UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

COD: USIN-EGSI-V1-2021-007

SANGOLQUI - ECUADOR
2021

INDICE:

1. REFERENCIAS

- Constitución de la República, Registro Oficial 449 de 20-oct.-2008

- Ley Orgánica de Transparencia y Acceso a la Información Pública LOTAIP, Registro Oficial Suplemento 337 de 18-may.-2004

- REGLAMENTO A LA LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, Número de registro: R.O. 310 Año 2008.

- ACUERDO No. SGPR-2019- 0107, emitido por la Presidencia de la República del Ecuador, del 10 de abril del 2019.

- Norma de Gestión Documental para Entidades de Administración Pública, Registro Oficial Suplemento 445 de 25-feb.-2015

- Acuerdo Ministerial No. 025-2019, del Ministerio de Telecomunicaciones y Sociedad de la Información, publicado en el Registro Oficial Edición Especial 228 del 10 de enero de 2020, mediante el cual se publica el Esquema Gubernamental de Seguridad de la Información (EGSI) v2.0, el cual es una traducción similar de la norma técnica ecuatoriana NTE-INEN ISO/IEC 27002:2017 que establece el código de prácticas para los controles de seguridad de la información.

- Orden General 043, Artículo 2°. - Acuerdo Ministerial Nro.- 134 del Ministerio de Defensa Nacional, acuerda, Art. 1: "Expedir la Directiva para la implementación del Esquema Gubernamental de Seguridad de la Información-EGSI 2.0, en el Comando Conjunto de las Fuerzas Armadas, Fuerzas: Terrestre, Naval y Aérea e Institutos Adscritos al Ministerio de Defensa Nacional".

- Acuerdo Ministerial N°. 372 del Ministerio de Defensa Nacional, en el que se acuerda expedir: "REGLAMENTO INTERNO PARA LA ELABORACIÓN, MANEJO, CUSTODIA, DIFUSIÓN Y SEGURIDAD DE LA INFORMACIÓN MILITAR CLASIFICADA".

- Estatuto de la Universidad de la Fuerzas Armadas – ESPE, aprobado por el Honorable Consejo Universitario

- Política de Seguridad de la Información, constante en la "*Actualización de las Políticas Generales y Específicas de Gestión Institucional al 2021*" de la Universidad de las Fuerzas Armadas - ESPE, documento anexo en la Orden de Rectorado Nro. 2020-029-ESPE-a-1 del 10 de febrero de 2020.

- Memorando Nro. ESPE-REC-2020-0736-M del 27 de julio de 2020, el señor rector de la Universidad de las Fuerzas Armadas – ESPE, conforma el Comité de Seguridad de la Información (CSI); y designó a los miembros del mismo.

- Memorando Nro. ESPE-VAG-2020-1296-M, del 18 de agosto de 2020, el señor Vicerrector Académico General, en su calidad de Presidente del Comité de Seguridad de la Información (CSI), informa al Sr. Rector; que el 31 de julio de 2020, se sesionó y resolvió ratificar a los miembros y designar a un secretario del Comité; y designar al Oficial de Seguridad de conformidad a lo establecido en el Art. 7. Del Acuerdo Ministerial No. 025-2019, el cual señala: *"El Comité de Seguridad de la Información (CSI) designará al interior de su institución e aun funcionario como Oficial de Seguridad de la Información (OSI)"*.

- Orden de Rectorado 2020-176-ESPE-a-1 del 15 de agosto de 2020, mediante la cual se resuelve:

    - **Art. 1.-** Designar a partir del 27 de julio de 2020, a los miembros del Comité de Seguridad de la Información (CSI).

- **Art. 2.-** Designar al Ing. Mauricio Javier Baldeón Garzón, Mgs., como Oficial de Seguridad de la Información de la Universidad de las Fuerzas Armadas – ESPE.

- **Art. 3.-** Los miembros del Comité de Seguridad de la Información y el Oficial de Seguridad de la Información de la Universidad de las Fuerzas Armadas – ESPE, respectivamente, deberán cumplir con sus atribuciones y responsabilidades de conformidad a lo establecido en el Acuerdo Ministerial No. 025-2019, del 20 de septiembre de 2019, del Ministerio de Telecomunicaciones y Sociedad de la Información, con el que se expide el Esquema Gubernamental de Seguridad de la Información-EGSI, y demás normativas correspondientes.

- **Art. 4.-** Esta Orden de Rectorado tiene vigencia a partir de su emisión y se responsabiliza de su estricto cumplimiento en sus ámbitos de competencia a los señores: Miembros del Comité de Seguridad de la Información (CSI) y al Oficial de Seguridad de la Información de la Universidad de las Fuerzas Armadas – ESPE. Y para conocimiento: Rectorado y Auditoría Interna.

2. OBJETIVO

Incrementar la seguridad de los recursos de información de la Universidad de las Fuerzas Armadas – ESPE, y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales; con el fin de garantizar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información mediante la implementación de lineamientos y procedimientos definidos en los diferentes ámbitos de gestión institucional.

3. DECLARATORIA ESTATUTARIA

El Honorable Consejo Universitario de la Universidad de las Fuerzas Armadas – ESPE, considerando:

Que, el 16 de junio de 1922, el señor doctor José Luis Tamayo, Presidente de la República, decreta la creación de la Escuela de Oficiales Ingenieros, raíz fecunda de la Escuela Técnica de Ingenieros creada en 1947, la que se constituye en Escuela Politécnica del Ejército, mediante Decreto Supremo No. 2029 publicado en el Registro Oficial No. 487 de 20 de diciembre de 1977, con domicilio en la ciudad de Quito y sede principal en la ciudad de Sangolquí, provincia de Pichincha;

Que, la Universidad Naval Comandante Rafael Morán Valverde, fue creada mediante Ley No. 2005-26 publicada en el Registro Oficial No. 182 de 6 de enero de 2006, como universidad particular autofinanciada, con sede principal en el cantón Salina, provincia del Guayas, ubicada actualmente en la provincia de Santa Elena, en razón de la división política territorial de la provincia del Guayas;

Que, el Instituto Tecnológico Superior Aeronáutico, fue creada por el Ministerio de Educación y Cultura, mediante acuerdo No. 3237 de 8 de noviembre de 1999; y registrado por el CONESUP con el número 05-003, con fecha 22 de septiembre de 2000, como institución particular cofinanciada, con sede en la ciudad de Latacunga, provincia de Cotopaxi;

Que, en la Disposición Transitoria Vigésima Segunda de la Ley Orgánica de Educación Superior, LOES, publicada en el Suplemento del Registro Oficial No. 298 de 12 de octubre de 2010, se dispone que partir de la vigencia de la LOES, se integrarán la Escuela Politécnica del Ejército ESPE, la Universidad Naval Comandante Rafael Morán Valverde – UNINAV y el Instituto Tecnológico Superior Aeronáutico – ITSA, para conforma la Universidad de las Fuerzas Armadas "ESPE", para lo cual formulará el estatuto de la universidad, de acuerdo con sus fines y objetivos específicos, conforme a las políticas que defina el Ministerio de Defensa Nacional;

Que, una de las instituciones que se integra, tiene a su cargo exclusivamente la oferta de nivel técnico y tecnológico, como es el Instituto Tecnológico Superior Aeronáutico –ITSA;

Que, el segundo inciso del artículo 118 reformado de la ley Orgánica de Educación Superior, dispone que las universidades y escuelas politécnicas podrán otorgar títulos de tercer nivel técnico-tecnológico superior;

Que el Ministerio de Defensa Nacional emitió las políticas para la integración de la Universidad de las Fuerzas Armadas, el 4 de febrero de 2011;

Que, la Disposición Transitoria Décima Tercera de la Ley Orgánica Reformatoria a la ley Orgánica de Educación Superior dispone: *"[…] En el plazo de ciento ochenta (180) días los órganos colegiados superiores de las instituciones de educación superior deberán aprobar las reformas a los estatutos que entrarán en vigencia de manera inmediata y los remitirán al Consejo de Educación Superior para su validación y conformidad con la Ley.";* y,

Que, la Universidad de las Fuerzas Armadas-ESPE, es parte de las Fuerzas Armadas, única universidad militar del país, siendo su jurisdicción y competencia prioritaria la defensa y la seguridad nacional; lo que hace la dependencia a la entidad rectora (Ministerio de Defensa Nacional) y a la entidad ejecutora (Comando Conjunto de las Fuerzas Amadas), resuelve: **APROBAR LAS REFORMAS AL ESTATUTO DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS-ESPE; Y, SU CODIFICACIÓN**.

CAPÍTULO I, DE LA BASE LEGAL Y MISIÓN

Art. 1. La Universidad de las Fuerzas Armadas-ESPE, es una institución de educación superior; con personería jurídica, de derecho público y sin fines de lucro; con autonomía académica, administrativa, financiera, orgánica y patrimonio propio. Como institución de educación superior de las Fuerzas Armadas es dependiente del Comando Conjunto de las Fuerzas Armadas en: política institucional en el ámbito de educación superior, designación de autoridades ejecutivas; y asignación del personal militar necesario para el funcionamiento de la Universidad, conforme al presente estatuto.

El domicilio de la Universidad está en Quito y la Matriz principal en el Campus Sangolquí con sedes en Latacunga (campus "General de División Guillermo Rodríguez Lara" y campus centro), Salinas, Guayaquil, Santo Domingo de los Tsáchilas y Galápagos; se rige por la Constitución de la República del Ecuador, la Ley Orgánica de Educación Superior, la Ley Orgánica Reformatoria a la Ley Orgánica de Educación Superior, y su Reglamento, Ley Orgánica de Servicio Público, El código de Trabajo, la Ley de Personal de las Fuerzas Armadas, y otras leyes conexas, al presente Estatuto, los reglamento expedidos de acuerdo con la Ley y normas emitidas por el órgano rector de la política de educación superior, el Consejo de Educación Superior y el Consejo de Aseguramiento de la Calidad de la Educación Superior.

El orden interno en la Universidad de las Fuerzas Armadas-ESPE, es de exclusiva competencia y responsabilidad de sus autoridades.

Art. 2. La Universidad de las Fuerzas Armadas-ESPE, es una comunidad de autoridades militares y civiles, personal académico, estudiantes, personal administrativo y trabajadores. Su misión es formar profesionales o investigadores de excelencia, creativos, humanistas, con capacidad de liderazgo, pensamiento crítico y alta conciencia ciudadana; generar y aplicar el conocimiento científico; y transferir tecnología, en el ámbito de sus dominios académicos, para contribuir con el desarrollo nacional y atender las necesidades de la sociedad y de la Fuerzas Armadas; siendo su visión se reconocida como un referente a nivel nacional y regional por su contribución en el ámbito de sus dominios académicos, al fortalecimiento de la Seguridad y Defensa, bajo un marco de valores éticos, cívico y de servicio a la comunidad.

4. ÁMBITO DE APLICACIÓN

Geográfico: La Política de Seguridad de la Información se aplicará en la Universidad de la Fuerzas Armadas – ESPE: Matriz (campus Sangolquí), Sede Latacunga (campus "General de División Guillermo Rodríguez Lara" y

campus centro) Sede Santo Domingo de los Tsáchilas, Unidades Académicas Externas (Pichincha – Quito y Rumiñahui) y en el ámbito académico de las Unidades Académicas Especiales (Quito, Salinas, Ambato y Shell Mera).

