las disposiciones previstas en la LOSEP, este Reglamento General, normas conexas y los reglamentos internos de cada institución que regulan sus actuaciones, la o el servidor será sancionado disciplinariamente conforme a las disposiciones establecidas en el Capítulo 4 del Título III de la LOSEP y en el presente Reglamento General.- Las sanciones se impondrán de conformidad con la gravedad de la falta;

Que, el artículo 79 del Reglamento General de la Ley Orgánica de Servicio Público determina que: Las UATH elaborarán obligatoriamente, en consideración de la naturaleza de la gestión institucional los reglamentos internos de administración del talento humano, en los que se establecerán las particularidades de la gestión institucional que serán objeto de sanciones derivadas de las faltas leves y graves establecidas en la Ley;

Que, la Sección II, de las sanciones artículo 80 del Reglamento General de la Ley Orgánica de Servicio Público determina: Todas las sanciones disciplinarias determinadas en el artículo 43 de la LOSEP, serán impuestas por la autoridad nominadora o su delegado, y ejecutadas por la UATH, previo el cumplimiento del procedimiento establecido en este Reglamento General. (…);

Que, el Esquema Gubernamental de Seguridad de la Información (Acuerdo Ministerial 025-2019) en su Disposición General Séptima manifiesta que: Es responsabilidad de la máxima autoridad de cada entidad gestionar la implementación del Esquema General de Seguridad de Información (EGSI) asignado los recursos necesarios;

Que, el artículo 7 del Esquema Gubernamental de Seguridad de la Información (Acuerdo Ministerial 025-2019) expresa que: Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 "Gestión del Riesgo en la Seguridad de la Información;

Que, el artículo 5 del EGSI manifiesta que: La máxima autoridad designará al interior de su Institución, un Comité de Seguridad de la Información(...) y su artículo 7 señala que el Comité de Seguridad de la Información (CSI) designará al interior de su Institución a un funcionario como Oficial de Seguridad de la Información (OSI).

Que, el Código Orgánico Integral Penal en el Art. 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.- Con igual pena será sancionada la persona que: 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. - 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad;

Que, el Estatuto de la universidad en el artículo 34, numeral 2, establece como atribuciones y deberes del Consejo Universitario expedir los reglamentos generales de la universidad.

Que, a través de oficio No. 039-2018-CJLR, de 20 de agosto de 2018, el Dr. Lenín Arroyo Baltán, Presidente de la Comisión Jurídica, Legislación y Reclamos, informó a la Dra. Iliana Fernández Fernández, Ph.D., Rectora (e) de la Universidad, que la Comisión Jurídica, Legislación y Reclamos, en sesiones ordinarias del 23 de julio y 16 de agosto de 2018, revisó y aprobó en primer y segundo debate el proyecto de Reglamento de Seguridad de la Información de la Universidad Laica "Eloy Alfaro" de Manabí y solicita se lo traslade al Órgano Colegiado Superior, para su análisis y aprobación en primer debate;

Que, el Órgano Colegiado Superior mediante Resolución RCU-SO-007-Nro.156-2018, adoptada en la Séptima Sesión Ordinaria efectuada el 31 de agosto de 2018, RESOLVIÓ: "(…) Aprobar en primer debate el proyecto de Reglamento de Seguridad de la Información de la Universidad Laica "Eloy Alfaro" de Manabí y disponer a la Secretaría General que remita las observaciones sugeridas por los

Miembros del Órgano Colegiado Superior, a la Comisión Jurídica, Legislación y Reclamos, para su análisis, consideración e informe correspondiente, previo a su aprobación en segundo debate";

Que, a través de oficio No. 018-2020-CJL, de 25 de agosto de 2020, el Dr. Lenin Arroyo Baltán, Presidente de la Comisión Jurídica y Legislación, presentó al Arq. Miguel Camino Solórzano, Ph.D., Rector de la IES, informe para aprobación en segundo debate del Proyecto de REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ, con observaciones a su texto, las mismas que constan en el documento de la referencia;

Que, el Órgano Colegiado Superior, mediante Resolución OCS-SO-007-No.086-2020, adoptada en la Séptima Sesión Ordinaria efectuada el 31 de agosto de 2020, RESOLVIÓ: "(…) Aprobar en segundo debate el **Proyecto de REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ** (…)"; con las observaciones que constan en la antes indicada Resolución;

En ejercicio de las atribuciones que le confieren el artículo 355 de la Constitución y el artículo 34, numeral 2 del Estatuto de la Universidad;

