UNIDAD DE TECNOLOGÍA

REGLAMENTO DE ASEGURAMIENTO DE LA INFORMACIÓN (basado en la norma ISO 27001)

OBJETIVO

El presente Reglamento tiene como objetivo establecer políticas, principios y requerimientos de Aseguramiento de la Información, que garanticen la disponibilidad, confidencialidad e integridad de la información que se procesa, intercambia, reproduce y conserva mediante el uso de las tecnologías de información en la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

1 CONTENIDO

2 ÍNDICE DE TABLAS

3 INTRODUCCIÓN

Actualmente la información juega un papel preponderante para promover el desarrollo, incrementar el nivel de competitividad y alcanzar el éxito de una institución, siendo esta, un elemento clave para el cumplimiento de los objetivos estratégicos. La Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López no es la excepción, genera y recibe información en su quehacer cotidiano a través de sus cuerpos académicos, investigaciones, estrategias, procesos, productos y servicios, además de la información relativa a su personal y alumnos.

En este contexto, es de relevancia mencionar que la información forma parte importante de los activos de información de la institución, al igual que las personas, los procesos, el software, hardware, medios de soporte de información, espacios físicos, red de telecomunicaciones, entre otros; los cuales deben protegerse por el valor que tienen para la Universidad, y son necesarios para mantener en operación los procesos institucionales.

La seguridad de la información incluye la protección de información, sistemas, recursos y demás activos contra desastres, errores (intencionales o no) y manipulación no autorizada, para reducir la probabilidad y el impacto de los incidentes de seguridad.

La política de seguridad de la información es un conjunto de lineamientos basados en unas normas y procedimientos que determinan las reglas y procedimientos a seguir para garantizar la seguridad de la información, de acuerdo con el tipo de negocio y los requisitos legales, contractuales, regulatorios y normativos aplicables a todo el alcance de la organización. Ella establecerá las directrices, límites, responsabilidades y objetivos de los controles que se deben implementar e implantar para garantizar los requisitos de protección de seguridad de la información en la organización.

4 OBJETIVO

El objetivo del Reglamento de Aseguramiento de la Información es el de establecer las medidas de seguridad de carácter general, así como de índole técnica y organizativa, dirigidas a asegurar el cumplimiento de las garantías de autenticidad, integridad, confidencialidad, disponibilidad, conservación de la información y trazabilidad.

5 ALCANCE

El presente Reglamento, será de estricta aplicabilidad y cumplimiento por parte de todos los funcionarios, docentes, estudiantes y terceros que presten sus servicios o tengan algún tipo de relación con la Institución; lo cual debe involucrar a todos los procesos y actividades desarrolladas por la Entidad.

6 NOTACIONES

- ADS: Área de Desarrollo de Software

- ESPAM MFL: Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.
- RAI: Reglamento de Aseguramiento de la Información
- UT: Unidad de Tecnología

7 TERMINOLOGÍA Y DEFINICIONES

- Autenticación: es la capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser.
- Backup: se hace para prevenir una posible pérdida de información.
- Cifrado: es el proceso de convertir texto legible, denominado texto plano, en un formato ilegible, denominado texto cifrado.
- Código Fuente: es un archivo o conjunto de archivos, que contienen instrucciones concretas, escritas en un lenguaje de programación, que posteriormente compilan uno o varios programas.
- Código Malicioso: es cualquier software corrupto, dañino, nocivo o no autorizado diseñado para infiltrarse y dañar un sistema informático.
- Comunidad politécnica: estudiantes, personal docente, empleados, trabajadores y todos quienes utilicen los activos de información institucionales.
- Credenciales: conjunto de datos que incluye la identificación y prueba de identificación que se utiliza para obtener acceso a recursos locales y de red.
- Criptografía: es el desarrollo de un conjunto de técnicas que permiten alterar y modificar mensajes o archivos con el objetivo de que no puedan ser leídos por todos aquellos usuarios que no estén autorizados a hacerlo.
- Criticidad: busca ubicar en diferentes zonas el riesgo que un activo le pudiera generar a la organización donde forma parte.
- Data Center (o centro de datos): es una instalación que proporciona acceso compartido a aplicaciones y datos mediante una infraestructura compleja de red, computación y almacenamiento.
- Firewall: mecanismo de seguridad que impide el acceso a una red.
- Firma Electrónica: es un archivo digital el cual contiene campos que permiten vincular y determinar la identidad de una persona determinada.
- Fraude Informático: se refiere al fraude realizado a través del uso de una computadora o del Internet.
- Hacker: se refiere a la persona o a una comunidad que posee conocimientos en el área de informática y se dedica a acceder a sistemas informáticos para realizar modificaciones en el mismo.
- Hardware: se refiere a todos los componentes físicos internos de un ordenador, es decir, la parte tangible del equipo.
- Incidente de Seguridad: corresponde a cualquier evento adverso relacionado con la seguridad, por ejemplo, robo de información, fuga y la obtención de un acceso no autorizado a la información.

- Ingeniería Social: técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.
- Firmware: se refiere al software integrado dentro del hardware, habitualmente en una memoria ROM, que lleva el sello o la firma del fabricante y que le especifica cómo ha de funcionar y cuál es su configuración.
- Phishing: es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito.
- Piratería: copia ilegal de software y se comercializa sin ningún tipo de licencia.
- Proxy: Servidor que realiza la conexión a Internet y que sirve de puerta de entrada a los ordenadores cliente.
- Radiación Electromagnética: se compone tanto de campos eléctricos como magnéticos. Surge de fuentes naturales o producidas por el hombre. (calor radiado, luz visible, rayos X o rayos gamma.).
- Ransonware: es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.
- Script: son fragmentos de código que tienen como objetivo realizar o añadir funciones dentro de una página web.
- Segregar: separar, dividir o apartar algo del resto de los objetos o personas.
- Servidor: equipo que controla el acceso de los usuarios a una red y les da servicio e información.
- Software: es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo.
- Soporte: es el proceso que se lleva a cabo para obtener asistencia y emplear diferentes herramientas y soluciones para los problemas informáticos.
- Spyware: software malicioso que infecta su ordenador o dispositivo móvil y recopila información sobre usted, su navegación y su uso habitual de Internet.
- Storage: consiste en la conservación de información empleando una tecnología específicamente desarrollada para mantener los datos y que se encuentren accesibles siempre que sean necesarios.
- Telecomunicación: es la trasmisión a distancia de datos de información a través de medios electrónicos y/o tecnológicos.
- Teletrabajo: se refiere a la actividad laboral que se desarrolla fuera de las instalaciones de la empresa, apelando a las tecnologías de la información y de la comunicación para el desarrollo de los quehaceres.
- Topología de red: hace referencia a la forma en la que está dispuesta una red, incluyendo sus nodos o puntos de intersección, conexión o enlace de varios elementos y las líneas utilizadas para asegurar la transmisión y recepción de datos de manera correcta y segura.

8 REFERENCIAS

- Constitución de la República del Ecuador
- Norma INEN ISO/IEC 27001
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley del Sistema Nacional de Registro de Datos Públicos
- Ley Orgánica y Normas de Control de la Contraloría General del Estado
- Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva
- Decreto Ejecutivo No. 1384 sobre Interoperabilidad Gubernamental en la Administración Pública.
- Google Workspace for Educations - Centro de privacidad y seguridad
- Manual del Aseguramiento de la Información (Unidad de Tecnología)

9 RESPONSABLES

- Es responsabilidad de la ESPAM MFL apoyar el proceso de implementación del Reglamento de Aseguramiento de la Información y asignar los recursos necesarios para su cumplimiento.
- La ESPAM MFL deberá aprobar la obligatoriedad del uso del presente Reglamento de Aseguramiento de la Información.
- Es responsabilidad de la UT elaborar y actualizar políticas de seguridad de la información a la comunidad politécnica.
- Es responsabilidad de la UT la implementación y administración de los controles técnicos aplicables a la Políticas de Seguridad de la Información.
- Es responsabilidad de la UT asegurar y verificar periódicamente la correcta aplicación y cumplimiento de estas políticas.
- Es responsabilidad de la UT realizar la comunicación y socialización de estas políticas a todos los usuarios.
- Es responsabilidad de los usuarios cumplir con las normas y procedimientos establecidos en esta política.

10 ESTRUCTURA

La norma ISO 27001 es una solución de mejora continua con base en estándares para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros. Sistema enfocado en el ciclo de mejora continua o de Deming (Planificar – Hacer – Verificar – Actuar), conocido también como ciclo PDCA.

Plan: Planificación; Do: Implementación y operación; Check: Monitorización y evaluación; - Act: Mantenimiento y mejora.

El presente reglamento llevará la siguiente estructura:

- Introducción
- Objetivo
- Alcance
- Términos y definiciones
- Estructura
- Análisis, Evaluación y Tratamiento de Riesgos
- Controles - NORMA ISO/IEC 27002:2013
- Políticas de Seguridad
- Aspectos Organizativos de la Seguridad de la información
- Seguridad ligada a los Recursos Humanos
- Gestión de Activos
- Control de Acceso
- Cifrado
- Seguridad Física y Ambiental
- Seguridad en la Operatividad
- Seguridad en las Telecomunicaciones
- Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información
- Relación con proveedores
- Gestión de Incidentes en la Seguridad de la Organización
- Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio
- Cumplimiento
- Registros
- Control de Cambios

11 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es fundamental para la supervivencia de las organizaciones en la era de la información. Varios problemas están involucrados, dado que la sociedad depende de la información almacenada en los sistemas informáticos para la toma de decisiones en las empresas, entre otros contextos organizacionales.