Procesos de la Universidad: La Universidad de las Fuerzas Armadas – ESPE, es un sistema abierto que interactúa con el ambiente externo, razón por la cual la Política de Seguridad de la Información, se implementarán en los:

- Macro procesos de dirección o gobierno;
- Macro procesos habilitantes de asesoría;
- Macro procesos habilitantes de apoyo; y,
- Macro procesos agregadores de valor.

La Política de Seguridad de la Información debe ser conocida y entendida por todos los miembros de la Comunidad Universitaria y de estricta aplicación en todos los Procesos de la Universidad a nivel nacional.

5. DEFINICIONES

- **Acuerdo de Intercambio de Información:** Acuerdo entre las partes que intercambian información para garantizar tanto el uso que se la va a dar a la información como los niveles de protección.

- **Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (usuarios, procesos e infraestructura) que tenga valor para la organización.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.

- **Ambiente de Desarrollo:** Es el entorno de desarrollo que un programador requiere de forma obligatoria y que le permite escribir su código, diseñar y maquetar una interfaz, generar y consultar resultados de diversa índole, y servir o visualizar los cambios.

- **Ambiente de Producción:** Es un ambiente real donde se procesa la información.

- **Ambiente de Pruebas:** Es un entorno cerrado que aísla los cambios en el código, fruto de la experimentación, del propio entorno de producción o entorno de edición.

- **Ataque de fuerza bruta:** Un ataque de fuerza bruta ocurre cuando el atacante emplea determinadas técnicas para probar combinaciones de contraseñas con el objetivo de descubrir las credenciales de una potencial víctima y así lograr acceso a una cuenta o sistema.

- **Auditabilidad:** Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría

- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Además, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- **Autorización:** Proceso mediante el cual se permite a alguien a tomar una determinada acción concreta.

- **Clave pública:** Se utiliza principalmente para cifrar los datos y se puede entregar libremente, ya que se usará para cifrar datos, no para descifrarlos.

- **Clave privada:** Se utiliza para descifrar los datos que se contraparte, la clave pública, ha cifrado. Esta clave debe protegerse ya que es la única clave que puede descifrar los datos cifrados.

- **Comité de Seguridad de la Información (CSI):** El Comité de Seguridad de la Información (CSI), es un cuerpo integrado por representantes del Vicerrector Académico General, Vicerrectorado de Docencia, Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología, Vicerrectorado Administrativo, Secretaria General, Unidad de Tecnologías de la Información y Comunicaciones, Unidad de Seguridad Integrada y Unidad de Asesoría Jurídica (Asesor del Comité de Seguridad de la Información) que tiene como objetivo, garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la Universidad de las Fuerzas Armadas - ESPE.

- **Confiabilidad de la Información:** Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

- **Confidencialidad:** Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Control de acceso:** Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad.

- **Cookies:** Es un paquete de datos que un navegador web almacena de forma automática en el ordenador de un usuario cuando esta visita una página web. La cookie es enviada desde el servidor al visitante de la página web. Posteriormente, cada vez que el usuario visite esa misma página web o alguna otra del mismo dominio, la cookie será leída por el navegador web, sin ser modificada, y devuelta al servidor web.

- **Copia de Seguridad:** Se refiere a la copia de archivos físicos, virtuales o bases de datos a un sitio secundario para su preservación en caso de falla del equipo u otra catástrofe. El proceso de copia de seguridad de los datos es fundamental para un plan de recuperación de desastres exitoso.

- **Credenciales:** Están conformadas por la cuenta de usuario y una contraseña.

- **Criptografía:** Técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.

- **Criptografía asimétrica:** Cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

- **Criptografía simétrica:** Cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.

- **Datos Personales:** Es aquella información de carácter personal o íntima, que son materia de protección.

- **Dirección IP:** Acrónimo de Protocolo de Internet. Un número único e irrepetible con el cual se identifica una computadora conectada a una red

- **Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

- **Dispositivo Móvil:** Es cualquier dispositivo electrónico que permita la comunicación a través de las redes de telefonía celular o de redes de conexión WIFI a internet, tales como computadores portátiles, tabletas electrónicas o teléfonos inteligentes, entre otros, los cuales también proporcionan capacidades de movilidad a sus usuarios

- **Equipos informáticos:** Son equipos que permiten almacenar y procesar información.

- **Ethical Hacking:** (Hackeo Ético), sirve para explotar las vulnerabilidades existentes en el sistema que se requiere evaluar, valiéndose de una prueba de intrusión, el cual permite verificar y evaluar la seguridad física y lógica de sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, otros componentes de la infraestructura tecnológica, con la intención de ganar acceso y demostrar que un sistema es vulnerable.

- **IMAP:** Se conoce como un protocolo de acceso a mensajes de internet. El cual; es un método de acceso a correos electrónicos en un servidor sin tener que descargarlos al disco duro local.

- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados. Es la consecuencia de la materialización de una amenaza sobre un activo. El costo para la institución de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros (Ej.: pérdida de reputación, implicaciones legales, entre otros).

- **Incidente de Seguridad de la Información:** Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad y disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o u intento o amenaza de romper los mecanismos de seguridad existentes

  Evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.

- **Información:** Es uno de los activos más importantes de las instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.

- **Instalaciones de procesamiento de la información:** Cualquier sistema de procesamiento de la información, servicio o infraestructura, o los lugares físicos que los albergan.

- **Integridad:** Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **Listas negras:** Es un mecanismo básico de control de acceso que permite el bloqueo a través de todos los elementos (direcciones de correo, usuarios, URLs, etc.), excepto aquellos indicados explícitamente. A los elementos en la lista se les deniega el acceso.

- **Malware:** Se refiere a cualquier tipo de “software malicioso” diseñado para infiltrase en los dispositivos informáticos sin conocimiento y consentimiento.

- **Oficial Seguridad de la Información (OSI):** Persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Comité de Seguridad de la Información, que así lo requieran

- **Parche:** Es informática, un parche es una actualización de un programa usado para solucionar problemas o la usabilidad de una versión previa de la aplicación.

- **Propiedad Intelectual:** Constituye el mecanismo más eficaz de protección e incentivación de la creatividad humana, al reconocer al autor del esfuerzo creativo la capacidad exclusiva de disponer explotar el resultado de tal esfuerzo.

- **Protocolo HTTPS:** Protocolo de aplicación de aplicación basado en HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

- **Puesto de Trabajo:** Lugar dispuesto para que los funcionarios o contratistas realicen las labores relacionadas con las funciones o el cumplimiento de las obligaciones contractuales, según el caso.

- **Remediación:** Acción que permite minimizar el impacto de las vulnerabilidades en la Organización.

- **Respaldo automático:** Se ejecuta bajo una frecuencia preestablecida, y es almacenado en equipos servidores centralizados administrador por la Unidad de Tecnologías de la Información y Comunicaciones. La información institucional respaldada debe estar debidamente identificada. Se deben ejecutar de acuerdo con el inventario de los activos de información de Tecnologías de la Información y Comunicaciones, previamente definidos. Los respaldos automáticos se almacenarán en las carpetas especificadas para ese efecto.

- **Respaldo bajo demanda:** Se ejecuta siempre que exista una solicitud específica por parte de los directores de la Unidades Académicas y Administrativas y corresponde a la información institucional almacenada en dispositivos móviles o fijos asignados a investigadores, docentes, servidores públicos o trabajadores de la Universidad.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Riesgo de la seguridad de la información:** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

- **Seguridad de la información:** La seguridad de la información garantiza la confidencialidad, disponibilidad y la integridad de la información. La seguridad de la información consiste en la aplicación y la gestión de los controles apropiados que implica la consideración de una amplia gama de amenazas, con el objetivo de garantizar el éxito comercial sostenido y la continuidad, y reducir al mínimo las consecuencias de los incidentes de seguridad de la información.

  La seguridad de la información se consigue mediante la implementación de un conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgos que se haya elegido y gestionado por medio de un SGSI, empleando políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados. Estos controles necesitan ser especificados, implementados, monitoreados revisados y mejorados cuando sea necesario, para garantizar que la seguridad y los objetivos de negocio y de seguridad específicos se cumplan. Se espera de estos controles de seguridad de la información sea pertinente para integrarse de forma coherente con los procesos de negocio de una organización.

- **Seguridad de los Activos de Información:** Es proteger, resguardar y asegurar la disponibilidad, confidencialidad e integridad de los activos de información y tecnologías para su procesamiento a efecto de garantizar la continuidad operacional de la Universidad de las Fuerzas Armadas – ESPE.

- **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizadas para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar la información.

- **Software:** Conjunto de programas y rutinas que permiten a las computadoras realizar determinadas tareas.

- **Software Libre:** El modelo de Software Libre se convierte en una política tecnológica, en donde el código abierto, las licencias de uso libre, el uso de estándares abiertos y el trabajo comunitario, facilitan la inclusión digital, la soberanía tecnológica y la innovación local, optimizando el gasto estatal, favoreciendo el desarrollo local y promoviendo la integración regional.

- **Spam:** Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

- **Tecnología de la Información:** Se refiere al hardware y software operados por la Universidad de las Fuerzas Armadas – ESPE o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Institución, sin tener en cuenta la tecnología utilizada, computación de datos, telecomunicaciones u otro tipo.

- **Teletrabajador:** Toda persona que tiene calidad de trabajador/a de conformidad como lo dispuesto en el Código de Trabajo, LOSEP, y que efectúe sus labores mediante teletrabajo fuera de las instalaciones en las que mantiene su actividad el empleador, sea de manera parcial o total; temporal o permanente.

- **Teletrabajo:** Una forma de prestación de servicios de carácter no presencial en jornadas ordinarias y especiales de trabajo a través de las cuales el trabajador/a realiza sus actividades fuera de las instalaciones del empleador, siempre que las necesidades y naturaleza del trabajo lo permitan, haciendo uso de las tecnologías de información y comunicación (TIC), tanto para su gestión como su administración y control. (Acuerdo Ministerial del Ministerio del Trabajo No. MDT-2016-190. Anexo 1).

- **Teletrabajo emergente:** Alternativa laboral de carácter no presencial, el cual constituye un mecanismo que facilita a la o el servidor público y trabajadores, la ejecución de sus actividades desde un lugar distintito al habitual, para mitigar la propagación de coronavirus (COVID-19).

- **Terceros:** Persona u organización ajena a la Universidad.

- **TIC:** Tecnologías de la Información y Comunicaciones.

- **VPN:** Por sus siglas en inglés, Virtual Private Network. Es una tecnología de red que se utiliza para conectar de manera segura una o más computadoras a una red privada utilizando Internet.

- **Videoconferencia:** Sistema interactivo que permite a varios usuarios mantener una conversación virtual por medio de la transmisión en tiempo real de video, sonido y texto a través de Internet

- **Vulnerabilidad:** Es la debilidad de un activo o control que puede ser explotada por una o más amenazas.

- **WIFI:** Tecnología que permite la interconexión inalámbrica de dispositivos electrónicos.

6. POLÍTICA GENERAL

Mediante Orden de Rectorado Nro. 2021-006-ESPE-a-1 del 12 de abril de 2021, el señor Rector de la Universidad de las Fuerzas Armadas – ESPE, resuelve: *"Art. 1.- Dictar, aprobar y poner en vigencia a partir de la presente fecha, las POLÍTICA GENERALES 2021 DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS-ESPE*".