RESUELVE:

Expedir el siguiente:

REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

CAPITULO I
DEL OBJETO, OBJETIVOS Y ÁMBITO DE APLICACIÓN DEL REGLAMENTO

Artículo 1.- Del Objeto. - El presente reglamento tiene por objeto establecer las normas y políticas para el cumplimento de obligaciones que rijan y garanticen la seguridad integral de la información institucional, sea esta física o digital de la Universidad Laica "Eloy Alfaro" de Manabí, regulando y controlando el ingreso y la gestión de la información en todo su ciclo de vida y formatos

Artículo 2.- Objetivos.- Este reglamento se constituye en un instrumento destinado a mejorar el desempeño informático de autoridades, docentes, servidoras y servidores y trabajadoras/es, estudiantes y usuarios externos de la Uleam, a efectos de proteger la información mediante la implementación de medidas de seguridad preventivas, detectivas, de repuesta y de recuperación, que contribuyan a garantizar la confidencialidad, integridad y disponibilidad de la información física y digital; gestión que a su vez debe estar alineada al cumplimiento de los objetivos institucionales y de las directrices que emanen del Comité Informático.

Artículo 3.- Ámbito de aplicación.- Se encuentran comprendidas en el presente reglamento todos los estamentos del quehacer universitario, es decir, Autoridades, Personal Académico, Personal Administrativo, Personal de Servicios, Estudiantes; incluyendo a Usuarios Externos.

Artículo 4.- Integración del Comité.- La Universidad Laica Eloy Alfaro de Manabí tiene constituido el Comité de informática, establecido en el Estatuto en su artículo 59, por lo que se conformará el Comité de Seguridad de la Información, de sus miembros ya determinados:

1. El/la Gerente Administrativo/a
2. El/la Secretario/a General
3. El/la Directora/a de Informática e Innovación Tecnológica
4. El/la directora/a de Comunicación e Imagen Institucional.
5. El/la directora/a de Asesoría Jurídica, con voz asesora y secretario del Comité.

CAPÍTULO II
CLASIFICACIÓN DE LA INFORMACIÓN

Artículo 5.- Clasificación de la Información. - En concordancia con la política de Seguridad de información, este reglamento clasifica la información como:

a) Grupo de información. - Es el conjunto de datos o documentos físicos y digitales que tienen características comunes de agrupación, y, que conforman una unidad de información independiente, tales como: base de datos, información de proyectos. expedientes de Talento Humano, etc.

b) Información Sensitiva Alta. - Es la información sujeta a restricción, con acceso restringido a un número limitado de servidores autorizados por la institución y comprende entre otros a:

- Datos personales de los servidores públicos y estudiantes de la Institución que se encuentren en sistemas, documentos, repositorios o almacenamiento de tipo físico y digital.

- Las estructuras de base de datos, diccionarios de datos, metadata, modelos entidad relación, procedimientos almacenados o cualquier otra característica técnica de las bases de datos institucionales o infraestructura tecnológica.

- La información técnica de los programas y sistemas tales como códigos fuentes, log de auditoria; programas o scripts de configuración, scripts o programas para ejecutar procesos individuales o por lotes que consten en funcionalidades liberadas para usuarios finales, estructura de directorio, detalles de la arquitectura

tecnológica, detalles técnicos sobre infraestructura o cualquier otro recurso técnico de los sistemas.

- La Información técnica de los Sistemas, en especial la relacionada con los módulos de seguridad, módulos de auditoría y repositorios de información o base de datos.

c) Información General. - Es aquella creada en los procesos administrativos, financieros, tecnológicos y de control de la Universidad Laica "Eloy Alfaro" de Manabí.

CAPÍTULO III
RESTRICCIONES Y PROHIBICIONES

Artículo 6.- Restricciones al uso y acceso a la información institucional. - La política de seguridad de la información y este reglamento establecen, entre otras, las siguientes restricciones:

1. El uso y acceso a la información institucional contenida en los repositorios centrales de almacenamiento, estarán restringidos según el nivel de sensibilidad de la información y aplicación de las medidas de protección que corresponda.

2. Será responsabilidad del servidor o servidora aplicar las medidas de protección que sean necesarias para proteger la información institucional, a fin de minimizar el riesgo de acceso y uso no autorizado, para evitar impacto negativo a la imagen y gestión de la institución y/o en perjuicio de la Universidad Laica "Eloy Alfaro" de Manabí, responsables o terceros.