La información puede existir en varios formatos: impresa, almacenada electrónicamente, hablada, transmitida por correo convencional de voz o electrónico, etc. Cualquiera que sea el formato o medio de transmisión o almacenamiento, se recomienda proteger la información de manera adecuada, para garantizar la continuidad del negocio, minimizar el riesgo y maximizar el retorno sobre la inversión. Problemas comunes:

- Destrucción de la información y otros recursos.
- Modificación o distorsión de información.
- Robo, eliminación o pérdida de información u otros recursos.
- La revelación de información.

- La interrupción de los servicios.

11.1 MODELOS DE ATAQUE

- Interrupción: Cuando un activo se destruye o queda indisponible (o inutilizable), caracterizando un ataque contra la disponibilidad.
- Interceptación: Cuando se accede a un activo por un tercero no autorizado (persona o programa), caracterizando un ataque contra la confidencialidad.
- Modificación: Cuando se accede a un activo por un tercero no autorizado (persona o programa) y se modifica, materializando un ataque contra la integridad.
- Fabricación: Cuando una parte no autorizada (persona o programa) inserta objetos falsificados en un activo, configurando un ataque contra la autenticidad.

12 ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS

En la actualidad, las empresas se enfrentan a muchos riesgos e inseguridades procedentes de focos diversos y la ESPAM MFL no está alejada de este escenario. Esto quiere decir que los activos de información de las empresas, uno de sus valores más importantes, se encuentran ligados o asociados a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades.

12.1 RIESGO

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

12.2 IDENTIFICACIÓN DE RIESGOS

La identificación del riesgo permite conocer los incidentes que puedan causar las alteraciones en el funcionamiento de la entidad, y pueden comprometer y afectar la confidencialidad, integridad y disponibilidad de la información.

El propósito principal de identificar el riesgo es determinar que puede suceder en el caso de tener una pérdida potencial de información y que acciones tomar al comprender el cómo, dónde y por qué puede ocurrir el evento.

12.3 ANÁLISIS DE RIESGOS

El análisis de riesgos identifica y estima los riesgos, teniendo en cuenta el uso sistemático de la información. Abarca el análisis de las amenazas, vulnerabilidades e impactos y se considera el punto clave de la política de seguridad de la información de una organización. Un correcto proceso de identificación de riesgos implica:

- Identificar todos aquellos activos de información que tienen algún valor para la organización.
- Asociar las amenazas relevantes con los activos identificados.
- Determinar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.
- Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

12.3.1 ACTIVOS

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), redes y comunicaciones, recursos administrativos, recursos físicos y recursos humanos

12.3.2 TIPOS DE ACTIVOS

- Servicios: Servicios o procesos que ofrece la organización con carácter interno o externo.
- Datos o información: Datos (en cualquier formato) que se manejan en la organización.
- Aplicaciones: Aplicaciones de Software.
- Hardware: Equipos para gestionar la información.
- Redes de comunicaciones: Redes que dan soporte a la organización (propias o subcontratadas).
- Personal: Todos aquellos que tengan acceso de una manera u otra a los activos (interno o externo).
- Equipamiento auxiliar: Son activos que no se han incluido en ninguno de los otros grupos (equipos de destrucción de documentación o de climatización).
- Soporte de información: Soportes físicos que permiten el almacenamiento de la información durante un largo periodo de tiempo.
- Instalaciones: Lugares en los que se alojan los sistemas de información.

12.3.3 AMENAZAS

Se define como cualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas.

- Usuarios: Es la principal amenaza, ya sea porque estos no adoptan buenas prácticas de ciberseguridad y se convierten en blancos fáciles, son ellos quienes roban información de forma intencional o su formación no es acorde a su puesto de trabajo.
    - Instalación de hardware y software no autorizado
    - Usuarios internos que practican actos ilegales
    - Desastres causados por personas

- Uso de contraseñas débiles
- Piratería
- Uso no autorizado del equipo
- Error en el uso o abuso de derechos
- Error por desconocimiento u omisión
- Falsificación
- Acceso a información confidencial impresa
- Ausencia o falta copias de seguridad
- Falta de gestión en recursos de red
- Consumo excesivo del ancho de banda
- Fraude Informático
- Fraudes basados en el uso de computadores
- Ingeniería Social
- Phishing

- Programas maliciosos: consisten en software maliciosos que se encargan de destruir archivos, espiar o robar información usar los recursos tecnológicos de forma no autorizada.
  - Códigos maliciosos
  - Virus informático
  - Ransonware
  - Activadores no oficiales
  - Crackeo de software
  - Spyware

- Fallos de programación: aunque se deban a errores en el desarrollo, representa un gran peligro porque fácilmente podrían infiltrarse softwares maliciosos, acceder a información no autorizada y robar información, por esta razón se deben mantener actualizados los sistemas operativos en todos los equipos.
  - Fallas en el diseño del software
  - Saturación del sistema de información
  - Incumplimiento en el mantenimiento del sistema de información
  - Errores en los sistemas operativos
  - Información comprometida
  - Monitoreo del tráfico de la red
  - Ataques de inyección SQL
  - Aplicaciones desactualizadas
  - Accesos no autorizados
  - Monitoreo de cambios

- Intrusos: se trata de personas no autorizadas que se introducen en los programas y archivos para espiar, robar o destruir información.
  - Invasión
  - Espionaje remoto

- Corrupción de datos
- Acceso a los archivos de contraseña
- Modificación de la información
- Ataques contra el sistema
- Chantaje
- Robo o suplantación de identidad
- Acceso a la red

- Siniestros: en este caso se produce pérdida de información o recursos a consecuencia de la negligencia por falta de oficio o mal intención de los usuarios.
  - Desastres por amenazas físicas (fuego, agua o pérdida suministro eléctrico)
  - Pérdida o fallas de suministros básicos (eléctrico, agua, aire acondicionado y equipos de comunicaciones)

- Catástrofes naturales: estas se dan por causas naturales.
  - Desastres Naturales (Fenómenos climáticos, sísmicos)
  - Penetración en el sistema (física)

- Fallos de equipo o electrónicos: estos pueden afectar los sistemas debido a fallas en la energía eléctrica o por desperfectos propios de los equipos.
  - Fallas del equipo
  - Daños físicos en los equipos
  - Equipo inadecuado para las operaciones

- Robo o hurto: cuando el encargado de custodiar la información sufre la pérdida de esta, por robo o hurto. Puede ser en la institución o fuera de ella.
  - Hurto de documentos
  - Hurto de equipos de cómputo
  - Asalto a un empleado
  - Robo de información

12.4 IDENTIFICACIÓN DE LAS VULNERABILIDADES

Las vulnerabilidades son las debilidades que se encuentran en un activo y se pueden explotar por una o más amenazas, lo que lo convierte en un riesgo de seguridad. Se deben identificar vulnerabilidades (debilidades) de acuerdo con los siguientes tipos:

- Hardware
  - Mantenimiento insuficiente
  - Ausencia de esquemas de reemplazo periódico
  - Sensibilidad a la radiación electromagnética
  - Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
  - Almacenamiento sin protección
  - Falta de cuidado en la disposición final
  - Copia no controlada

- Pérdida de funcionalidad del equipo
- Depreciación de la vida útil de equipos
- Ubicación y adecuación en la operación de los equipos

- Software
  - Ausencia o insuficiencia de pruebas de software
  - Ausencia de terminación de sesión
  - Ausencia de registros de auditoría
  - Asignación errada de los derechos de acceso
  - Interfaz de usuario compleja
  - Ausencia de documentación
  - Ausencia de mecanismos de identificación y autenticación de usuarios
  - Contraseñas sin encriptación
  - Software nuevo o inmaduro
  - Software ilegal

- Red
  - Ausencia de pruebas de envío o recepción de mensajes
  - Líneas de comunicación sin protección
  - Conexión deficiente de cableado
  - Tráfico sensible sin protección
  - Punto único de falla
  - Falta de seguridad firmware
  - Falta de herramientas de monitoreo
  - Topología de red inadecuada

- Personal
  - Ausencia del personal
  - Entrenamiento insuficiente
  - Concienciación en seguridad de la información
  - Ausencia de políticas de uso aceptable
  - Trabajo no supervisado de personal externo o de limpieza
  - Configuración inadecuada de equipos
  - Segregación de actividades
  - Formación no es acorde a su puesto de trabajo

- Lugar
  - Uso inadecuado de los controles de acceso al edificio
  - Áreas susceptibles a inundación
  - Conexiones eléctricas inadecuadas y ausencia de backup para problemas de energía
  - Red eléctrica inestable
  - Ausencia de protección en puertas o ventanas
  - Ausencia de procedimiento de registro/retiro de usuarios

- Ausencia de proceso para supervisión de derechos de acceso
- Ausencia de control de los activos que se encuentran dentro y fuera de las instalaciones
- Ausencia de mecanismos de monitoreo de video vigilancia
- Climatización inadecuada

12.5 EVALUACIÓN DE RIESGOS

La evaluación del riesgo se hace de manera cualitativa y cuantitativa, generando una comparación, donde se obtiene como resultado el análisis de la probabilidad de ocurrencia del riesgo versus el impacto de este.

12.6 IMPACTO

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza.

TABLA DE PROBABILIDAD			
NIVEL	TIPO	DESCRIPCIÓN	FRECUENCIA
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos 5 años.
3	Posible	El evento podría ocurrir en algún momento.	Al menos una vez en los últimos 2 años.
4	Probable	El evento probablemente ocurra en la mayoría de las circunstancias.	Al menos una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.