Política General, numeral 1.4: "*Fortalecer los componentes del sistema de seguridad integrada: seguridad y salud ocupacional, seguridad ambiental, seguridad de la información y seguridad física*".

El señor Rector, las Autoridades Militares y Civiles de la Universidad de las Fuerzas Armadas – ESPE; manifiestan su compromiso con la seguridad de la información que se genera, utiliza, procesa, comparte y que se la almacena en medios electrónicos y escritos, clasificada como publica, confidencial y reservada; para lo cual en cumplimiento de la normativa vigente implementará los controles de seguridad establecidos en el Esquema Gubernamental de Seguridad de la Información (EGSI) v2.0; a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera.

Con la participación conjunta de los actores claves, se evaluará la eficacia de los controles implementados para mejorar permanentemente el Sistema de Gestión de Seguridad de la Información, de tal forma que permita alcanzar los objetivos establecidos por la Universidad para la gestión de seguridad de sus activos de información, superando las expectativas de los clientes y partes interesadas.

7. DISPOSICIONES GENERALES

a) Las disposiciones previstas en el presente documento son de aplicación obligatoria para autoridades militares y civiles, personal académico, estudiantes, personal administrativo y trabajadores de la Universidad de las Fuerzas Armadas – ESPE, relacionados con la ejecución de los procesos correspondiente.

b) Todos los aspectos que no se encuentren normados de forma expresa en el presente documento institucional o requieran ser modificados por la normativa vigente deberán ser complementados o suplidos en forma temporal por las disposiciones formales emitidas por parte del responsable de éste proceso y servicio, o su línea de supervisión jerárquica según corresponda, hasta la siguiente actualización del documento institucional.

c) El presente documento se encuentra alineado con la ***"Actualización de las Políticas Generales y Específicas de Gestión Institucional al 2021"*** y demás documentos institucionales vigente de la Universidad de las Fuerzas Armadas – ESPE.

d) La evaluación, supervisión y control del sistema de gestión de seguridad de la información implementado es de responsabilidad de la USIN, para lo cual presentará informes de evaluaciones con sus respectivos Planes de Acción para levantar no conformidades y acciones correctivas; así como también luego de las revisiones por la dirección dispondrá la implementación de acciones para aprovechar las oportunidades de mejora.

e) Autoridades militares y civiles, personal académico, personal administrativo y trabajadores de la Universidad de las Fuerzas Armadas – ESPE que incumplieren sus obligaciones o contravinieren las disposiciones descritas en la presente Política, así como las leyes y normativa conexa, incurrirá en responsabilidades administrativa que será sancionada disciplinariamente previa aplicación del debido proceso y cumpliendo las garantías establecidas en el artículo 76 de la Constitución de la Repúblicas del Ecuador.

f) De existir sugerencias por parte de los Directores de las Unidades Académicas y/o Administrativas, estas deberán ser remitidas formalmente al señor Presidente del Comité de Seguridad de la Información, fin sea consideradas en futuras actualizaciones del presente documento.

g) La información que se genere en los diversos procesos a través de los sistemas de información de la Universidad será responsabilidad del director de cada proceso.

h) Los directores de las Unidades Académicas y Administrativas, en cumplimiento a su rol de revisión y supervisión, otorgarán o revocarán accesos lógicos, autorizarán transacciones y operaciones, y aplicarán mecanismos de control sobre el talento humano bajo su dirección, de tal manera que se garantice la continua y permanente Seguridad de la Información que se genera, procesa, mantiene y elimina la Universidad de las Fuerzas Armadas – ESPE.

i) La Unidad de Tecnologías de la Información y Comunicaciones habilitará, deshabilitará o suspenderá los accesos lógicos para los aplicativos informáticos a Autoridades militares y civiles, personal académico, personal administrativo y trabajadores de acuerdo con lo solicitado por la Unidad de Talento Humano; y, a estudiantes según lo requerido por la Unidad de Admisión y Registro.

7.1. ROLES Y RESPONSABILIDADES

Rector: Responsable de aprobar la Política de Seguridad de la Información y de autorizar futuras modificaciones con la asesoría del Comité de Seguridad de la Información (CSI). Dispondrá la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en la Universidad de las Fuerzas Armadas – ESPE.

Comité de Seguridad de la Información (CSI): Órgano Colegiado Administrativo, destinado a asegurar la implantación del Esquema Gubernamental de Seguridad de la Información (EGSI) v2.0 en la Universidad de las Fuerzas Armadas - ESPE, responsable de:

- 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.

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

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

- Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.

- Promover la difusión de la Seguridad de la Información dentro de la institución.

- 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.

- Convocar a Sesiones Ordinarios de manera trimestral o cuando las circunstancias lo ameriten, se deberá llevar registros y actas de las reuniones.

- Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

- Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

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

- Revisar anualmente la Política de Seguridad de la Información, a efectos de mantenerla actualizada. Además, efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como: cambios tecnológicos, variación de los costos de los controles, reformas al estatuto orgánico por procesos, impacto de los incidentes de seguridad, entre otros.

Oficial de Seguridad de la Información (OSI): Funcionario de la Universidad de las Fuerzas Armadas – ESPE con conocimientos de Seguridad de la Información y Gestión de Proyectos, designado por el Comité de Seguridad de la Información (CSI). Se encarga de supervisar el cumplimiento de la Política de Seguridad de la Información y de coordinar las funciones del CSI. El Oficial de Seguridad de la Información tendrá las siguientes responsabilidades:

- Identificar todas las personas o instituciones públicas o privadas, que de alguna forman influyen o impactan en la implementación del EGSI.

- Generar propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI).

- Elaborar el Plan de concienciación en Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información (EGSI).

- Coordinar con la Unidad de Tecnologías de la Información y Comunicaciones la elaboración del Plan de Continuidad de TIC´s.

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

- Coordinar la gestión de incidentes de seguridad con nivel de impacto alto a través de otras instituciones.

- Mantener la documentación de la implementación del EGSI debidamente organizada.

- Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.

- Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), así como las alertas que impidan su implementación.

Directores de Sedes, Departamentos, Carreras y Unidades Administrativas: Son los responsables del cumplimiento de la Política de Seguridad de la Información por parte de su equipo de trabajo dentro de sus dependencias.

Director de la Unidad de Tecnologías de la Información y Comunicaciones: Verificará el cumplimiento de la presente Política en coordinación con la ejecución de los procesos de UTIC:

- Planificación de TI
- Desarrollo de Aplicaciones TIC
- Gestión Infraestructura de TIC´s
- Gestión de Provisión de servicio de TIC´s
- Control y evaluación de servicios y aplicativos de TIC´s

Emitir directrices y/o lineamientos para la ejecución de la seguridad de TI, realizando el control y evaluación continua.

Director de la Unidad de Talento Humano y Director de la Unidad Comunicación Social: En coordinación con el responsable de Cambio de Cultura Organizacional, comunicarán a los miembros de la Comunidad Universitaria, sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas procedimientos y prácticas que de ella surjan. Adicionalmente, tendrán a su cargo, de los cambios que en ella se produzcan y las tareas de capacitación continua en materia de seguridad de la información. La Unidad de Talento Humano será la responsable de la suscripción de los Acuerdos de Confidencialidad (entre otros).

Coordinador Jurídico: Verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la Universidad de las Fuerzas Armadas – ESPE con los contratistas. Además, asesorará en materia legal al Comité de Seguridad de la Información.

Propietarios de la Información: Responsables de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

Comunidad Universitaria y Terceros: Son las autoridades militares y civiles, personal académico, estudiantes, personal administrativo y trabajadores de la Universidad de las Fuerzas Armadas – ESPE (bajo cualquier modalidad de prestación de servicios); contratistas, proveedores y cualquier otra persona u organización que por su relación con la Institución tenga acceso a la información y hagan uso de los activos de información y los sistemas para procesamiento; responsables de conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigentes y además tienen la responsabilidad de reportar incidentes de seguridad.

8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- La Seguridad de la Información, deberá entenderse como un proceso integral constituido por todos los recursos técnicos, humanos, materiales y organizativos relacionados con los servicios prestados por la Universidad.

- Un análisis y gestión de riesgos actualizados son una parte esencial del proceso de seguridad.

- La prevención, detección y recuperación, son medidas que permitirán un enfoque integral de la seguridad de la información, evitando incidencias y reduciendo el impacto de aquellas que finalmente ocurran.

- Los servicios deben estructurarse con diferentes líneas de defensa; constituidas por medidas organizativas, físicas y lógicas, de modo que una amenaza que se materialice no pueda desarrollar todo su potencial y se reduzca el daño ocasionado, en el menor tiempo posible.

- Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

- La segregación de roles para asegurar la calidad y evitar posibles conflictos de intereses, asegurando la consistencia de la seguridad de la información, mediante actuaciones coordinadas entre todos los actores implicados.

- No dejar vacíos de responsabilidades, asegurando que el ciclo de vida de las medidas de seguridad de la información esté cubierto: definición, implantación/operación, revisión y mejora.

- Permitir la toma de decisiones para hacer frente a los retos, problemas e incidencias relacionadas con la seguridad de la información.

8.1. ESTRUCTURA ORGANIZATIVA DE LA SEGURIDAD DE LA INFORMACIÓN

El señor Rector de la Universidad de las Fuerzas Armadas – ESPE, dispone la conformación del Comité de Seguridad de la Información (CSI) y designa a sus miembros. El Comité de Seguridad de la Información, designa al Oficial de Seguridad de la Información (OSI).

El siguiente diagrama representa el esquema de decisión y coordinación de la Seguridad de la Información en la Universidad, mediante el cual se pretende:

- Disponer de una coordinación fluida y consistente en actuaciones de seguridad: Comité de Seguridad de la Información (CSI) y Oficial de Seguridad de la Información (OSI).
- Reportar a los distintos responsables.
- Gestionar los riesgos relacionados con la Seguridad de la Información.
- Elaborar, comunicar y hacer cumplir la reglamentación interna de la Universidad de las Fuerzas Armadas – ESPE en materia de seguridad de la información.