3. Los usuarios de los servicios y sistemas no deben divulgar a terceras personas y/o partes, las credenciales de autenticación y acceso a los servicios y sistemas de información que la institución pone a su disposición, para realizar las actividades inherentes a sus roles y funciones.

Artículo 7.- Prohibiciones al uso y acceso a la información institucional. - La política de seguridad de la información y este reglamento establecen, entre otras, las siguientes prohibiciones:

1. Intentar vulnerar las seguridades de los diferentes sistemas (físicos o digitales), acceso a red, internet y del servicio de correo electrónico institucional.

2. Acceder a la información no autorizada, no asignada o no permitida.

Artículo 8.- Sanciones.- Los Docentes o Estudiantes que revelen, dispongan, guarden, extraigan, archiven, reproduzcan, modifiquen y/o eliminen información con fines ajenos al ejercicio específico de sus funciones, serán sancionado según corresponda, garantizando el debido proceso y el derecho a la defensa,

conforme al Régimen Disciplinario establecido en la Ley Orgánica de Educación Superior LOES y en el estatuto de la Universidad, sin perjuicio de las sanciones tipificadas en el Código Orgánico Integral Penal.

El servidor o servidora administrativo/a o de servicio que revele, disponga, guarde, extraiga, archive, reproduzca, modifiquen y/o elimine información con fines ajenos al ejercicio específico de sus funciones será sancionado según corresponda, garantizando el debido proceso y el derecho a la defensa, conforme a lo establecido en la Ley Orgánica de Servicio Público LOSEP, el Código de Trabajo, respectivamente, y en el Estatuto Universitario, sin perjuicio de las sanciones tipificadas en el Código Orgánico Integral Penal.

CAPÍTULO IV
DE LOS USUARIOS FINALES

Artículo 9.- Usuarios finales. - Los usuarios finales o usuarios de sistemas son las personas que tienen credenciales de autenticación y autorización para utilizar u operar los servicios y sistemas que la institución pone a su disposición en el ámbito de sus funciones.

Los Usuarios finales utilizarán los servicios y sistemas de información de la Universidad únicamente para los propósitos autorizados en el ámbito de las funciones propias de su cargo y roles asignados; y, estarán obligados a sustentar y documentar el uso de las opciones de los diferentes servicios y sistemas de información que contengan sus roles o perfiles de usuario.

En caso de que, en el rol o perfil de usuario final, tuviera activada opciones que no correspondan a sus funciones deberá abstenerse de utilizar dichas opciones y notificar de manera inmediata a la Autoridad competente.

Artículo 10.- Captura y Procesamiento de Datos. - En relación con los datos que captura, procesa y presentan los sistemas para usuarios finales, la Dirección de Informática e Innovación Tecnológica permitirá los accesos únicamente desde las funcionalidades o aplicaciones que haya liberado para tal efecto y de acuerdo a los roles establecidos.

Artículo 11.- Responsabilidad para el acceso y uso de servicios y sistemas de información. - Para garantizar el uso responsable y la seguridad de los sistemas de información propiedad de la Uleam, se establece la firma de un Acuerdo para el Acceso y Uso Responsable de Servicios de Sistemas de Información.

Para estudiantes y usuarios externos, el Acuerdo para el Acceso y Uso Responsable de Servicios y Sistemas de Información, deberá ser aceptado de forma electrónica e impreso, y una vez firmado deberá entregarse en la unidad académica o administrativa que corresponda; en el caso de estudiantes la impresión y entrega del documento será solamente por una ocasión.

CAPÍTULO V
DE LA DIRECCIÓN DE INFORMÁTICA E INNOVACIÓN TECNOLÓGICA

Artículo 12.- Competencia de la DIIT. - En el ámbito de su competencia a la Dirección de Informática e Innovación Tecnológica le corresponde la identificación y mitigación de los riesgos tecnológicos y de seguridad de los activos de información bajo su competencia y responsabilidad.

Artículo 13.- Personal Técnico y no Técnico.- Las personas que participen en proyectos de desarrollo de aplicaciones, procesos de Extracción, Transformación y Carga (ETL por sus siglas en inglés), procesos de inteligencia de negocios o procesos de administración de redes de la Dirección de Informática e Innovación Tecnológica DIIT, podrán tener acceso a información técnica únicamente en ambientes de "desarrollo y pruebas" bajo el principio del menor privilegio y será concedido por autorización del Director/a de la DIIT por el tiempo de participación en los proyectos.