Tabla 1 Evaluación de Riesgos - Probabilidades

TABLA DE IMPACTO		
NIVEL	TIPO	DESCRIPCIÓN
1	Insignificante	Si llegara a presentarse, tendría consecuencias o efecto mínimo sobre la entidad.
2	Menor	Si llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad.
3	Moderado	Si llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad.
4	Mayor	Si llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5	Catastrófico	Si llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Tabla 2 Evaluación de Riesgos - Impactos

Fórmula para calcular la criticidad: CRITICIDAD = PROBABILIDAD * IMPACTO.

PROBABILIDAD	IMPACTO				
	Catastrófico (5)	Mayor (4)	Moderado (3)	Menor (2)	Insignificante (1)
Casi seguro (5)	25	20	15	10	5
Probable (4)	20	16	12	8	4
Posible (3)	15	12	9	6	3
Improbable (2)	10	8	6	4	2
Raro (1)	5	4	3	2	1

Tabla 3 Criticidad de Riesgos - Cuantitativa

Criticidad	EXTREMO	ALTO	MODERADO	BAJO
Rango	25 – 20 – 16 - 15	12 – 10 - 9	8 – 6 - 5	4 – 3 – 2 - 1

Tabla 4 Rangos de criticidad

PROBABILIDAD	IMPACTO				
	Catastrófico (5)	Mayor (4)	Moderado (3)	Menor (2)	Insignificante (1)
Casi seguro (5)	E	E	E	A	M
Probable (4)	E	E	A	M	B
Posible (3)	E	A	A	M	B
Improbable (2)	A	M	M	B	B
Raro (1)	M	B	B	B	B

Tabla 5 Criticidad de Riesgos - Cuantitativa

B: Zona de Riesgo Baja	Asumir el riesgo
M: Zona de Riesgo Moderada	Asumir el riesgo, Reducir el Riesgo
A: Zona de Riesgo Alta	Reducir el riesgo, Compartir o Transferir
E: Zona de Riesgo Extrema	Reducir el riesgo, Evitar, Compartir o Transferir

Tabla 6 Tratamiento de Riesgos

12.7 EL TRATAMIENTO DE LOS RIESGOS

El tratamiento de los riesgos es tomar decisiones frente a los diferentes riesgos existentes de acuerdo con la estrategia de la institución. Se deben seleccionar controles para reducir, aceptar/retener, evitar o transferir los riesgos y se debe definir un plan para el tratamiento del riesgo. Existen cuatro opciones disponibles para el tratamiento del riesgo:

12.7.1 EVITAR EL RIESGO

- Esta opción de tratamiento busca eliminar la probabilidad de ocurrencia o el impacto del riesgo.
- Tomar las medidas necesarias para prevenir la materialización del riesgo.

12.7.2 REDUCIR RIESGOS

- Se implementa cuando el riesgo se puede tratar internamente y puede llevarse a un nivel aceptable.
- Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección).

12.7.3 TRANSFERIR TODO O PARTE DEL RIESGO

- Requiere hacer un traslado a terceros u otras organizaciones parte del impacto negativo de una amenaza, como contratos a riesgo compartido.
- Al transferir el riesgo a un tercero le damos la responsabilidad para su administración, pero no significa que eliminamos el riesgo.

12.7.4 ASUMIR EL RIESGO

- Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el encargado del proceso acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

12.8 SELECCIÓN DE CONTROLES

Los controles son medidas adoptadas para hacer frente a las vulnerabilidades y reducir el riesgo de incidentes de seguridad de la información. El control es cualquier mecanismo útil para gestionar los riesgos, incluyendo las políticas, procedimientos, directrices, o estructuras organizativas que pueden ser de carácter administrativo, técnico, de gestión o legal. A continuación, se detalla matriz de Análisis, Evaluación y Tratamiento de riesgos:

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	Tipo de Activo	Descripción del Activo	Tipo de Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Criticidad	Tipo de Impacto	Medida de Respuesta	Control /es
REDES Y TELECOMUNICACIONES	Hardware, Redes y Telecomunicaciones	Rack, Switch, Router, Transiver	Personal no autorizado con acceso a equipos	Usuarios: ● Usuarios que practican actos ilegales ● Desastres causados por personas ● Uso no autorizado del equipo Fallos de programación: ● Accesos no autorizados Robo o hurto: ● Hurto de equipos de cómputo ● Asalto a un empleado	Personal: ● Trabajo no supervisado de personal externo o de limpieza ● Configuración inadecuada de equipos Lugar: ● Uso inadecuado de los controles de acceso al edificio ● Ausencia de protección en puertas y ventanas ● Ausencia de procedimiento de registro/retiro de usuarios	2	3	6	Servicio de internet interrumpido	Asumir el riesgo y Reducir el riesgo	5.1.1 9.1.1 9.1.2 9.2.1 11.1.2
		Switch, Router y Access Point	Falta de equipos robustos para acceso a redes inalámbricas simultáneos	Usuarios: ● Falta de gestión en recursos de red ● Consumo excesivo del ancho de banda Fallos de equipos o electrónicos: ● Fallas del equipo ● Daños físicos en los equipos ● Equipo inadecuado para las operaciones	Hardware: ● Ausencia de esquemas de reemplazo periódico ● Pérdida de funcionalidad del equipo ● Depreciación de la vida útil del equipo Personal: ● Ausencia de políticas de uso aceptable	3	3	9	Pérdida de funcionalidad del equipo e intermitencia en el servicio de internet	Reducir el riesgo, Compartir o Transferir	6.1.3 13.1.3
	Redes y Telecomunicaciones	Equipos de redes y telecomunicaciones	Daños a equipos por inconvenientes eléctricos	Usuarios: ● Desastres causados por personas Siniestros: ● Pérdida o fallas de suministros básicos Fallos de equipos o electrónicos: ● Daños físicos en los equipos	Hardware: ● Susceptibilidad a las variaciones de temperatura Lugar: ● Conexiones eléctricas inadecuadas y ausencia de backup para problemas de energía ● Red eléctrica inestable	5	3	15	Desconfiguración de equipos de redes y telecomunicaciones	Reducir el riesgo, Evitar, Compartir o Transferir	11.1.4 11.2.2 11.2.4
		Equipos de redes y telecomunicaciones	Fallas en la conectividad por falta de segmentación del ancho de banda para usuario final	Usuarios: ● Consumo excesivo del ancho de banda ● Usuarios internos que practican actos ilegales	Hardware: ● Pérdida de funcionalidad del equipo ● Ausencia de esquemas de reemplazo periódico Red: ● Topología de red inadecuada	4	3	12	Inestabilidad en la conectividad	Reducir el riesgo, Compartir o Transferir	5.1.1 12.4.1 13.1.1 13.1.2 13.1.3

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS												
Área	Tipo de Activo	Descripción del Activo	Tipo de Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Criticidad	Tipo de Impacto	Medida de Respuesta	Control /es
	Instalaciones	Edificio donde reposan los equipos de redes y telecomunicaciones	Fácil acceso y poca seguridad en lugares donde se encuentran equipos de red	Robo o hurto: ● Hurto de equipos de cómputo Usuarios: ● Usuarios internos que practican actos ilegales	Lugar: ● Lugares inadecuados para instalación de equipos ● Ausencia de procedimiento de registro/retiro de usuarios ● Ausencia de mecanismos de monitoreo de video vigilancia	5	5	25	Sustracción, desconexión y daños en los equipos	Reducir el riesgo, Evitar, Compartir o Transferir	11.1.1 11.1.2 11.1.3
		Lugares no aclimatados para equipos de redes telecomunicaciones	Lugares expuestos a temperaturas altas	Siniestros: ● Desastres por amenazas físicas ● Pérdida o fallas de suministros básicos Catástrofes naturales: ● Desastres naturales	Hardware: ● Susceptibilidad a las variaciones de temperatura Lugar: ● Climatización inadecuada ● Red eléctrica inestable	2	2	4	Calentamiento excesivo y/o quema los equipos y sus componentes	Asumir el riesgo	11.1.4
	Datos o Información	Seguridad de datos en la red	Hackeo o acceso de intrusos	Usuarios: ● Usuarios que practican actos ilegales ● Uso de contraseñas débiles Programas maliciosos: ● Códigos maliciosos, ● Spyware Intrusos: ● Acceso a la red, Espionaje remoto ● Ataques contra el sistema	Software: ● Ausencia de mecanismos de identificación y autenticación de usuarios Red: ● Tráfico sensible sin protección ● Ausencia de pruebas de envío o recepción de mensajes ● Falta de seguridad de firmware	3	2	6	Pérdida de información o bloqueo de acceso a equipos	Asumir el riesgo y Reducir el riesgo	9.1.2 9.2.2 9.2.4 9.4.1
	Personal	Administrador de equipos de redes y telecomunicaciones	Fallas en el monitoreo y soporte técnico, poco personal encargado de administrar el acceso	Usuarios: ● Error en el uso o abuso de derechos ● Falta de gestión en recursos de red Fallos de programación: ● Monitoreo del tráfico de la red	Red: ● Falta de herramientas de monitoreo Personal: ● Ausencia del personal ● Segregación de Actividades	3	3	9	Inestabilidad en el servicio, incumplimiento en el soporte técnico	Reducir el riesgo, Compartir o Transferir	6.1.2 9.1.2 13.1.1 13.1.2 13.1.3
	Servicios	Seguridad a la conectividad	Personal no autorizado con acceso a la administración de los equipos de red	Usuarios: ● Uso no autorizado del equipo ● Error por desconocimiento u omisión Intrusos: ● Acceso a la red ● Acceso a los archivos de contraseñas	Red: ● Configuración inadecuada de equipos Software: ● Ausencia de terminación de sesión ● Asignación errada de los derechos de acceso Personal:	1	3	3	Inestabilidad en todo el sistema de red	Asumir el riesgo	9.1.1 9.1.2 9.2.1 9.2.2 9.2.3 9.2.5 9.2.6 9.4.2 10.1.2