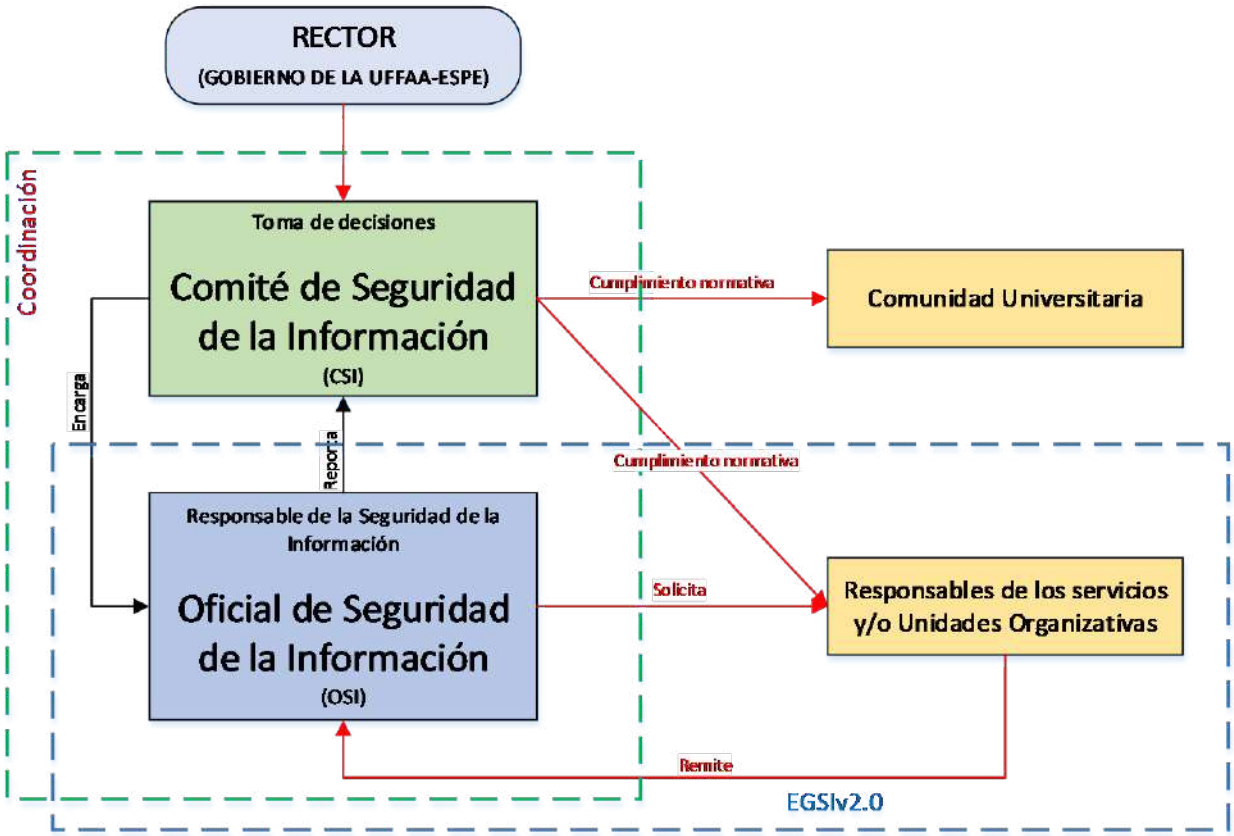

Ilustración 1: Esquema de decisión y coordinación de la Seguridad de la Información

El Presidente del Comité de Seguridad de la Información, deberá coordinar y será el responsable de promover la implementación de la Política de Seguridad de la Información.

El Oficial de Seguridad de la Información asistirá a los miembros de la Comunidad Universitaria en materia de seguridad de la información y coordinará la interacción con instituciones especializadas. Además, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la Universidad y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

Los responsables de los servicios de Tecnologías de la Información y Comunicaciones, Unidades Académicas y Administrativas cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su responsabilidad.

El Vicerrector Administrativo y/o el Coordinador Jurídico, cumplirán la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas, a través del Acuerdo de confidencialidad de la información y buen uso de las Tecnologías de la Información y Comunicaciones - TIC; pertenecientes a la Universidad de las Fuerzas Armadas – ESPE.

9. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

La Universidad de las Fuerzas Armadas – ESPE, es una comunidad de autoridades militares y civiles, personal académico, estudiantes, personal administrativo y trabajadores. Su misión es formar profesionales e investigadores de excelencia, creativos, humanistas, con capacidad de liderazgo, pensamiento crítico y alta conciencia ciudadana; generar y aplicar el conocimiento científico; y transferir tecnología, en el ámbito de sus dominios académicos, para contribuir con el desarrollo nacional y atender las necesidades de la sociedad y de la Fuerzas Armadas; siendo su visión ser reconocida como un referente a nivel nacional y regional por su contribución en el ámbito de sus dominios académicos, al fortalecimiento de la Seguridad y Defensa, bajo un marco de valores éticos, cívicos y de servicio a la comunidad.

La Universidad de las Fuerzas Armadas – ESPE; manifiesta su compromiso con la seguridad de la información que genera, utiliza, procesa, comparte y que la almacena en medios físicos y electrónicos, clasificada como pública, confidencial y reservada; para lo cual en cumplimiento de la normativa vigente implementará los controles de seguridad establecidos en el Esquema Gubernamental de Seguridad de la Información (EGSI) v2.0; a fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

Con la participación conjunta de autoridades militares y civiles, personal académico, estudiantes, personal administrativo y trabajadores; se evaluará la eficacia de los controles implementados para mejorar permanentemente el Sistema de Gestión de Seguridad de la Información.

La Universidad de las Fuerzas Armadas – ESPE, emite formalmente la política específica de Seguridad de la Información, misma que será difundida y estará disponible para los miembros de la Comunidad Universitaria y partes interesadas.

Para la aplicación de la Política Específica de Seguridad de la Información se debe considerar las siguientes directrices:

9.1. USO DE DEQUIPOS INFORMÁTICOS MÓVILES Y FIJOS

a. Los equipos informáticos de propiedad de la Universidad de las Fuerzas Armadas – ESPE, asignados a los usuarios, deberán ser utilizados únicamente para lo fines relacionados con sus actividades laborales.

b. Las autoridades militares y civiles, personal académico, estudiantes, personal administrativo y trabajadores de la Universidad de las Fuerzas Armadas - ESPE no podrán realizar ningún tipo de cambio, alteración, modificación o actualización de los componentes de software y/o hardware instalados en el quipo entregado o que se encuentre a disposición en laboratorios, biblioteca, entre otros.

c. La Unidad de Tecnologías de la Información y Comunicaciones deberá implementar un controlador de dominio en el que se registren los equipos informáticos, propiedad de la Universidad de las Fuerzas Armadas – ESPE.

d. Los equipos informáticos móviles que contengan información importante, sensible o crítica; no deben ser desatendidos y en lo posible deberán ser guardados bajo llaves o se deberán utilizar mecanismos especiales para asegurarlos.

e. La Unidad de Tecnologías de la Información y Comunicaciones, a través de la Mesa de Servicios de Tecnología, previo análisis de funcionalidad y uso, realizará la instalación de software, sea éste licenciado o de uso libre, en los equipos informáticos móviles y fijos de propiedad de la Universidad de las Fuerzas Armadas – ESPE.

f. Las autoridades militares y civiles, personal académico, personal administrativo y trabajadores que hacen uso de los equipos informáticos móviles pertenecientes a la Universidad, deben evitar establecer conexiones hacia los sistemas de información de la Institución a través de redes disponibles en sitios públicos; en caso de ser necesario, se deberá tener la precaución de que la información no se encuentre al alcance de personas no autorizadas y utilizar mecanismos técnicos de seguridad implementados por la Unidad de Tecnologías de la Información y Comunicaciones; por ejemplo, una Red Virtual Privada (VPN).

g. La Universidad de las Fuerzas Armadas – ESPE, a través de la Unidad de Tecnologías de la Información y Comunicaciones mantendrá, a disposición de los miembros de la Comunidad Universitaria que hacen uso de dispositivos móviles, una solución de seguridad que permita registrar y controlar el acceso a los sistemas de información de la Universidad.

h. A fin de garantizar el principio de confidencialidad, la Unidad de Tecnologías de la Información y Comunicaciones controlará el acceso a los sistemas de información; a través de la implementación de técnicas y algoritmos criptográficos; independientes de la autenticación del sistema operativo de los dispositivos informáticos.

i. La Unidad de Tecnologías de la Información y Comunicaciones deberá instalar y poner en operación en los dispositivos informáticos una de solución de antivirus; el cual permita reconocer e impedir que estos generen sus efectos. Adicionalmente; de manera frecuente monitoreará la operación de la solución de antivirus para asegurarse que los usuarios no los hayan desactivado o, mejor aún, los usuarios deben estar impedidos de hacerlo.

j. Las autoridades militares y civiles, personal académico, personal administrativo y trabajadores de la Universidad, que hacen uso de los equipos informáticos; deben estar seguros del origen de los programas ejecutables y de los archivos a abrir; inclusive los correos electrónicos de origen conocido deben ser considerados sospechosos, en virtud de que los virus pueden controlar la lista de correos de un usuario y enviar mensajes utilizando cualquier nombre. En caso de que los usuarios de los equipos informáticos, no se encuentren seguros sobre el origen de un programa ejecutable o de un correo electrónico, deben contactarse y solicitar la asistencia técnica de la Mesa de Servicio de Tecnología; para verificar la procedencia de los mismos.

k. La Unidad de Tecnologías de la Información y Comunicaciones, deberá desinstalar todos los programas utilitarios innecesarios que se encuentren en los equipos informáticos que hayan sido asignados por la Universidad.

l. Cuando una autoridad militar o civil, personal académico, personal administrativo y trabajador se desvincule de la Universidad, la Unidad de Tecnologías de la Información y Comunicaciones, deberá realizar el "*borrado seguro*" del equipo informático. Mediante este borrado, el almacenamiento del equipo queda completamente vacío; impidiendo que la información pueda ser recuperada en un futuro.

m. En cumplimiento a lo dispuesto en la presente política, los miembros de la Comunidad Universitaria podrán hacer uso de equipos informáticos de uso personal o privado; para acceder a los sistemas de información y servicios de red institucionales.

n. La Unidad de Tecnologías de la Información y Comunicaciones, a través de la Mesa de Servicios de Tecnología, brindará asistencia técnica únicamente a usuarios a los cuales se les haya asignado un equipo informático institucional, no deberá atender requerimientos para solventar problemas en equipos informáticos personales o privados.

9.2. SEGURIDAD DE LA INFORMACIÓN PARA EL PERSONAL QUE SE ENCUENTRA BAJO LA MODALIDAD DE TELETRABAJO EMERGENTE

El teletrabajo emergente, es una modalidad laboral de carácter no presencial, a fin de que las autoridades militares y civiles, personal académico, personal administrativo y trabajadores, puedan desempeñar las actividades de docencia y administrativas, utilizando mecanismos que faciliten la ejecución de las mismas, desde un lugar distinto al habitual, siempre y cuando la naturaleza del puesto lo permita.

a. Las autoridades militares y civiles, personal académico, personal administrativo y trabajadores de la Universidad de las Fuerzas Armadas – ESPE, que se acojan a la modalidad de teletrabajo emergente son responsable de mantener y preservar la Confidencialidad, Integridad y Disponibilidad de la información que le haya sido entregada o generada en cumplimiento de sus funciones.

b. Las autoridades militares y civiles, personal académico, personal administrativo y trabajadores de la Universidad de las Fuerzas Armadas – ESPE, deberán custodiar y velar por el buen uso de los equipos y/o sistemas de información que la institución les haya provisto para le ejecución de las actividades de teletrabajo emergente, cumpliendo con la normativa vigente y los procedimientos institucionales establecidos.

c. Dar cumplimiento a las recomendaciones definidas en el *"Protocolo para la creación y buen uso de contraseñas de acceso a los Sistemas de Información o Servicios de TIC´s de la Universidad de las Fuerzas Armadas – ESPE".*

d. Responsabilidades del jefe inmediato

- Controlar y monitorear las actividades que deben ser ejecutadas por los funcionarios que se han acogido a la modalidad de Teletrabajo emergente y el cumplimiento de las medidas de seguridad orientadas a mantener y preservar la Confidencialidad, Integridad y Disponibilidad de la información.