Artículo 14.- Del acceso para el personal del Área de Desarrollo. - En cuanto a los accesos para el área de desarrollo, los funcionarios de esta área solo tendrán acceso a los ambientes de "desarrollo y pruebas" con herramientas autorizadas para tal efecto con todos los privilegios que requieran para llevar a cabo sus funciones.

Artículo 15.- Del Área de Operaciones. - El personal del área de Operaciones tendrá privilegios controlados con fines específicos previa solicitud del Director de Informática e Innovación Tecnológica y posterior autorización del Rector/a, en el ámbito de sus procesos y/o competencias, esto exclusivamente para el ambiente en producción.

Artículo 16.- Implementación y Despliegue de Sistemas. - Si la implementación, despliegue o mantenimiento de los diferentes sistemas requiere que el personal de operaciones realice actividades de inserción, modificación o eliminación de datos, estas actividades deberán contar con la autorización escrita de las máximas autoridades de la institución, de acuerdo a su ámbito y competencias y con el sustento suficiente para realizar dichos cambios.

Artículo 17.- Responsabilidades del Director de la Dirección de Informática e Innovación Tecnológica. - Las Atribuciones y Responsabilidades del Director de la Dirección de Informática e Innovación Tecnológica (DIIT) en el ámbito de la seguridad de la información, serán entre otras, las siguientes:

a) Definir procedimientos para el control de cambios a los procesos operativos, los sistemas e instalaciones, de manera que no afecten la seguridad de la información.
b) Establecer criterios de seguridad para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas antes de su aprobación definitiva.

c) Evaluar el posible impacto operativo a nivel de seguridad de los cambios previstos a sistemas y equipamiento, asignando responsabilidades.
d) Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
e) Asegurar el registro de las actividades realizadas por el personal en ambiente de producción.
f) Monitorear el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permitan tomar medidas correctivas.
g) Implementar los controles de seguridad definidos a nivel de estaciones de trabajo, a nivel perimetral y por segmento de usuarios, y

Las demás que por naturaleza de las actividades de gestión de la seguridad de la información deban ser cumplidas y ejecutadas conforme a la ley.

CAPÍTULO VI
DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y EL OFICIAL DE SEGURIDAD DE INFORMACIÓN

Artículo 18.- La Universidad contará con un Comité de Seguridad de la Información que tendrá como objetivo, garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la institución. El Comité en su primera convocatoria definirá su agenda y su reglamento interno.

Artículo 19.- El Comité de Seguridad de la Información, tendrá las siguientes responsabilidades:

a) Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución,

b) Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto dentro de la organización.

d) Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios de la administración central y procesos académicos, en base al Esquema Gubernamental de Seguridad de la Información (EGSI).

e) Promover la difusión de la seguridad de la información dentro de la institución.

f) Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.

g) El comité deberá convocarse trimestralmente o cuando las circunstancias lo ameriten, se deberá llevar registros y actas de las reuniones.

h) Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), como modelo adaptado dentro de la Universidad.

i) Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema de Seguridad de la Información aplicado en la Institución.

j) Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

Artículo 20.- La Universidad contará con un Oficial de Seguridad de la Información con sus respectivas funciones y responsabilidades determinadas en este Reglamento. El Oficial responderá al Comité de Seguridad de la Información y a la máxima autoridad de la Institución.

Artículo 21.- El Oficial de Seguridad de la Información tendrá las siguientes responsabilidades:

a) Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del Esquema de Seguridad de la Información de la Institución.

b) Generar propuestas para la elaboración de la documentación esencial del Esquema de Seguridad de la Información de la Institución.

c) Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas.

d) Elaborar el Plan de concienciación en Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información adaptado a la Institución.

e) Elaborar un plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas.

f) Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información

g) Orientar y generar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información presentados al interior de la institución.

h) Coordinar la gestión de incidentes de seguridad con nivel de impacto alto con la máxima autoridad, el Comité de Seguridad de la Información, y al interior de la Institución.

i) Mantener la documentación de la implementación del Esquema de Seguridad de la Información de la Institución debidamente organizada.

j) Verificar el cumplimiento de las normas procedimientos y controles de seguridad institucionales establecidos.

k) Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información adaptado a la Institución, así como las alertas que impidan su implementación.

l) Previa la terminación de sus funciones el Oficial de Seguridad realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de Seguridad, en caso de ausencia, al Comité de Seguridad de la Información.