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	Tipo de Activo	Descripción del Activo	Tipo de Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Criticidad	Tipo de Impacto	Medida de Respuesta	Control /es
					• Concienciación en seguridad de la información						
		Equipos de redes y telecomunicaciones	Falta de recursos económicos para adquirir equipos	Usuarios: • Falta de gestión en recursos de red • Error por desconocimiento u omisión	Hardware: • Ausencia de esquemas de reemplazo periódico • Pérdida de funcionalidad del equipo • Depreciación de la vida útil de equipos	4	5	20	Falta de conectividad al Internet	Reducir el riesgo, Evitar, Compartir o Transferir	5.1.1 6.1.3
MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS DE CÓMPUTO	Aplicaciones	Antivirus sin licencia o licencia caducada	Equipos de cómputo con poca o nula seguridad	Usuarios: • Instalación de hardware y software no autorizado Programas maliciosos: • Virus informático • Activadores no oficiales • Crackeo de software Intrusos: • Espionaje remoto	Software: • Software ilegal Red: • Falta de herramientas de monitoreo	3	3	9	Puertas traseras abiertas que vulneran el sistema fácilmente y permiten infección de información	Reducir el riesgo, Compartir o Transferir	11.2.4 12.2.1
	Hardware	Equipos de cómputo	Descargas y variaciones eléctricas que producen desperfectos en los equipos	Siniestros: • Pérdida o fallas de suministros básicos	Lugar: • Conexiones eléctricas inadecuadas y backup para problemas de energía • Red eléctrica inestable	5	3	15	Daños en el sistema operativo y en dispositivos o periféricos	Reducir el riesgo, Evitar, Compartir o Transferir	11.1.3 11.1.4
		Equipos de cómputo, dispositivos y periféricos	Daños de equipos y pérdida de información por parte de los usuarios	Usuarios: • Instalación de hardware y software no autorizado • Usuarios internos que practican actos ilegales • Desastres causados por personas • Ingeniería social Siniestros: • Desastres por amenazas físicas Robo o hurto: • Hurto de equipos de cómputo	Hardware: • Mantenimiento insuficiente • Copia no controlada • Personal: • Ausencia del personal • Entrenamiento insuficiente • Concienciación en seguridad de la información • Ausencia de políticas de uso aceptable	5	3	15	Entorpece las actividades y pérdida de información	Reducir el riesgo, Evitar, Compartir o Transferir	7.2.2 8.1.3 9.4.1 11.2.1
		Equipos de cómputo,	Fallas en hardware por falta de	Usuarios: • Instalación de hardware y software no autorizado	Hardware: • Susceptibilidad a las variaciones de temperatura	4	3	12	Daños en los equipos de cómputo,	Reducir el riesgo, Compartir	11.1.3 11.1.5 11.2.4

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	Tipo de Activo	Descripción del Activo	Tipo de Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Criticidad	Tipo de Impacto	Medida de Respuesta	Control /es
		dispositivos y periféricos	mantenimiento preventivo físico	● Desastres causados por personas ● Error por desconocimiento u omisión Siniestros: ● Desastres por amenazas físicas Fallos de equipos o electrónicos: ● Fallas del equipo ● Daños físicos en los equipos ● Equipo inadecuado para las operaciones	● Mantenimiento insuficiente Personal: ● Entrenamiento insuficiente ● Concienciación en seguridad de la información ● Ausencia de políticas de uso aceptable ● Configuración inadecuada de equipos Lugar: ● Climatización inadecuada				dispositivos o periféricos y pérdida de información	o Transferir	
		Impresoras compartidas en red	Compromiso de la información y acciones no autorizadas, por seguridad reducida en configuración de uso compartido de archivos e impresoras	Usuarios: ● Usuarios internos que practican actos ilegales ● Uso de contraseñas débiles ● Uso no autorizado del equipo Programas maliciosos: ● Códigos maliciosos ● Virus informático Fallos de programación: ● Información comprometida ● Accesos no autorizados Intrusos: ● Modificación de la información ● Acceso a la Red	Software: ● Ausencia de terminación de sesión ● Software ilegal Red: ● Falta de herramientas de monitoreo Personal: ● Concienciación en seguridad de la información	1	3	3	Infección con archivos maliciosos y compromiso de la información por acceso de personas no autorizadas	Asumir el riesgo	7.2.2 9.2.4 9.3.1
		Equipos de cómputo e impresoras	Traslado de equipos de un área a otra, sin precauciones de seguridad ante robos, accidentes o siniestros	Usuarios: ● Desastres causados por personas ● Uso de contraseñas débiles Siniestros: ● Desastres por amenazas físicas Robo o hurto: ● Hurto de equipos de cómputo ● Asalto a un empleado ● Robo de información	Personal: ● Falta de conciencia en seguridad de la información	3	4	12	Daños por caídas de los equipos al trasladarlos a otras áreas, pérdida o robo de equipos de cómputo e información	Reducir el riesgo	6.2.1 7.2.2 11.1.4 11.2.1 11.2.5 11.2.6
	Datos o Información	Información institucional	Pérdida de información por mal uso o configuración	Usuarios: ● Usuarios internos que practican actos ilegales	Hardware: ● Almacenamiento sin protección Software:	3	2	6	Acceso a equipos por parte de	Asumir el riesgo y	7.2.2 8.1.3 9.1.1

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	Tipo de Activo	Descripción del Activo	Tipo de Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Criticidad	Tipo de Impacto	Medida de Respuesta	Control /es
			inadecuada de contraseñas de los usuarios	● Uso de contraseñas débiles Programas maliciosos: ● Rasonware Fallos de programación: ● Accesos no autorizados Intrusos: ● Robo o suplantación de identidad Robo o hurto: ● Hurto de equipos de cómputo	● Ausencia de terminación de sesión ● Contraseñas sin encriptación Personal: ● Entrenamiento insuficiente ● Concienciación en seguridad de la información ● Ausencia de políticas de uso aceptable				personas no autorizadas	Reducir el riesgo	9.4.1 9.4.2 9.4.3
	Software	Sistema operativo y aplicaciones	Fallas en software y aplicaciones	Usuarios: ● Instalación de hardware y software no autorizado ● Error por desconocimiento u omisión ● Ausencia o falta de copias de seguridad Programas maliciosos: ● Virus informático ● Activadores no oficiales ● Crackeo de software Fallos de programación: ● Errores en los sistemas operativos ● Aplicaciones desactualizadas Fallos de equipo o electrónicos: ● Fallos del equipo	Hardware: ● Mantenimiento insuficiente Software: ● Software nuevo o inmaduro ● Software ilegal Personal: ● Entrenamiento insuficiente ● Concienciación en seguridad de la información ● Ausencia de políticas de uso aceptable ● Configuración inadecuada de equipos	4	4	16	Daños en el sistema operativo y pérdida de información	Reducir el riesgo, Evitar, Compartir o Transferir	11.2.4
	Servicios, Datos e Información	Datos e Información	Pérdida de información por falta de procedimientos efectivos para recuperación de información	Usuarios: ● Uso no autorizado del equipo ● Error por desconocimiento u omisión ● Ausencia o falta de copias de seguridad Fallos de programación: ● Información comprometida Robo o hurto: ● Hurto de equipos de cómputo	Hardware: ● Almacenamiento sin protección ● Copia no controlada ● Pérdida de funcionalidad del equipo ● Depreciación de la vida útil de equipos Personal: ● Entrenamiento insuficiente ● Formación no es acorde a su puesto de trabajo	2	4	8	Daño de disco duro, pérdida de información y respaldos históricos	Asumir el riesgo y Reducir el riesgo	5.1.1 12.3.1