- Brindar las herramientas, información y facilidades necesarias para el cumplimiento de las actividades durante la jornada de teletrabajo emergente.

e. El Oficial de Seguridad de la Información y la Unidad de Tecnologías de la Información y Comunicaciones definirán mecanismos seguros que permitan establecer y/o monitorear las conexiones durante las jornadas de Teletrabajo emergente (accesos a VPN, correo electrónico, certificado de seguridad), de acuerdo con su nivel de acceso.

f. A través de las Unidades Académicas y Administrativas, se mantendrá el control y supervisión respecto de la salida y retorno de los equipos informáticos fijos y móviles, provistos por la Universidad, durante el periodo que dure el Teletrabajo Emergente. Se dará cumplimiento a lo establecido en el "*Procedimiento de salida de los activos fuera de la institución*"

9.2.1. MEDIDAS PARA LA SEGURIDAD DE LA INFORMACIÓN DURANTE LA MODALIDAD DE TELETRABAJO EMERGENTE

a. Se deberá realizar el cifrado completo de los discos duros y verificar la instalación, habilitación y actualización de los programas de antivirus, malware y firewall de los equipos informáticos pertenecientes a la Universidad, que tengan que salir o ya hayan salido de las instalaciones de la institución por motivos de Teletrabajo Emergente, a fin de garantizar; que en caso el dispositivo llegue a manos equivocadas, no se pueda acceder a información de la Universidad.

b. Mantener actualizado el Sistema Operativo de los equipos informáticos que las autoridades militares y civiles, personal académico, personal administrativo y trabajadores, utilice para el teletrabajo emergente.

c. Se recomienda cifrar la conexión wifi del domicilio, con la finalidad de evitar que cualquier persona pueda interceptar la información que se reciba o envíe a través de este medio. De nada servirá que el computador se encuentre protegido si un intruso puede conectarse a la red inalámbrica que se utilice para el teletrabajo emergente.

d. Usar únicamente los servicios institucionales (Sistema Integrado de Gestión Académica y Administrativa de la Universidad de las Fuerzas Armadas – ESPE, "miespe", Sistema de Gestión Documental "QUIPUX", correo electrónico institucional, entre otros) para el intercambio de documentos y demás información, referente al trabajo.

e. Las autoridades militares y civiles, personal académico, personal administrativo y trabajadores deberán cerrar la sesión o bloquear el equipo informático cuando el funcionario no vaya a ser uso del equipo informático; esto permitirá limitar la oportunidad de acceso no autorizado a la información institucional.

f. No perder de vista el dispositivo; incluso cuando tenga la necesidad de movilizarse, tampoco dejar el computador a la vista pública, sin supervisión

9.3. CONTROL DE ACCESO A LOS SISTEMA DE INFORMACIÓN Y EQUIPOS INFORMÁTICOS

a. La necesidad de conocer la información para ejecutar las actividades académicas y administrativas; y la necesidad de usar la información para su procesamiento; deberá ser controlada mediante la limitación del acceso a la información y a las instalaciones donde se procesa la información de la Universidad de las Fuerzas Armadas – ESPE.

b. Los accesos lógicos para usuarios finales a los sistemas de información de la Universidad los realiza la Unidad de Talento Humano, considerando los roles y perfiles.

c. Los directores de las Unidades Académicas y Administrativas en coordinación con la Unidad de Talento Humano son los responsables de otorgar, mantener o revocar el acceso lógicos del personal académico, personal administrativo y trabajadores del departamento/unidad a su cargo conforme a los perfiles y roles asignados, para ello deben aplicar el principio del menor privilegio, el cual establece que se debe únicamente otorgar los permisos y accesos necesarios para que los usuarios puedan cumplir sus funciones.

d. El acceso de los usuarios a la red y a los servicios de red; es específicamente el que se lo haya autorizado.

e. El "*Procedimiento para la habilitación y deshabilitación de los Recursos por Ingresos/Cambios/Salida de personal*" vigente, debe contemplar actualizaciones semestrales de la información de los funcionarios; propias del proceso.

f. El permiso de acceso para usuario "*Administrador*" sobre los equipos informáticos móviles y fijos, será solicitado debidamente motivado y justificado al jefe inmediato de la Unidad Académica o Administrativa; quien a su vez presenta el requerimiento a la Unidad de Tecnologías de la Información y Comunicación; la

cual, previo al otorgamiento del permiso deberá verificar la necesidad a través de la Mesa de Servicios de Tecnología.

g. Toda contraseña correspondiente a cuentas de usuario final es personal e intransferible, por lo cual, la misma no debe compartirse por ningún motivo, aún si fuese requerida por el Jefe Inmediato, por la Mesa de Servicios de Tecnología, o terceros. Adicionalmente, se debe dar cumplimiento a las recomendaciones definidas en el *"Protocolo para la creación y buen uso de contraseñas de acceso a los Sistemas de Información o Servicios de TIC´s de la Universidad de las Fuerzas Armadas – ESPE"*.

h. Las credenciales de acceso para la administración y operación de la infraestructura tecnológica de la Universidad deberán ser actualizadas cada ciento ochenta (180) días calendario.

i. Las cuentas específicas que se utilizan para subir e iniciar servicios informáticos para aplicaciones o de red, bases de datos, réplicas de información con entidades externas, interfaces, sistemas operativos, e infraestructura tecnológica, deben ser configuradas de tal manera que no permitan el inicio de sesión de manera automática sin intervención humana.

j. Se debe deshabilitar o renombrar las cuentas por defecto que contienen los sistemas de información.

k. El Oficial de Seguridad en coordinación con la Unidad requirente y la Unidad de Tecnologías de la Información y Comunicaciones deberán designar un responsable que reciba las credenciales de acceso, en caso de existir intercambio de información con instituciones externas; con la finalidad de implementar los mecanismos técnicos necesarios para llevar a cabo los acuerdos de intercambio.

l. La Unidad de Tecnologías de la Información y Comunicaciones, tiene la responsabilidad de implementar el registro de pistas de auditoría respecto a la autorización y proceso de accesos lógicos y de servicios tecnológicos.

m. El uso de las cuentas con niveles de privilegios altos o cuentas de estructuras de bases de datos, no se utilizarán para las tareas de administración o monitoreo diarias; únicamente deben ser utilizadas en la ejecución de liberaciones, casos excepcionales o emergentes y con un mecanismo de control de uso de éstas.

n. Se deberá establecer para los usuarios con privilegios "altos", lo siguiente:

- Toda cuenta que disponga de altos privilegios debe tener asignado un custodio responsable de aplicar la presente política.

- El inventario de las cuentas con altos niveles de privilegios y sus respectivos custodios deberán ser reportados trimestralmente a la Unidad de Talento Humano y al Oficial de Seguridad de la Información de la Universidad.

9.4. ACCESO A REDES Y SERVICIOS DE RED

a) El acceso a las redes y a los servicios de red de la Universidad de las Fuerzas Armadas – ESPE, es de uso exclusivo para el cumplimiento de las funciones para las que ha sido contratado un usuario o para el desarrollo de las actividades académicas de los estudiantes o personal externo a la institución. Los miembros de la Comunidad Universitaria o externos; asumen la responsabilidad del correcto uso de estos servicios, cuyo funcionamiento se encuentra sujeto a monitoreo y control.

b) La Universidad de las Fuerzas Armadas – ESPE se reserva el derecho de habilitar, deshabilitar, ampliar o restringir el acceso a las redes y servicios de redes institucionales, a autoridades militares y civiles, personal

académico, estudiantes, personal administrativo y trabajadores y personal externo autorizado, como medidas para asegurar el uso aceptable de los mismos y la seguridad de la información institucional.

c) Todos los equipos informáticos móviles y fijos asignados por la Universidad de las Fuerzas Armadas – ESPE a autoridades militares y civiles, personal académico, personal administrativo y trabajadores, deberán tener instalado y activado el antivirus institucional, a fin de protegerlo contra amenazas de código malicioso.

d) Para la autorización de acceso a las redes de la Universidad a dispositivos de personal externo autorizado y de estudiantes, estos deben contar con las actualizaciones del sistema operativo instalado y con un software antivirus actualizado y activado.

e) Los repositorios centrales de almacenamiento de información digital de la Universidad deben ser utilizados exclusivamente para guardar información relacionada con las funciones que cumplen las autoridades militares y civiles, personal académico, personal administrativo y trabajadores de la institución. La Unidad de Tecnologías de la Información y Comunicaciones será la responsable de la administración técnica de la operación y mantenimiento del sistema de almacenamiento central de la Universidad.

f) Es responsabilidad de los Directores de las Unidades Académicas y Administrativas, conocer, evaluar y autorizar el acceso a los servicios de red que requieran de aprobación, respecto del talento humano bajo su cargo, considerando el principio de menor privilegio. Se debe otorgar permisos y autorizaciones únicamente cuando son necesarios para el desempeño de actividades asignadas.

g) Se debe determinar condiciones y restricciones de seguridad para conexiones remotas hacia la red y servicios de red de la Universidad; cuando se realicen actividades de teletrabajo emergente, de conformidad con la normativa establecida por el Ministerio de Trabajo.

9.5. USO DE LA INFORMACIÓN CONFIDENCIAL PARA LA AUTENTICACIÓN

a) Todos los miembros de la Comunidad Universitaria y terceros deben mantener la confidencialidad de la información de autenticación, asegurando su no divulgación.

b) Las credenciales de usuario para autoridades militares y civiles, personal académico, estudiantes, personal administrativo, y trabajadores deben ser creadas por los sistemas de información y de admisión o por otro método automatizado.

c) Se debe evitar guardar (en papel, agendas personales, fichero software o en un dispositivo portátil) las credenciales de acceso, a no ser que estas puedan ser almacenadas de forma segura y que el método de almacenamiento haya sido aprobado, como por ejemplo repositorios seguros para contraseñas recomendados por la Unidad de Tecnologías de la Información y Comunicaciones.

d) Para los miembros de la Comunidad Universitaria, el nombre de la cuenta estará conformada por la inicial del primer nombre, la inicial del segundo nombre, primer apellido completo y en caso de repetición se deberá agregar al final un secuencial.

e) La creación de las credenciales de los estudiantes se las realizará una vez que éste sea admitido en la Universidad.

f) Las credenciales de usuario de los miembros de la Comunidad Universitaria que se hayan desvinculado de la institución, serán deshabilitadas.

g) Las credenciales de usuarios de autoridades militares y civiles, personal académico, personal administrativo y trabajadores se deshabilitarán únicamente por notificación expresa de la Unidad de Talento Humano; una vez se haya efectuado la desvinculación oficial del personal.

h) La Unidad de Tecnologías de la Información y Comunicaciones deshabilitará inmediatamente la cuenta de un usuario, sin el consentimiento, en caso de detectar alguna incidencia de seguridad o por su mal uso como medida preventiva, sin embargo; se le notificará al usuario por los canales internos de comunicación establecidos.

i) En caso de que un usuario se haya desvinculado de la Universidad y requiera por algún motivo acceder a su cuenta en un período determinado de tiempo; lo deberá solicitar formalmente al Vicerrectorado según corresponda.

j) Se debe cambiar las contraseñas de autenticación a los sistemas de información, siempre que haya indicios de su posible divulgación.

k) Para la creación de contraseñas, los miembros de la Comunidad Universitaria, deben dar cumplimiento al *"Protocolo para la creación y buen uso de contraseñas de acceso a los sistemas de información o servicios de TIC´s de la Universidad de las Fuerzas Armadas – ESPE"*.

l) Se debe asegurar una protección adecuada de las contraseñas que son utilizadas como información clasificada de autenticación y almacenadas en procesos automáticos de inicio de sesión.

m) Se debe evitar usar las mismas contraseñas de autenticación para propósitos laborales y privados.

n) La pantalla del computador (escritorio) no deberá contener ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias para que los usuarios ejerzan sus funciones.