Artículo 22.- De la confidencialidad de la información personal e información técnica. - Para garantizar la confidencialidad de la información de los servicios y sistemas, se establece la firma de acuerdos de Confidencialidad para la protección de los datos personales y los datos de clasificación Sensitiva Alta de la Institución.

DISPOSICIONES GENERALES

PRIMERA. - El Comité de Seguridad de la Información a través de la Dirección de Informática e Innovación Tecnológica, enviará la terna correspondiente ante el Señor Rector para que designe a un funcionario como Oficial de Seguridad de la Información. El Oficial de Seguridad debe tener conocimiento en Seguridad de la Información y Gestión de Proyectos, formación académica en Tecnologías de la Información de al menos tercer nivel, y un mínimo de tres años de experiencia profesional en el ámbito de Seguridad, Infraestructura y Sistemas Informáticos."

SEGUNDA. - La Dirección de Talento Humano definirá como política para el ingreso o vinculación laboral del personal a la universidad, bajo cualquier modalidad (nombramiento, contrato ocasional o servicios profesionales), suscribir el Acuerdo para el Acceso y Uso Responsable de Servicios de Sistemas de Información, manteniéndolo en el expediente físico del servidor.

DISPOSICIONES TRANSITORIAS

PRIMERA. - En el plazo de sesenta (60) días a partir de la entrada en vigencia del presente reglamento, la máxima autoridad de la Universidad designará la conformación del CSI, considerando los aspectos de educación virtual y teletrabajo.

SEGUNDA. - En un plazo máximo de sesenta (60) días, a partir de la conformación del CSI, se designará al Oficial de Seguridad de la Información de la Institución, a través de una terna propuesta por el CSI y enviada a la máxima autoridad para su designación.

TERCERA. - En el plazo de noventa (90) días a partir de la entrada en vigencia del presente reglamento, cada Dirección y Unidad Académica de la

Institución clasificará la información física y digital que corresponda como Información Sensitiva Alta. Esta clasificación será enviada al Oficial de Seguridad de Información y a la Dirección de Informática e Innovación Tecnológica, a través del formato documental que se haga llegar para el efecto.

CUARTA. - Para dar cumplimiento a lo establecido en el artículo 10 de este reglamento, La Dirección de Talento Humano deberá en un plazo de noventa (90) días a partir de la entrada en vigencia del presente reglamento, suscribir el Acuerdo para el Acceso y Uso Responsable de Servicios y Sistemas de Información con cada uno de los Servidores Públicos de la Institución, de los diferentes regímenes laborales.

QUINTA. - En el plazo de noventa (90) días a partir de la entrada en vigencia del presente Reglamento, la Dirección de Informática e Innovación Tecnológica, elaborará el Acuerdo Electrónico para el Acceso y Uso Responsable de Servicios de Sistemas de Información para estudiantes y usuarios externos, el mismo que se incluirá como una opción que requiera aceptación en los sistemas de información.

SEXTA. - En el plazo de ciento veinte (120) días a partir de la entrada en vigencia del presente Reglamento, el Comité de la Seguridad la Información elaborará y revisará las reformas necesarias al Estatuto para que se incluyan las funciones y responsabilidades del Comité de la Seguridad la Información, de la DIIT, y del Oficial de Seguridad de Información, para que sean enviadas posteriormente al Órgano Colegiado Superior para su conocimiento y aprobación.

DISPOSICIÓN DEROGATORIA

PRIMERA. - Se derogan todas las normas de igual o inferior jerarquía contrarias al contenido del presente reglamento, emitidas en la Universidad.

DISPOSICIÓN FINAL

El presente reglamento entrará en vigencia a partir de su aprobación por parte del Órgano Colegiado Superior (OCS), y publicado en la página oficial de la Universidad Laica "Eloy Alfaro" de Manabí.

Dado y firmado en la sala de sesiones del Órgano Colegiado Superior el 31 de agosto de 2020.

Arq. Miguel Camino Solórzano, RECTOR
Rector de la Universidad

Lcdo. Pedro Roca Piloso, PhD.
Secretario General

LA SECRETARÍA GENERAL DE LA UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

El infrascrito Secretario General de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICA que el **REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ,** fue aprobado por el Órgano Colegiado Superior en primera instancia en la Séptima Sesión Ordinaria, realizada el 31 de agosto de 2018, mediante Resolución RCU-SO-007-Nro.156-2018 y en segundo debate en la Séptima Sesión Ordinaria, efectuada el 31 de agosto de 2020, mediante Resolución OCS-SO-007-No.086-2020.

Manta, 31 de agosto de 2020