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	Tipo de Activo	Descripción del Activo	Tipo de Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Criticidad	Tipo de Impacto	Medida de Respuesta	Control /es
	Personal	Software y aplicaciones	Instalación de programas por parte de los usuarios, sin la autorización de la UT	Usuarios: ● Instalación de hardware y software no autorizado ● Usuarios internos que practican actos ilegales Programas maliciosos: ● Activadores no oficiales ● Crackeo de software	Hardware: ● Mantenimiento insuficiente Software: ● Ausencia o insuficiencia de pruebas de software ● Software ilegal Red: ● Falta de herramientas de monitoreo Personal: ● Concienciación en seguridad	4	4	16	Acceso de intrusos e infección con archivos maliciosos	Reducir y Evitar el riesgo	5.1.1 6.1.1 7.2.2 9.4.4 12.6.2
DESARROLLO DE SOFTWARE Y NUEVAS TECNOLOGÍAS	Servicios y Personal	Correo electrónico institucional	Acceso de los usuarios a correos de dudosa procedencia	Intrusos: ● Ataques contra el sistema ● Robo o suplantación de identidad	Personal: ● Falta de conciencia en seguridad de la información	3	4	12	Pérdida de información, infección y/o bloqueo de acceso a equipos	Asumir el riesgo y Reducir el riesgo	6.1.1 10.1.2 12.2.1 13.2.1
	Información y Datos	Base de datos institucional	Acceso no autorizado a las bases de datos	Intrusos: ● Acceso a los archivos de contraseña Usuario: ● Usuarios internos que practican actos ilegales	Personal: ● Ausencia de políticas de uso aceptable Software: ● Ausencia de terminación de sesión ● Ausencia de registros de auditoría	3	4	12	Integridad de los datos comprometida (reportería o certificaciones)	Asumir el riesgo y Reducir el riesgo	5.1.1 6.1.1 7.2.2 9.2.2 9.2.3 9.2.4 9.2.6 9.4.1 9.4.2
	Aplicaciones	Aplicaciones institucionales	Software en producción sin pruebas	Fallos de programación: ● Fallas en el diseño de software Usuario: ● Error en el uso o abuso de derechos	Software: ● Ausencia o insuficiencia de pruebas de software ● Software nuevo o inmaduro Personal: ● Entrenamiento insuficiente ● Falta de concienciación en seguridad	3	1	3	Inconsistencias al entregar el sistema y fallas de este al estar en ejecución	Asumir el riesgo	12.1.4 12.5.1 12.6.2 14.2.1 14.2.2 14.2.6 14.2.8 14.2.9 14.3.1
		Aplicaciones institucionales	Código fuente de aplicaciones no sincronizado	Usuario: ● Desastres causados por personas Fallos de programación:	Personal: ● Configuración inadecuada de equipos	2	2	4	Confusiones en la sincronización	Asumir el riesgo	9.4.4 9.4.5 12.7.1

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	Tipo de Activo	Descripción del Activo	Tipo de Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Criticidad	Tipo de Impacto	Medida de Respuesta	Control /es
				● Incumplimiento en el mantenimiento del sistema de información	● Entrenamiento insuficiente Lugar: ● Ausencia de control de los activos que se encuentran dentro y fuera de las instalaciones				y respaldos del código fuente		14.2.1 14.2.2 14.2.6
		Equipos de cómputo	Aplicaciones para desarrollo de software sin soporte y licencias	Usuarios: ● Error en el uso o abuso de derechos Fallos de programación: ● Aplicaciones desactualizadas	Software: ● Software ilegal	3	2	6	Funcionalidad disminuida de aplicaciones e infecciones por activadores	Asumir el riesgo y Reducir el riesgo	11.2.4 14.2.1 14.2.5
	Soporte de información	Base de datos institucional	Respaldos no automatizados de las bases de datos	Fallos de programación: ● Monitoreo de cambios Siniestros: ● Fallas de suministros básicos Fallos del equipo o electrónico: ● Fallos del equipo	Hardware: ● Almacenamiento sin protección Software: ● Ausencia de documentación Red: ● Punto único de falla Personal: ● Entrenamiento insuficiente	2	2	4	Pérdida de información relevante y pérdida de la continuidad del negocio.	Asumir el riesgo	5.1.1 6.1.1 12.1.1 12.1.2 12.3.1 12.6.1 17.1.1
	Hardware	Equipos de cómputo	Equipos de desarrollo no adecuado	Fallas de equipo o electrónico: ● Fallas de equipo ● Equipo no adecuado para operaciones	Hardware: ● Pérdida de funcionalidad del equipo ● Depreciación de vida útil del equipo	3	4	12	Retardo en la producción de software y soporte de aplicaciones	Reducir y compartir o transferir el riesgo	8 11.2.4 12.6.1 14.1.1
	Servicio	Aplicaciones institucionales	Soporte técnico de aplicaciones sin seguimiento	Usuarios: ● Instalación de hardware y software no autorizado ● Desastres causados por personas ● Error por desconocimiento u omisión ● Ausencia o falta de copias de seguridad Fallos de programación: ● Fallas en el diseño del software ● Incumplimiento en el mantenimiento del sistema de información	Hardware: ● Almacenamiento sin protección ● Copia no controlada Software: ● Ausencia o insuficiencia de pruebas de software ● Ausencia de documentación ● Software nuevo o inmaduro Personal: ● Entrenamiento insuficiente ● Segregación de actividades ● Formación no es acorde a su puesto de trabajo	3	3	9	Inhabilitación de aplicaciones sin soporte, servicios de aplicaciones detenidos	Reducir y compartir o transferir el riesgo	5.1.1 8.1.1 9.2.3 9.4.4 9.4.5 11.2.4 12.1.1 12.4.3 14.1.1 14.2.1 14.2.2 14.2.5 16.1.4 16.1.5

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	Tipo de Activo	Descripción del Activo	Tipo de Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Criticidad	Tipo de Impacto	Medida de Respuesta	Control /es
	Personal	Aplicaciones institucionales	Usuarios sin actualizar credenciales periódicamente	Usuarios: ● Uso de contraseñas débiles ● Error por desconocimiento u omisión	Software: ● Interfaz de usuario compleja Personal: ● Falta de concienciación en seguridad	5	2	10	Alteración de datos en roles específicos y confidencialidad expuesta a otros usuarios	Reducir y compartir o transferir el riesgo	6.1.1 7.2.2 8.1.3 9.1.1 9.2.5 9.4.2 9.4.3
		Equipo de trabajo	Falta de personal de desarrollo	Usuarios: ● Desastres causados por personas ● Error el uso o abuso de derechos ● Error por desconocimiento u omisión	Software: ● Ausencia o insuficiencia de pruebas de software Personal: ● Ausencia de personal ● Formación no es acorde a su puesto de trabajo	4	2	8	Sistemas sin actualizar y vulnerables, rendimiento en aplicaciones muy bajo	Asumir el riesgo y Reducir el riesgo	7.1.2 7.2.1 7.2.3 8
		Aplicaciones y/o sitios institucionales	Información errónea cargada a sitios o aplicaciones institucionales	Usuarios: ● Desastres causados por personas ● Error por desconocimiento u omisión Fallos de programación: ● Fallas en el diseño del software ● Accesos no autorizados ● Monitoreo de cambios Intrusos: ● Corrupción de datos ● Modificación de la información	Software: ● Ausencia de terminación de sesión ● Asignación errada de los derechos de acceso ● Interfaz de usuario compleja ● Software nuevo o inmaduro Personal: ● Ausencia de personal ● Entrenamiento insuficiente	4	3	12	Desinformación por canales oficiales, atenta contra la reputación de la empresa	Reducir y compartir o transferir el riesgo	5.1.1 6.1.1 14.2.2 14.2.4 17.1.3
DATA CENTER	Hardware, Redes y Telecomunicaciones, Personal, Instalación	Equipos y acceso a aplicaciones y bases de datos	Acceso no controlado al centro de datos	Usuarios: ● Instalación de hardware y software no autorizado ● Usuarios internos q practican actos ilegales ● Desastres causados por personas ● Error en el uso o abuso de derechos Siniestros: ● Desastres por amenazas físicas. Catástrofes Naturales: ● Desastres Naturales ● Penetración en el sistema	Hardware: ● Ausencia de esquemas de reemplazo periódico ● Pérdida de funcionalidad del equipo ● Depreciación de la vida útil de equipos Red: ● Tráfico sensible sin protección Personal: ● Ausencia de políticas de uso aceptable ● Entrenamiento insuficiente	5	5	25	Pérdida absoluta de información crítica y equipos de la ESPAM MFL	Reducir el riesgo, Evitar, Compartir o Transferir	8.1.1 11.1.2 11.1.3 11.2.1 11.2.5 11.2.6

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	Tipo de Activo	Descripción del Activo	Tipo de Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Criticidad	Tipo de Impacto	Medida de Respuesta	Control /es
				Fallas de equipo o electrónico: ● Fallas del equipo ● Daños físicos en los equipos ● Equipo inadecuado para las operaciones	● Trabajo no supervisado de personal externo o de limpieza Lugar: ● Uso inadecuado de los controles de acceso al edificio						
	Hardware, Soporte de Información, Servicios, Aplicaciones	Servidores	Manipulación indebida de los equipos físicos	Usuario: ● Uso no autorizado del equipo Programas maliciosos: ● Virus informáticos ● Activadores no oficiales ● Spyware Fallos de programación: ● Aplicaciones desactualizadas Intrusos: ● Corrupción de datos ● Acceso a los archivos de contraseña ● Acceso a la red Fallos de equipo o electrónicos: ● Daños físicos en los equipos Robo o hurto: ● Robo de información	Hardware: ● Mantenimiento insuficiente ● Pérdida de funcionalidad del equipo ● Depreciación de la vida útil de los equipos Software: ● Ausencia de registros de auditoría Red: ● Conexión deficiente de cableado ● Líneas de comunicación sin protección Personal: ● Concienciación en seguridad de la información ● Trabajo no supervisado de personal externo o de limpieza	3	2	6	Acceso no consentido a los siste32mas informáticos	Asumir el riesgo y Reducir el riesgo	8.1.1 8.1.3 8.1.4 8.2.3 11.1.2 11.1.3 11.1.4 11.2.1 11.2.2 11.2.3 11.2.7 11.2.8 11.2.9 13.1.2 15.1.1 16.1.2
	Hardware y Redes de Telecomunicaciones, Servicios	Data Center	Fallas energéticas	Siniestros: ● Desastres por amenazas físicas ● Pérdidas o fallas de suministros básicos Catástrofes naturales: ● Desastres naturales Fallos de equipo o electrónicos: ● Fallas del equipo ● Daños físicos en los equipos	Hardware: ● Pérdida de funcionalidad del equipo Lugar: ● Conexiones eléctricas inadecuadas y backup para problemas de energía ● Red eléctrica inestable	4	4	16	Daños críticos en los componentes hardware de los servidores	Reducir el riesgo, Evitar, Compartir o Transferir	11.1.4 11.1.5
	Aplicaciones y Servicios	Sistemas operativos e información general de la institución	Sistemas de respaldo no inmutado ante Ransonware	Usuario: ● Piratería ● Falsificación ● Fraude informático Programas maliciosos: ● Ransonware Fallos de programación:	Hardware: ● Almacenamiento sin protección ● Copia no controlada ● Pérdida de funcionalidad del equipo Software: ● Ausencia de registros de auditoría	4	4	16	Pérdida completa de los sistemas de backup por ataque de Ransonware	Reducir el riesgo, Evitar, Compartir o Transferir	12.3.1 12.4.1 12.4.2 12.6.1 12.6.2 12.7.1 16.1.1