9.6. USO DE CONTROLES CRIPTOGRÁFICOS

a) La Unidad de Tecnologías de la Información y Comunicaciones definirá las aplicaciones y/o servicios de TI que permitan la administración de los accesos controlados a través de mecanismos criptográficos de autenticación (por ejemplo, uso de usuarios y contraseñas) y autorización (por ejemplo, el uso de roles y perfiles para asignar los diferentes niveles de acceso).

b) La Unidad de Tecnologías de la Información y Comunicaciones, debe establecer los procedimientos y algoritmos criptográficos (cifrado) que serán utilizados en los sistemas de información institucionales, dependiendo del tipo de control a aplicar, el propósito y los requerimientos específicos del Responsable del proceso y/o servicio institucional.

c) Las contraseñas de acceso a los aplicativos y bases de datos, deben ser protegidos con controles criptográficos. Las contraseñas serán codificadas, cifradas previo a su almacenamiento en la base de datos y/o archivos de parámetros, cuando lo soporten.

d) Para conexiones remotas, se debe utilizar controles criptográficos para Matriz, Sedes, Extensiones, Unidades Académicas Externas y Unidades Académicas Especiales. En caso de existir excepciones deberán ser autorizadas por el responsable del proceso y del servicio; e, informar al Oficial de Seguridad de la Información.

e) Se deben utilizar certificados electrónicos de entidades de certificación de información reconocidas por el Estado Ecuatoriano para la firma de cualquier tipo de documento, mensaje de datos, transacción que se

procese electrónicamente o para comunicaciones entre sistemas, aplicaciones y medios físicos cuando aplique.

9.7. ADMINISTRACIÓN DE CLAVES CIFRADAS

a) La Unidad de Tecnologías de la Información y Comunicaciones definirá los algoritmos criptográficos a ser utilizados de acuerdo con cada sistema de información; y, proporcionará una protección adecuada de la infraestructura tecnológica utilizada para gestionar las claves, considerándola crítica o de alto riesgo.

b) La Unidad de Tecnologías de la Información y Comunicaciones, gestionará las claves para incorporar la funcionalidad de cambio o actualizaciones de las mismas, tomando en consideración las recomendaciones o mejores prácticas para su administración (cuando cambiarlas, como hacerlo, la forma en que los usuarios autorizados tendrán acceso, y como eliminarlas).

c) Bajo pedido del usuario que pierde una clave se generará una nueva, la entrega será a través del procedimiento definido por la Unidad de Tecnologías de la Información y Comunicaciones.

d) Las claves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas durante este lapso de tiempo. Se debe permitir la destrucción de claves que se dejen de utilizar.

e) Además de la administración segura de las claves secretas y privadas, se deberá tener en cuenta la protección de las claves públicas.

f) Los procesos de administración de los certificados de clave pública deberán ser absolutamente confiables, para lo cual se lo debe llevar a cabo mediante una entidad denominada Autoridad de Certificación o Certificador, la Unidad de Tecnologías de la Información y Comunicaciones, gestionará la implementación del certificado para el uso de los sistemas de información definidos.

g) Se deberá habilitar en el Sistema de Información, la generación de claves en la creación de usuarios. Se generará la primera clave la cual deberá obligatoriamente cambiar el propio usuario la primera vez que se ingresa al sistema.

9.8. SEGURIDAD DE LOS ACTIVOS FUERA DE LAS INSTALACIONES

a) Se deberá dejar en constancia que el custodio que recibe los bienes, se encargará de velar por: el buen uso, la conservación, la administración y utilización, así también certifica y garantiza que los bienes están siendo usados para fines Institucionales, sus condiciones son adecuadas y no se encuentran en riesgo de deterioro, de acuerdo con lo que estipulan los Arts. 7, 20, 44 y 47 del Reglamento General Sustitutivo para la Administración, Utilización, Manejo y Control de los Bienes e inventarios del Sector Público y con las Normas de Control Interno 406-07 y 406-08.

b) Autoridades militares y civiles, personal académico, personal administrativo y trabajadores deberán tener en cuentas las siguientes directrices:

- Los activos, propiedad de la Universidad de las Fuerzas Armadas – ESPE que son utilizados fuera de las instalaciones de la institución, deberán ser permanentemente vigilados; poniendo principal atención en lugares púbicos donde puedan ser extraídos o robados.

- El personal académico, personal administrativo o trabajadores deben formalizar al Director de la Unidad Académica o Administrativa, la salida de los activos propiedad de la Universidad fuera de las instalaciones, de acuerdo al *"Formulario para autorización de salida de bienes de propiedad de la Universidad y bienes de control administrativo de la Institución"*, establecido por la Unidad de Logística.

- Los activos, propiedad de la Universidad de las Fuerzas Armadas – ESPE, deberán ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física

- En caso de pérdida o robo de un activo, propiedad de la Universidad de las Fuerzas Armadas – ESPE, se deberá proceder de acuerdo a lo que señala la normativa vigente.

9.9. PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA

a) Los puestos de trabajo de autoridades militares y civiles, personal académico, personal administrativo y trabajadores deben permanecer limpios y ordenados.

b) La pantalla del equipo informático (escritorio) no deberá contener ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias para que los usuarios ejerzan sus funciones laborales.

c) Los gabinetes, cajones y archivadores que contengan documentos y/o medios extraíbles con información confidencial y/o reservada deberán permanecer asegurados durante la hora del almuerzo y al finalizar la jornada laboral.

d) Guardar bajo llave, cuando corresponda, los documentos impresos o físicos y medios extraíbles en gabinetes u otro mobiliario; cuando estos no estén siendo utilizados y/o especialmente fuera de la jornada laboral.

e) Almacenar bajo llave la información que se considere confidencial y/o reservada de la Universidad de las Fuerzas Armadas – ESPE, cuando no está en uso, especialmente cuando no se encuentre personal en las oficinas.

f) Apagar o desconectar de la red, del sistema o de los servicios de red, los dispositivos de uso personal o privado, terminales e impresoras asignadas; cuando estos se encuentren desatendidos. Los mismos deberán ser protegidos con candados de seguridad, contraseñas y/u otros controles cuando no estén en uso.

g) En medida de lo posible, los directores de las Unidades Académicas y Administrativas, designarán un responsable en la Unidad o Departamento bajo su cargo, a fin que mantenga un registro de las contraseñas o copias de las llaves de seguridad de la oficina. Tales elementos deberán ser protegidos en sobre cerrado y bajo llave para impedir accesos no autorizados; pudiendo ser utilizados únicamente ante una posible contingencia.

h) Se prohíbe pegar papeles adhesivos que contengan contraseñas, claves o información que permita el acceso no autorizado a los sistemas de información de la Universidad o externos.

i) La Unidad de Tecnologías de la Información y Comunicaciones, a través de directivas de domino u otro método, habilitará el protector de pantalla con contraseñas, cuando los dispositivos móviles o fijos se encuentren inactivos por un tiempo de diez (10) minutos.

j) Toda vez que el usuario se ausente de su lugar de trabajo, deberá bloquear el dispositivo móvil o fijo, a fin de proteger el acceso a las aplicaciones y servicios institucionales.

k) Para hacer uso de las impresoras, cada usuario dispondrá de una contraseña. Las impresoras deberán ser bloqueadas automáticamente cuando se encuentre desatendidas y fuera del horario normal de trabajo.

l) Se prohíbe dejar documentación en la bandeja de salida de las impresoras, se deberá retirar inmediatamente la documentación, una vez que ésta haya sido impresa.

m) Una vez terminada la jornada laboral, los usuarios deberán obligatoriamente guardar bajo llaves cualquier tipo de información y asegurarse que los equipos informáticos se encuentren totalmente apagados.

9.10. EQUIPO DE USUARIO DESATENDIDO

a) Autoridades militares y civiles, personal académico, personal administrativo y trabajadores deberán garantizar que los equipos informáticos no sean desatendidos y, por el contrario, sean permanentemente protegidos.

b) Los equipos informáticos asignados a autoridades militares y civiles, personal académico, personal administrativo y trabajadores; deberán tener una protección específica contra accesos no autorizados, cuando se encuentren desatendidos.

c) El Oficial de Seguridad de la Información de la Universidad deberá comunicar y socializar a toda la Comunidad Universitaria y externos, acerca de los requerimientos y procedimiento de seguridad, para la protección de equipos que se encuentren desatendidos, así como también la responsabilidad de cumplir dichos requerimientos.

d) Autoridades militares y civiles, personal académico, personal administrativo y trabajadores, para asegurar que los equipos desatendidos se encuentren seguros, deberán bloquear adecuadamente la pantalla del equipo informático cuando el usuario requiera abandonar la estación de trabajo. La Unidad de Tecnologías de la Información y Comunicaciones habilitará un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla que se active a los diez (10) minutos de no evidenciar actividad y que permita la sesión reiniciar la sesión mediante la contraseña de usuario.

9.11. USO DE SOFTWARE NO AUTORIZADO

a) Todo software instalado y utilizado sobre los equipos informáticos propiedad de la Universidad de las Fuerzas Armadas - ESPE, deberá cumplir con los principios constitucionales, los acuerdos internacionales y la legislación nacional vigente sobre derechos de autor, y en todo caso está sujeto al respeto de los derechos o voluntad expresada según el modo y vigencia sobre derechos de autor en documentos físicos o digitales de licenciamiento.

b) La adopción y uso de software en la Universidad de las Fuerzas Armadas – ESPE, podrá ser mediante: Proyectos de Investigación, adquisición de bienes, contratación de servicio de uso de licencias de software académico y/o comercial, ejecución de contratos, donaciones, cualquier proceso que conlleve la utilización de programas nuevos en los equipos informáticos de la institución.

c) El software licenciado y adquirido por la Universidad de las Fuerzas Armadas - ESPE, como cualquier otro activo de información de TIC, deberá estar asociado a un responsable dentro del inventario de la Unidad de Tecnologías de la Información y Comunicaciones.

d) Todo programa o proyecto de software solicitado para adopción y uso en los equipos móviles o fijos de propiedad de la Universidad, bien sea para ser desarrollado u obtenido por cualquiera de los modos de licenciamiento aceptados, estará sujeto a aprobación y autorización de uso.

e) La Unidad de Tecnologías de Información y Comunicaciones realizará la identificación y definición del software el mismo que podrá ser usado en los procesos de Investigación, Vinculación con la Sociedad, Académicos y Administrativos.

f) Todo software propuesto para desarrollar con recursos de la Universidad de las Fuerzas Armadas – ESPE deberá pasar por un proceso de estudio de factibilidad técnica y económica. En caso de que el software sea desarrollado internamente se deberá aplicar la *"Metodología de Desarrollo de Software"*, vigente.

g) Se debe fomentar en la Universidad de las Fuerzas Armadas – ESPE, el uso de *"Software Libre"*; de acuerdo con lo establecido en el *"Código Orgánico de Economía Social de los Conocimientos, Creatividad e Innovación*, *Apartado Segundo de las Tecnologías libres y formatos abiertos"*, del Ministerio de Telecomunicaciones y Sociedad de la Información en los artículos 142, 145, 151.

h) La Unidad de Tecnologías de la Información y Comunicaciones deberá mantener un inventario centralizado del software que puede ser instalado y utilizado en la Universidad de las Fuerzas Armadas – ESPE, identificado como *"Software Base"*. Adicionalmente, dispondrá de un repositorio centralizado que garantice el conocimiento, disponibilidad y gestión eficiente de los activos de software.

i) La Unidad de Tecnologías de la Información y Comunicaciones, deberá implementar controles para:

- Que los sistemas operativos y sistemas de procesamiento de información se mantengan actualizados con las últimas versiones de seguridad disponibles a fin de mitigar los riesgos de contagio de malware en los equipos informáticos móviles y fijos de la Universidad.