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	Tipo de Activo	Descripción del Activo	Tipo de Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Criticidad	Tipo de Impacto	Medida de Respuesta	Control /es
				● Errores en los sistemas operativos ● Información comprometida Intrusos: ● Espionaje remoto ● Corrupción de datos ● Ataques contra el sistema ● Chantaje ● Acceso a la red Robo o hurto: ● Hurto de documentos ● Robo de información	● Software ilegal Red: ● Falta de herramientas de monitoreo Personal: ● Concienciación en seguridad de la información ● Entrenamiento insuficiente						16.1.5 16.1.6 16.1.7
	Hardware, Servicios y Redes de Telecomunicaciones	Servidores	Inhibición de los servidores por procesamiento	Usuario: ● Error por desconocimiento u omisión ● Instalación de hardware y software no autorizado Programas maliciosos: ● Códigos maliciosos Intrusos: ● Invasión ● Espionaje remoto Fallas de equipo o electrónicos: ● Fallas del equipo ● Equipo inadecuado para las operaciones	Hardware: ● Mantenimiento insuficiente ● Pérdida de la funcionalidad del equipo Red: ● Punto único de falla Personal: ● Configuración inadecuada de equipos Lugar: ● Climatización inadecuada	1	3	3	Servicios colapsados por falla de equipo	Asumir el riesgo	8.1.3 8.2.3 11.1.4 11.2.4
	Datos o información, Servicios, y Aplicaciones	Sistemas operativos, aplicaciones y bases de datos	Ataques hacia las aplicaciones	Usuarios: ● Piratería ● Ingeniería social ● Uso no autorizado del equipo Programas maliciosos: ● Spyware ● Código malicioso ● Ransonware Intrusos: ● Corrupción de datos ● Invasión ● Ataques contra el sistema ● Robo o suplantación de identidad Robo o hurto:	Hardware: ● Almacenamiento sin protección Software: ● Contraseñas sin encriptación Red: ● Tráfico sensible sin protección Personal: ● Concienciación en seguridad de la información ● Configuración inadecuada de equipos ● Entrenamiento insuficiente	4	4	16	Información comprometida de la institución, Servicios institucionales no disponibles	Reducir el riesgo, Evitar, Compartir o Transferir	9.1.2 9.4.5 10.1.2 11.1.3 11.1.4 12.2.1 12.6.2 12.7.1 13.1.2 13.1.3 14.1.2 14.2.5 16.1.3 16.1.4

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	Tipo de Activo	Descripción del Activo	Tipo de Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Criticidad	Tipo de Impacto	Medida de Respuesta	Control /es
				● Robo de información							16.1.5
	Hardware, Datos o información, Aplicaciones	Instancias virtuales y servidores físicos y storage de almacenamiento masivo	Servidores no actualizados	Fallos de programación.: ● Aplicaciones desactualizadas Intrusos: ● Ataques contra el sistema	Hardware: ● Mantenimiento insuficiente ● Depreciación de la vida útil de los equipos Software: ● Ausencia de registros de auditoria Red: ● Líneas de comunicación sin protección Personal: ● Entrenamiento insuficiente ● Configuración inadecuada de equipos	5	5	25	Pérdida completa de los sistemas de backup por ataque de Ransonware	Reducir el riesgo, Evitar, Compartir o Transferir	8.1.3 8.2.3 8.3.1 8.3.2 9.4.4 11.2.1 11.2.2 11.2.4 12.4.4 16.1.1
	Servicios, Datos o información	Sistemas operativos y servicios en producción	Defectuosa gestión de proceso de licenciamiento	Usuarios: ● Instalación de hardware y software no autorizado Programas maliciosos: ● Códigos maliciosos ● Virus informático Fallos de programación: ● Fallas en el diseño de software Intrusos: ● Invasión ● Corrupción de datos	Hardware: ● Mantenimiento insuficiente Software: ● Ausencia o insuficiencia de pruebas de software Personal: ● Ausencia de políticas de uso aceptable	5	5	25	Reinicio y apagado de los sistemas	Reducir el riesgo, Evitar, Compartir o Transferir	8 8.1.3 11.2.4 12.1.1 12.2.1 14.2.5 16.1.1

Tabla 7 Matriz Análisis, Evaluación y Tratamiento de Riesgos

13 NORMA ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la información
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

14 POLÍTICAS DE SEGURIDAD

Las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan. La ESPAM MFL:

1. Protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros, o como resultado de un servicio tercerizados.
2. Protegerá y controlará la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.
3. Protegerá su información de las amenazas originadas por el personal interno.
4. Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
5. Implementará control de acceso a la información, sistemas y recursos de red.
6. Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
7. Garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
8. Garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
9. Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
10. Fortalecer la cultura de seguridad de la información en los estudiantes, docentes, personal administrativo y terceros.
11. Garantizar la continuidad del negocio frente a incidentes.

El incumplimiento a las políticas de seguridad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

14.1 PROPIEDAD Y USO

1. Toda la información generada y/o contenida en los activos de información institucionales, excluyendo la información personal de los miembros de la comunidad politécnica, es propiedad de la ESPAM MFL.
2. Toda la información generada en activos de información que no son institucionales, producto del ámbito de competencia de los miembros de la comunidad politécnica, es propiedad de la ESPAM MFL.
3. Toda información y activo de información institucional, se utilizará y estará, en forma exclusiva, al servicio de los intereses de la ESPAM MFL y sus dependencias.

4. Es responsabilidad de los miembros de la comunidad politécnica el uso adecuado de la información, así como de los activos de información institucionales.
5. La UT podrá presentar directrices y/o procedimientos para que los activos de información se encuentren actualizados y asegurados.
6. La UT podrá gestionar mecanismos para la protección de los activos de información institucionales.
7. La UT podrá realizar evaluaciones técnicas en los activos de información de propiedad de la ESPAM MFL e informará a las autoridades sobre actividades consideradas no permitidas con respecto a tales activos.
8. El uso o divulgación ilegal o inadecuada de información o activos de información institucional dará lugar a las acciones legales y disciplinarias pertinentes.
9. No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución y el ordenamiento jurídico interno.
10. Los usuarios que tienen acceso a información generada por cualquier actividad de investigación realizada por la Universidad tendrán prohibido efectuar copias de esta y realizar ventas fraudulentas en formato digital.
11. Los usuarios tienen prohibido sustraer y divulgar información confidencial de la ESPAM MFL a terceras personas ajenas a la Institución.
12. Los usuarios tienen prohibido falsificar información en nombre de la ESPAM MFL.
13. La información institucional contenida en los servidores deberá ser asegurada por parte del administrador de servidores, mediante cifrado, niveles de control de acceso y contraseñas de usuario.
14. Para tener acceso a información confidencial contenida en los servidores, deberá existir la aprobación de uso por parte de la máxima autoridad de la ESPAM MFL y del Coordinador de la UT.
15. El usuario es responsable de evitar la fuga de información confidencial de la Universidad, contenida en los equipos de cómputo que estén bajo su custodia.
16. Es obligación de los usuarios proteger cualquier información que consideren sensible o vulnerable mediante derechos de acceso si el programa donde lo desarrolló lo permite.

14.2 ACUERDOS DE CONFIDENCIALIDAD Y NO DIVULGACIÓN

1. La UT gestionará los acuerdos de confidencialidad y no divulgación de la Información con los miembros de la comunidad politécnica.
2. La UT gestionará los acuerdos de confidencialidad y no divulgación de la Información con los proveedores contratados u otras instituciones públicas o privadas que requieren acceso a los activos de información institucional.
3. Los datos personales de los miembros de la comunidad politécnica son confidenciales y podrán ser utilizados solamente para fines de gestión, investigación, docencia y vinculación de la ESPAM MFL.

4. La UT deberá generar y podrá actualizar procedimientos para que se apliquen criterios de confidencialidad en los sistemas de información.
5. La UT implementará y difundirá buenas prácticas de seguridad que contemplen la sensibilización en temas de información confidencial a la comunidad politécnica.