- Detectar el uso de software no autorizado.

- Evitar la navegación en sitios maliciosos o considerados como *"Listas Negras"*.

- Evitar que obtenga o descargue archivos y software desde o a través de redes externas o por cualquier otro medio.

- Instalar y actualizar periódicamente software de antivirus y contra código malicioso.

- Verificar antes del uso de un software, la presencia de virus en archivos de medios electrónicos o en archivos recibidos a través de redes no confiables, correos electrónicos y/o archivos descargados.

- Realizar el filtrado de: virus, spam, programas maliciosos (malware), en el perímetro externo, de ser necesario para la Universidad.

j) La Unidad de Tecnologías de la Información y Comunicaciones desarrollará, implementará y socializará planes de continuidad de TIC´s, para la recuperación ante ataques informáticos. Adicionalmente, se deberá aislar ambientes donde puedan producirse impactos catastróficos en activos de información de Tecnologías de la Información y Comunicaciones críticos.

k) Se deberá socializar a los miembros de la Comunidad Universitaria, información puntual sobre posibles ataques informáticos y sus posibles afectaciones a los sistemas de información y equipos informáticos; con el fin de concienciar a los miembros de la Comunidad Universitaria acerca del problema de los virus y cómo proceder frente a los mismos.

9.12. RESPALDOS Y COPIAS DE SEGURIDAD DE LA INFORMACIÓN

La Universidad de las Fuerzas Armadas – ESPE, con el propósito de mantener y preservar la confidencialidad, integridad y disponibilidad de la información establece que se deberá realizar copias de seguridad de la información, del software y de los sistemas de información; mismas que deberán ser verificadas periódicamente.

a) El director de la Unidad de Tecnologías de la Información y Comunicaciones, junto con el administrador del módulo de un sistema/aplicativo o infraestructura de Tecnologías de la Información y Comunicaciones, será

quienes determinen los procedimientos formales para el respaldo, resguardo y contención de la información que se genera en los sistemas/aplicativos de Tecnologías de la Información y Comunicaciones.

b) El procedimiento deberá definir el etiquetado de las copias de respaldo, de acuerdo a la normativa interna de la Universidad vigente y en el que se identifique su contenido, periodicidad y retención.

c) Se deberá establecer los procedimientos para la verificación y restauración de la información contenida en los medios de respaldos para garantizar que estos sean confiables para uso de emergencia.

d) Se deberá definir la extensión (incremental/completo) y la frecuencia de generación de los respaldos, de acuerdo a los requisitos de la Universidad.

e) Se deberá definir un sitio alterno seguro y lejano, el cual se encuentre a una distancia considerable para evitar cualquier daño ocasionado por desastres en la Universidad de las Fuerzas Armadas – ESPE, Campus Sangolquí.

f) El sitio alterno seguro, servirá para almacenar los respaldos de la información generados en la Universidad de las Fuerzas Armadas – ESPE.

g) Una vez concluida la vida útil de los respaldos de la información, se deberá proceder con la destrucción segura de los medios.

h) Se debe garantizar que el sitio alterno seguro, donde se va a almacenar los respaldos de la información, cuente con las seguridades físicas y ambientales adecuadas.

i) Se deberá comprobar periódicamente la integridad de los medios de respaldos de la información; para asegurar el funcionamiento correcto del procedimiento de recuperación de la información.

j) Se debe garantizar que los respaldos de la información sean protegidos mediante técnicas de cifrado.

k) Las autoridades militares y civiles, personal académico, personal administrativo y trabajadores serán responsable de la información almacenada en los equipos informáticos móviles y fijos asignados, en cumplimiento a lo establecido en el Art. 28 "*DE LOS RESPALDOS DE INFORMACIÓN*" del *"REGLAMENTO INTERNO PARA LA ASIGNACIÓN, USO Y CONTROL DE LA INFRAESTRUCTURA Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE",* vigente.

9.13. MONITOREO CONTÍNUO, GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS

a) La Unidad de Tecnologías de la Información y Comunicaciones, deberá definir y establecer las responsabilidades sobre un Servidor Público, para que realice la gestión, supervisión, evaluación de riesgos de las vulnerabilidades técnicas, el seguimiento de los activos de información de TIC.

b) Previa la puesta en producción de los sistemas de información o de los aplicativos, se deberá realizar un análisis de las amenazas y de las vulnerabilidades técnicas para determinar la severidad del impacto; sobre la base de lo cual se establecerá los controles que permitan mitigar el riesgo, el responsable del activo de información de TIC deberá gestionar la remediación y aceptará o no la puesta en producción.

c) El análisis de vulnerabilidades técnicas para los sistemas de información y equipos informáticos de la Universidad de las Fuerzas Armadas – ESPE, tendrá una periodicidad anual en base al alcance que determine el Oficial de Seguridad de la Información, y, cada vez que se produzcan cambios significativos.

d) El alcance que defina el Oficial de Seguridad de la Información, será en base al inventario y valoración por de pérdida de la confidencialidad, integridad y disponibilidad de los activos de información declarados por la Unidad de Tecnologías de la Información y Comunicaciones. El alcance será el 10% del total de activos de información de TIC, de los cuales el 6% corresponderá a los activos de información de TIC catalogados con criticidad alta y el 4% con criticidad media.

e) El Oficial de Seguridad de la Información, deberá coordinar la ejecución de un Ethical Hacking; con personal interno o externo a la Universidad.

f) La Unidad de Tecnologías de la Información y Comunicaciones; en base a los resultados obtenidos en una evaluación de seguridad de TIC, establecerá los controles de seguridad de TIC y dará seguimiento a su implementación para reducir el nivel de riesgo asociado.

g) La Unidad de Tecnologías de la Información y Comunicaciones, deberá mantener actualizado el inventario de los activos de información de TIC, considerando cambios o nuevos recursos, con el propósito de asociar los riesgos que se deriven.

h) La Unidad de Tecnologías de la Información y Comunicaciones será responsable de evaluar los riesgos asociados con la instalación de un parche para cubrir vulnerabilidades; además, se deberá probar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables, las pruebas se las debe realizar en ambientes controlados, similares a los de producción, manteniendo un registro de todos los procedimientos adoptados.

i) En caso de que no exista ningún parche disponible, deberían considerarse otros controles como:

- Desactivar servicios o capacidades relacionadas con la vulnerabilidad.
- Adaptar o incluir controles de acceso.
- Incrementar la supervisión para detectar o evitar ataques reales.
- Aumentar la concienciación en el personal interno de la Unidad de Tecnologías de la Información y Comunicaciones y usuarios sobre las vulnerabilidades técnicas identificadas.

j) La gestión de las vulnerabilidades técnicas debe ser supervisada y evaluada semestralmente para garantizar su eficacia y eficiencia.

k) Para que la gestión de vulnerabilidades técnicas sea eficaz, ésta debe estar alineada con las actividades de gestión de incidentes, para comunicar información sobre las vulnerabilidades relativas a la función de respuestas a incidentes y proporcionar procedimientos técnicos a desarrollar cuando ocurra un incidente.

9.14. INSTALACIÓN DE SOFTWARE POR PARTE DE LOS USUARIOS

a) Toda instalación de software nuevo, de cualquier tipo de licenciamiento o implementación deberá previamente ser informado y coordinado con la Unidad de Tecnologías de la Información a través de la Mesa de Servicios y el personal operativo a cargo (Jefe de laboratorio, laboratorista, técnico u administrador del contrato o proyecto) para su instalación. Los usuarios de la Universidad de las Fuerzas Armadas - ESPE, no podrán realizar ningún tipo de cambio, alteración, modificación o actualización de los componentes de software.

b) La Unidad de Tecnologías de la Información y Comunicaciones, deberá identificar qué tipos de instalaciones de software están permitidas (por ejemplo, software base, actualizaciones y parches de seguridad para el

software existente) y que tipos de instalaciones están prohibidas (por ejemplo, software que es solo de uso personal y software cuya procedencia se desconoce o se sospecha).

c) Para la instalación del software adicional, el usuario o la unidad requirente solicitará al jefe inmediato la autorización de instalación, el mismo que remitirá el pedido a la Unidad de Tecnologías de información y Comunicaciones, para su análisis y validación de los términos y condiciones del software (propietario o libre).

d) La Unidad de Tecnologías de la Información y Comunicaciones, Jefe de laboratorio y/o laboratorista serán responsables de mantener el equipo informático libre de instalación de software no autorizado, a través del mantenimiento preventivo y procedimientos de preparación y reparación.

9.15. INTERCAMBIO DE INFORMACIÓN

a) La Unidad de Tecnologías de la Información y Comunicaciones, deberá establecer los controles cuando se utilizan los servicios de TIC.

b) La Unidad de Tecnologías de la Información y Comunicaciones definirá:
   - Definirá directrices para el uso de las redes inalámbricas disponibles en cada uno de los Campus Universitarios, en base a los riesgos identificados.
   - Definirá controles para la detección y protección de las comunicaciones electrónicas contra posibles malware que pueden ser transmitidos.
   - Establecerá controles criptográficos.
   - Establecerá los controles y lineamientos que se encuentren asociados con el uso de los recursos de comunicación.

c) Autoridades militares y civiles, personal académico, personal administrativo y trabajadores deberán evitar dejar información sensible en copiadoras e impresoras, en virtud de que esta puede ser reproducida por personas no autorizadas.