14.3 RECURSO DE LOS USUARIOS

1. Los usuarios deberán cuidar, respetar y hacer buen uso de los recursos informáticos de la ESPAM MFL, de acuerdo con las políticas que en este documento se mencionan.
2. La información de trabajo generada en los recursos informáticos de la institución deberá ser almacenada en el espacio lógico asignado a los usuarios.
3. Es responsabilidad del usuario interno, mantener seguras las contraseñas de sus cuentas de usuario de correo electrónico o de sistemas informáticos, y no compartirlas con terceras personas.
4. Se debe mantener conectado el equipo de cómputo a un UPS o regulador de voltaje, para evitar daños, en casos de variaciones o cortes de energía eléctrica.
5. Todo usuario al finalizar su día de trabajo debe apagar los equipos de cómputo asignados. No se permite dejar equipos de cómputo encendidos de un día para otro. Esta regla no aplica a equipos que estén realizando procesos nocturnos, procesos de prueba o diagnósticos cuyo conocimiento lo tenga la UT.
6. Los medios de almacenamiento externo (Flash Memory, Disco Duro, DVD, CD externo) provistos por la ESPAM MFL, son exclusivamente para trabajos dentro de la institución, estos no podrán salir, salvo aprobación de la máxima autoridad.
7. No se debe instalar o manipular software, imágenes, videos o sonidos no autorizados, que puedan afectar la seguridad e integridad de la información, de los equipos de cómputo o la red de datos.

14.4 USO DE SISTEMAS INFORMÁTICOS INSTITUCIONALES

1. Los usuarios autorizados podrán tener acceso a los sistemas informáticos institucionales, para realizar sus labores diarias.
2. Los usuarios no podrán cambiar datos del sistema informático como notas, valores, entre otros sin la previa aprobación de la autoridad competente y por escrito.
3. Los usuarios no podrán hacer mal uso de la información descargada de los sistemas informáticos.

14.5 USO DE ANTIVIRUS INSTITUCIONAL

1. Todo equipo que se conecte a la red de datos o algún sistema de información de la ESPAM MFL debe estar ejecutando un antivirus actualizado.
2. Todos los equipos de cómputo pertenecientes a la Institución deberán tener instalado el antivirus con licencia, adquirido por la ESPAM MFL.

3. La UT es la encargada y responsable de la administración de la plataforma del software antivirus.
4. Los usuarios al detectar algún virus informático no deberán tomar acciones para eliminar el virus, debe contactarse con la UT para que el técnico delegado proceda a dar solución al incidente.
5. Los usuarios deben ejecutar el antivirus antes de utilizar medios de almacenamiento extraíble.
6. Los técnicos de la UT son los únicos autorizados para instalar y actualizar el antivirus, solo en los equipos de cómputo pertenecientes a la ESPAM MFL.
7. Los usuarios tienen prohibido instalar o descargar software, programas o aplicativos que no cuenten con licencia o provengan de algún sitio web desconocido, lo cual podría ocasionar la infección del equipo de cómputo por virus informáticos.
8. La UT se encargará de realizar revisiones periódicas a los equipos y sistemas, con el fin de mantener protegidos los recursos informáticos y evitar futuros inconvenientes, realizando lo siguiente:
   a. Actualización automática de las bases de virus y análisis al equipo de cómputo que se encuentran conectados a la red de datos institucional.
   b. Actualización manual de las bases y análisis al equipo que no están conectados a la red.
9. Los usuarios tienen prohibido desinstalar el antivirus del equipo que se encuentre bajo su responsabilidad, ya que podría ocasionar la vulnerabilidad de este.

14.5.1 USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

1. Las cuentas de correo electrónico institucional son generadas por la UT, con el empleo de dominios válidos autorizados por la ESPAM MFL.
2. Los usuarios que requieran de la creación del correo electrónico la solicitarán a la UT, con la debida autorización del Director, Coordinador o Jefe del departamento solicitante, mediante formato de solicitud, oficio o correo electrónico.
3. Los usuarios asumen la responsabilidad del uso que hacen de su cuenta de correo electrónico institucional, siendo conscientes de que cualquier mensaje que lleve el dominio @espam.edu.ec representa a la Universidad en su conjunto.
4. Las cuentas de correo electrónico institucional no deben ser usadas para difundir contenidos discriminatorios, despectivos, difamatorios, acosadores o violentos.
5. Los usuarios de las cuentas de correo electrónico son los responsables del contenido emitido y enviado en los mensajes electrónicos, así como de la información adjunta que se remita.
6. La UT deberá generar y podrá actualizar la directriz para el "Políticas de uso correcto correos electrónicos".
7. El correo electrónico institucional asignado al personal administrativo y docentes, será para uso obligatorio y exclusivo del envío y recepción de mensajes relacionados con las actividades laborales y académicas.

8. Los usuarios no deberán crear o reenviar a través de correo electrónico cadenas o cualquier otro tipo de esquemas de pirámides.
9. No está permitido utilizar el correo electrónico con fines comerciales o financieros.
10. Si se detecta que un usuario ha hecho uso inapropiado del correo electrónico institucional, se lo notificará formalmente por escrito, sin perjuicio de la aplicación, si procede, de acuerdo con el régimen disciplinario correspondiente.
11. La UT se encargará de depurar las cuentas de correo electrónico institucional, de tal forma que solo estén registrados los usuarios que actualmente laboran en la ESPAM MFL, respaldados y autorizados por el departamento de Talento Humano.
12. Los usuarios deben tener extrema precaución cuando revisen archivos adjuntos recibidos en mensajes de correo electrónico que provengan de remitentes conocidos o desconocidos, pues estos deben contener algún tipo de virus.
13. Los usuarios de correo electrónico son responsables de mantener segura la clave y la información contenida en el mismo. La UT no se hace responsable por perdida de información del correo institucional.

14.6 INSTALACIÓN DE SOFTWARE

1. El software y aplicaciones que se instalan en los dispositivos tecnológicos que pertenecen a la ESPAM MFL deben ser licenciados.
2. No está permitida la instalación de software o aplicaciones piratas o de dudosa procedencia.
3. La UT podrá desinstalar todo software y/o aplicación pirata o de dudosa procedencia que se haya configurado en los dispositivos tecnológicos de la Institución.

14.7 AUDITORÍA Y EVALUACIÓN DE VULNERABILIDADES

1. La UT verificará el cumplimiento de la normativa interna relacionada con seguridad informática, así como el seguimiento a las recomendaciones emitidas en informes ante los incidentes de seguridad informática que se han gestionado.
2. La UT podrá realizar auditorías y/o revisiones de seguridad informática, con periodicidad anual.
3. La UT podrá analizar, dar soporte y coordinar la respuesta a los incidentes de seguridad informática que se presenten con los activos de información institucionales.
4. La UT podrá gestionar las vulnerabilidades detectadas en los activos de información institucional.
5. Los resultados de las evaluaciones y auditorias de seguridad informática podrán ser comunicados por la UT a la máxima autoridad de la institución.

14.7.1 ADMINISTRACIÓN DE LOS SERVIDORES

1. La UT a través del administrador de servidores tendrá la responsabilidad de controlar, verificar y comprobar la instalación, configuración e implementación de la seguridad de los servidores en la red de datos de la ESPAM MFL.
2. El Coordinador de la UT designará a la persona autorizada y responsable de la Administración de los servidores de la Institución.
3. Se deberá notificar a la UT la instalación y/o configuración de cualquier equipo servidor que deseen conectar a la red de la Universidad, para ser asesorados y brindarles los permisos requeridos por el administrador de servidores.
4. Los equipos servidores que serán destinados para uso y bajo custodio de la UT, solo será responsabilidad del administrador de servidores.
5. El administrador de servidores al realizar configuraciones debe aplicar normas y estándares establecidos, para la correcta operación de estos, así como la restricción de directorios y programas que serán usados por los usuarios.
6. Los servidores que brindan servicios de internet, correo electrónico, impresión, entre otros; deberán:
   a. Funcionar las 24 horas del día y durante todo el año.
   b. Recibir mantenimiento preventivo físico y lógico dos veces al año.
   c. Deben ser monitoreados por el administrador de servidores.
   d. La información contenida en los servidores deberá estar respaldada.
7. Los equipos servidores deberán ser ubicados dentro de un área que cumpla todas las normas y estándares actuales, para mantenerlos seguros.

15 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Se distinguirá entre la gestión de la seguridad de la información en el seno de la propia administración y la seguridad que se mantenga con los activos de información que sean accesibles por usuarios externos u otras organizaciones.

15.1 COMPROMISO DE LA MÁXIMA AUTORIDAD DE LA INSTITUCIÓN CON LA SEGURIDAD DE LA INFORMACIÓN

1. Realizar el seguimiento de la puesta en marcha de las normas de este documento.
2. Disponer la difusión, capacitación y sensibilización del contenido de este documento.
3. Conformar oficialmente la comisión que se encargará de gestionar la Seguridad de la Información institucional.

15.1.1 IDENTIFICACIÓN DE LOS RIESGOS RELACIONADOS CON LAS PARTES EXTERNAS

1. Identificar y evaluar los riesgos para la información y los servicios de procesamiento de información de la entidad en los procesos que involucran a terceros e implementar los controles apropiados antes de autorizar el acceso.
2. Bloquear el acceso a la información de la organización a terceros, hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones del caso, así como acuerdos de confidencialidad respecto de la información a la tendrán acceso.
3. Garantizar que terceros esté consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de información de la organización.
4. Registrar y mantener a terceros vinculados a la entidad considerando los siguientes tipos: proveedores de servicios (Internet, proveedores de red, servicios telefónicos, servicios de mantenimiento, energía eléctrica, agua, entre otros).

15.2 ORGANIZACIÓN INTERNA

15.2.1 COORDINACIÓN DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La coordinación estará a cargo de la comisión encargada de gestionar la Seguridad de la Información, el cual tendrá las siguientes funciones:

1. Definir y mantener la política y normas institucionales particulares en materia de seguridad de la información y gestionar la aprobación y puesta en vigencia por parte de la máxima autoridad de la institución, así como el cumplimiento por parte de los funcionarios de la institución.
2. Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
3. Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
4. Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada área.
5. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
6. Promover la difusión y apoyo a la seguridad de la información dentro de la institución.
7. 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.
8. Designar a los custodios o responsables de la información de las diferentes áreas de la entidad, que deberá ser formalizada en un documento físico o electrónico.