9.16. MENSAJERÍA ELECTRÓNICA

a) Se deberá cifrar los contenidos y/o informaciones clasificadas que puedan enviarse por mensajería electrónica; utilizando firmas electrónicas reconocidas por el Estado Ecuatoriano y otras tecnologías evaluadas y aprobadas por la Universidad de las Fuerzas Armadas – ESPE.

b) El servicio de correo electrónico institucional se asigna a todo miembro de la Comunidad Universitaria que tiene creado un usuario en el Sistema Integrado de Gestión Académica y Administrativa institucional. El servicio de correo electrónico se determinará de acuerdo a los requerimientos de la Universidad para ser gestionado por la Unidad de Tecnologías de la Información y Comunicaciones.

c) La Unidad de Tecnologías de la Información y Comunicaciones, a través de la Mesa de Servicios de Tecnología, instalará en las computadoras de escritorio o portátiles asignadas a las autoridades militares y civiles, personal académico, personal administrativo y trabajadores de la Universidad un software cliente para el acceso al correo electrónico institucional. La configuración deberá realizarse a través del protocolo IMAP.

d) La cuenta de correo electrónico institucional asignada a un servidor o al personal externo autorizado, es personal e intransferible, por lo que se prohíbe su acceso y/o uso a otras personas.

e) Todas las cuentas de correo creadas bajo el dominio "@espe.edu.ec", serán consideradas como provenientes de la Universidad de las Fuerzas Armadas - ESPE, su contenido es confidencial y propio de los usuarios, siendo los únicos y exclusivos responsables del contenido enviado en el mensaje y de la información adjunta que se remita desde su cuenta.

f) El envío masivo de mensajes de correo electrónico, se encuentra autorizado únicamente a la cuenta institucional bajo la administración de la Unidad de Comunicación Social.

g) Se prohíbe la difusión de correos masivos desde el dominio de correo electrónico institucional "@espe.edu.ec".

h) Los miembros de la Comunidad Universitaria, deberán depurar permanentemente los correos electrónicos, específicamente aquellos que provengan de cuentas electrónicas de remitentes de procedencia desconocida, a fin de evitar problemas de saturación y conectividad, infección o propagación de código malicioso.

i) El uso del correo electrónico institucional "@espe.edu.ec" es para uso exclusivo de actividades inherentes al cumplimiento de las funciones académicas o administrativas.

j) Todo mensaje de correo electrónico que sea enviado a través del servicio correo electrónico institucional deberá incluir una cláusula de confidencialidad, cuyo contenido deberá ser elaborado y entregado por el Oficial de Seguridad de la Información de la Universidad, la cual deberá ser agregada al final del correo saliente de forma automática.

k) Todas las cuentas de correo electrónico dispondrán de una cuota de almacenamiento y un tamaño máximo para el envío de documentos adjuntos de acuerdo a los requerimientos institucionales y al análisis técnico de la Unidad de Tecnologías de la Información y Comunicaciones. En caso de que se requiera compartir archivos de mayor tamaño estos deben ser cargados temporalmente en la Google Drive, sistema de almacenamiento en la nube autorizado por la Universidad de las Fuerzas Armadas – ESPE.

9.17. USO ACEPTABLE DEL SERVICIO DE INTERNET INSTITUCIONAL

a) La Unidad de Tecnologías de la Información y Comunicaciones en coordinación con el Oficial de Seguridad de la Información definirán las categorías, grupos y listas de navegación del servicio de internet institucional.

b) Se deberá bloquear el acceso a portales, aplicaciones o servicios de la internet y la web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses y valores de la institución.

c) Se deberá dar cumplimiento al "*CAPÍTULO IV DEL USO DEL SERVICIO DE INTERNET"* del "*REGLAMENTO INTERNO PARA LA ASIGNACIÓN, USO Y CONTROL DE LA INFRAESTRUCTURA Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS –ESPE*", que trata sobre "*USO Y CONTROL DE EQUIPOS INFORMÁTICOS A NIVEL DE USUARIO*".

9.18. DESARROLLO SEGURO DE APLICACIONES Y SISTEMAS

a) La Unidad de Tecnologías de la Información y Comunicaciones, deberá garantizar que los principios de confidencialidad, integridad y disponibilidad; sea una parte integral de los aplicativos informáticos desarrollados durante todo el ciclo de vida del desarrollo.

b) Los desarrollos de nuevos requerimientos se alinearán a los controles de seguridad establecidos en el Sistema de Gestión Académica y Administrativa de la Universidad de las Fuerzas Armadas ESPE.

c) La Unidad de Tecnologías de la Información y Comunicaciones, a través del proceso de Desarrollo de Aplicaciones, deberá establecer las directrices para el desarrollo de aplicativos y sistemas de información.

d) La Unidad de Tecnologías de la Información y Comunicaciones, deberá definir y actualizar el estándar tecnológico de desarrollo de aplicaciones, cuando sea necesario.

e) El Oficial de Seguridad de la Información y un responsable designado por la Unidad de Tecnologías de la Información y Comunicaciones, realizará la validación y verificación del cumplimiento de estándares de seguridad de aplicativos informáticos, para lo cual se llevará a cabo las pruebas funcionales de seguridad, de acuerdo a lo establecido en el *"Lista de verificación de pruebas de seguridad del sistema"*, vigente.

f) Para los pasos a producción de los aplicativos informáticos, se deberá verificar el cumplimiento de *"Listas de verificación de pruebas de aceptación de sistemas"*, vigente; y, los datos de prueba se deben seleccionar, proteger y controlar. Los cambios a los aplicativos dentro del ciclo de vida de desarrollo se deben controlar mediante la normativa de control de cambios aprobada.

g) Para las pistas de auditoría de las transacciones definidas, los responsables funcionales de los aplicativos podrían considerar la identificación del usuario que realiza el cambio, y/o fecha de modificación cuando se originaron las transacciones o acciones (para los aplicativos y servicios de TIC´s que sea factible), si se requiere se entregará reportes que les permitan realizar revisiones de auditoría.

h) La Unidad de Tecnologías de la Información y Comunicaciones deberá establecer controles para la liberación y despliegue de los aplicativos (producción) de la Universidad de las Fuerzas Armadas - ESPE.

i) Para dar atención a incidentes, los Servidores Públicos del proceso de Desarrollo de Aplicaciones, deberán tener autorización de acceso al ambiente de producción únicamente a consultas, para evitar que se realicen cambios en el mismo.

j) La Unidad de Tecnologías de la Información y Comunicaciones, restringirá el acceso al código fuente de los aplicativos informáticos institucionales a personas no autorizadas.

k) Las solicitudes de extracción directa de información de las bases de datos, se las debe canalizar formalmente desde el responsable funcional del aplicativo al Director de la Unidad de Tecnologías de la Información y Comunicaciones, quien autorizará solamente en aquellos casos que no se encuentren disponibles reportes o procesos automatizados, aquellos requerimientos recurrentes deberán ser automatizados. Estas extracciones deberán cumplir las siguientes condiciones:

   - Estar asociadas a un caso, transacción u operación de un proceso, producto o servicio institucional.

   - Ser solicitadas formalmente y de manera justificada; la cual deberá registrarse en una bitácora (Registrar la copia y la utilización de la información para futuras auditorías) para futuras referencias.

l) Las solicitudes para realizar copias de información, desde las bases de datos de ambientes de producción a ambientes de desarrollo y pruebas, deberán cumplir con las siguientes condiciones:

   - Realizar actividades de desarrollo y mantenimiento de sistemas de información institucionales para agregar o modificar funcionalidades y reproducir errores en los servicios tecnológicos

   - Ejecutar pruebas y/o migraciones de sistemas de información y/o de herramientas tecnológicas, previo a su implementación en ambientes productivos.

m) Sobre la información en ambientes previos al paso a producción, deberá aplicarse los mismos procedimientos de control de acceso que existen en los ambientes de producción.

9.19. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

a) Las Unidades de la Universidad de las Fuerzas Armadas ESPE, deberán identificar, documentar los tipos de proveedores, a los cuales la institución permitirá acceder a su información.

b) La Unidad de Tecnologías de la Información y Comunicaciones deberá establecer y acordar todos los requisitos de seguridad de la información de TIC pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de TIC para los Sistemas de Información de la Universidad, mismos que deberán ser documentados.

c) La Unidad de Tecnologías de la Información y Comunicaciones deberá dar seguimiento y revisar con regularidad la prestación de servicios de TIC con los proveedores/contratistas.

d) Se debe gestionar los cambios en el suministro de servicios por parte de los proveedores/contratistas, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de la Universidad de las Fuerzas Armadas ESPE involucrados, y la revaloración de los riesgos.

9.20. PROTECCIÓN Y PRIVACIDAD DE LA INFORMACIÓN

a) La Universidad de las Fuerzas Armadas – ESPE no compartirá información sobre datos personales de los miembros de la Comunidad Universitaria a terceros.

b) Únicamente se deberá utilizar la información de los miembros de la Comunidad Universitaria disponible en los portales o sistemas web para mejorar el contenido, usabilidad y su experiencia.

c) La Universidad de las Fuerzas Armadas – ESPE podrá actualizar su Política de Privacidad cuando sea necesario. Si se realiza cambios sustanciales, se procederá a notificar mediante un aviso en el respectivo portal o sistema web.

d) Los portales web de la Universidad de las Fuerzas Armadas – ESPE utilizarán “cookies” para mejorar la navegación, calidad y experiencia del usuario.

e) La Universidad de las Fuerzas Armadas – ESPE utilizará el protocolo HTTPS para brindar seguridad en el uso de los canales electrónicos y manejar los riesgos, acorde lo que se indica en la normativa vigente.

f) El uso de los portales de la Universidad de las Fuerzas Armadas – ESPE o de cualquiera de sus componentes, implicará la aceptación expresa de los presentes Término y condiciones de uso.

g) La Universidad de las Fuerzas Armadas – ESPE dispondrá de los portales y sistemas web para prestar información a los miembros de la Comunidad Universitaria y público en general sobre la Gestión Académica y Administrativa.

h) La Universidad de las Fuerzas Armadas – ESPE únicamente será responsable del tratamiento y uso de los datos personales que recabe en forma directa a través de los portales y sistemas web. No asumirá responsabilidades que pueda generar el usuario por el uso inadecuado o contrario a los fines de los canales electrónicos.

i) Serán obligaciones del usuario:

- No destruir, inhabilitar, modificar o perjudicar los canales electrónicos a los que tiene acceso, ni tampoco los contenidos incorporados y almacenados en éstos.

- No utilizar versiones de sistemas modificados con el fin de obtener accesos no autorizados a cualquier canal electrónico, contenido y/o servicios ofrecidos a través de estos.

- No interferir ni interrumpir el acceso, funcionalidad y utilización de canales electrónicos y redes conectados al mismo.

- Acceder únicamente a la información otorgada conforme a su rol o perfil.

10. VIGENCIA, AUTORIZACIÓN Y CONTROL DE CAMBIOS

10.1. VIGENCIA

La presente Política de Seguridad de la Información, tiene vigencia a partir de su emisión y se responsabiliza de su estricto cumplimiento en su ámbito de competencia al Comité de Seguridad de la Información y al Oficial de Seguridad de la Información.

Para garantizar la vigencia de la Política de Seguridad de la Información, en la Universidad de las Fuerzas Armadas – ESPE, esta deberá ser revisada anualmente o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológico, económico, entre otros; los cuales deberán ser documentados y versionados.

10.2. AUTORIZACIÓN

ELABORADO POR:	REVISADO POR:	Aprobado por:
Unidad de Seguridad Integrada	**Unidad de Seguridad Integrada**	**Vicerrectorado Académico General**
_____ Ing. Mauricio Javier Baldeón Garzón, Mgs. **Especialista de Seguridad Integrada / Oficial de Seguridad de la Información**	_____ Tcrn. (SP) David Alfredo Molina Vizcaíno **Director**	_____ Víctor Emilio Villavicencio Álvarez, PhD. **Vicerrector / Presidente del Comité de Seguridad de la Información**

10.3. CONTROL DE CAMBIOS

Versión	Fecha	Detalle de la modificación
1.0	25-08-2021	Elaboración del Hito Homologado: Políticas de Seguridad de la Información