9. Gestionar la provisión permanente de recursos económicos, tecnológicos y humanos para la gestión de la seguridad de la información.

15.2.2 CONTACTO CON LAS AUTORIDADES

1. Establecer un procedimiento que especifique cuándo y a cuáles autoridades se reportarán los incidentes derivados por infringir las políticas de seguridad o por acciones de seguridad de cualquier origen (fiscalía, policía, bomberos, 911). Todo incidente de seguridad de la información que sea considerado crítico deberá ser reportado a la UT y la máxima autoridad según los casos.
2. Reportar oportunamente los incidentes identificados de la seguridad de la información a las autoridades nacionales, si se sospecha de incumplimiento de la ley o que provoquen indisponibilidad o continuidad.
3. Identificar y mantener actualizados los datos de contacto de proveedores de bienes o servicios de telecomunicaciones para gestionar potenciales incidentes.
4. Establecer acuerdos para compartir información con el objetivo de mejorar la cooperación y la coordinación de los temas de la seguridad. Tales acuerdos deberían identificar los requisitos para la protección de la información sensible.

15.2.3 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

1. Ejecutar revisiones independientes de la gestión de la seguridad a intervalos planificados o cuando ocurran cambios significativos en la implementación.
2. Identificar oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control a partir de las revisiones independientes. La revisión deberá contemplar las actuaciones de la alta dirección, de la comisión de seguridad.
3. Registrar y documentar todas las revisiones independientes de la gestión de la seguridad de la información que la institución realice.

15.3 DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO

El objetivo de este apartado es poder garantizar la seguridad en dispositivos móviles y en las condiciones del teletrabajo. Se debe considerar lo siguiente:

15.3.1 DISPOSITIVOS MÓVILES

1. El registro de nuevos dispositivos.
2. La cancelación de registro de dispositivos móviles.
3. Requisitos de seguridad física.
4. Requisitos de seguridad técnica incluidas conexiones remotas.
5. Control de software.
6. Control de acceso y encriptación en reposo y de dispositivos en tránsito.

15.3.2 TELETRABAJO

1. Evaluar que activos de información están involucrados en el teletrabajo.
2. Realizar una evaluación de riesgos aplicada a los activos de la información y a las actividades del teletrabajo.
3. Aplicar los controles adecuados para mitigar los riesgos identificados.

16 SEGURIDAD DE LOS RECURSOS HUMANOS

Se debe asegurar que cualquier persona que participe en la organización, conozca y acepte la responsabilidad que conlleva la seguridad de la información, de sus sistemas, redes y demás activos.

16.1 ANTES DE LA CONTRATACIÓN

16.1.1 TÉRMINOS Y CONDICIONES LABORALES

1. Realizar la firma de un acuerdo de confidencialidad o no-divulgación, antes de que los empleados, contratistas y terceros, tengan acceso a la información. Dicho acuerdo debe establecer los parámetros vigencia del acuerdo, información confidencial referida, formas de acceso, responsabilidades y funciones.
2. Socializar los derechos y responsabilidades legales de los empleados, los contratistas y cualquier otro usuario sobre la protección de datos; dejando constancia de lo actuado a través de hojas de registro, informes o similares, que evidencie la realización de esta.
3. Responsabilizar al personal sobre el manejo y creación de la información resultante durante el contrato laboral con la institución.

16.2 DURANTE LA CONTRATACIÓN

1. Explicar y definir las funciones y las responsabilidades respecto a la seguridad de la información, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles.
2. Lograr la concienciación sobre la seguridad de la información correspondiente a sus funciones y responsabilidades dentro de la institución.
3. Acordar los términos y las condiciones laborales, las cuales incluyen políticas de la seguridad de la información de la institución y los métodos apropiados de trabajo.
4. Verificar el cumplimiento de las funciones y responsabilidades respecto a la seguridad de la información mediante la utilización de reportes e informes.

16.3 CESE O CAMBIO DE PUESTO DE TRABAJO

1. Retirar los privilegios de acceso a los activos de información y a los servicios de procesamiento de información (sistema de directorio, correo electrónico, accesos

físicos, sistemas) inmediatamente luego de que se comunique formalmente a la UT la terminación de la relación laboral por parte del área correspondiente
2. Se debe realizar la devolución de activos, tales como equipos, documentos, software, computadores, tarjetas de acceso, carnets, etc.
3. Retire los derechos de acceso a la información y recursos. En caso de cambio de cargo, se deben revisar los derechos y roles, con el fin de no permitir accesos que no han sido aprobados para la nueva función.

17 GESTIÓN DE ACTIVOS

La gestión de activos permite que una organización disponga de un conocimiento profundo de toda su infraestructura, facilitando la entrega de servicios y la resolución de cualquier incidencia relacionada con las tecnologías de la información.

17.1 RESPONSABILIDAD SOBRE LOS ACTIVOS

1. Elaborar el inventario de los activos a su cargo y mantenerlo actualizado.
2. Clasificar, documentar y mantener actualizada la información y los activos, y definir los permisos de acceso a la información.
3. Consolidar los inventarios de los activos a cargo del responsable del Activo, por área o unidad organizativa.
4. El resguardo para los equipos de cómputo tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

17.2 INVENTARIAR LOS ACTIVOS PRIMARIOS, EN FORMATOS FÍSICOS Y/O ELECTRÓNICOS

1. Los manuales e instructivos de sistemas informáticos: instalación, manual de usuario, operación, administración, mantenimiento, entre otros.
2. Los aplicativos informáticos de los servicios informáticos: datos y metadatos asociados, archivos de configuración, código fuente, respaldos, versiones, etc.
3. Del desarrollo de aplicativos de los servicios informáticos: actas de levantamiento de requerimientos, documento de análisis de requerimientos, modelado, diseño de componentes, casos de uso, diagramas de flujo y estado, casos de prueba.
4. Del soporte de aplicativos de los servicios informáticos: tickets de soporte, reportes físicos y electrónicos, evaluaciones y encuestas, libros de trabajo para capacitación, etc.

17.3 INVENTARIAR LOS ACTIVOS DE SOPORTE DE HARDWARE

1. Equipos móviles: teléfono inteligente (smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc.
2. Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc.

3. Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, etc.
4. Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plotter, máquina de fax, etc.
5. Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos CD, DVD, Blu-ray, memoria USB, etc.
6. Periféricos de comunicaciones: tarjeta USB para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta PCMCIA para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta USB para redes alámbricas/inalámbricas de datos y de telefonía, etc.
7. Tableros: de transferencia (bypass) de la unidad sin interrupción de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.
8. Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de video vigilancia, etc.

17.4 INVENTARIAR LOS ACTIVOS DE SOPORTE DE SOFTWARE

1. Sistemas operativos.
2. Paquetes de software o software base de: suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, vídeo conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc.
3. Aplicativos informáticos del negocio.

17.5 INVENTARIAR LOS ACTIVOS DE SOPORTE DE REDES

1. Cables de comunicaciones (interfaces: RJ-45 o RJ-11, SC, ST o MT-RJ, interfaz V35, RS232, USB, SCSI, LPT), panel de conexión (patch panel), tomas o puntos de red, racks (cerrado o abierto, de piso o pared), etc.
2. Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-point, transceiver, equipo terminal de datos, etc.).
3. Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc.
4. Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc.

17.6 RETIRO/DEVOLUCIÓN DE ACTIVOS DE LA PROPIEDAD

1. Tener autorización previa para el retiro de cualquier equipo, información o software.
2. Identificar a los empleados, contratistas y usuarios de terceras partes, que tienen la autorización para el retiro de activos de la institución.

3. Establecer límites de tiempo para el retiro de equipos y verificar el cumplimiento en el momento de la devolución.
4. Registrar cuando el equipo o activo sea retirado y cuando sea devuelto.

17.7 USO ACEPTABLE DE LOS ACTIVOS

1. Los activos deben utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.
2. Concientizar al usuario sobre el uso correcto o aceptable de los activos, asimismo, de las responsabilidades que conlleve no cumplir con estas disposiciones.

17.8 CLASIFICACIÓN DE LA INFORMACIÓN

Se pueden establecer niveles para clasificar la información, según el carácter confidencial de la misma:

1. Confidencial: cuando el nivel de confidencialidad de la información se incremente.
2. Restringido: para niveles medios de confidencialidad.
3. Uso interno: información con un nivel bajo de confidencialidad.
4. Público: cuando todas las personas pueden ver la información.

17.8.1 PROCEDIMIENTOS PARA EL MANEJO DE LA INFORMACIÓN

1. Establecer procedimientos para el manejo y etiquetado de todos los medios de acuerdo con su nivel de clasificación.
2. Establecer controles de acceso para evitar el acceso de personal no autorizado.
3. Tener un registro actualizado de los receptores de los medios.
4. Establecer controles de protección según el nivel de sensibilidad de los datos que reside en la memoria temporal.
5. Almacenar los medios según especificaciones del fabricante.

17.8.2 SEGURIDAD DE LA DOCUMENTACIÓN DEL SISTEMA.

1. Guardar con seguridad toda la documentación de los sistemas informáticos.
2. Mantener una lista de acceso mínima a la documentación del sistema y con su debida autorización.
3. Mantener una protección adecuada de la documentación del sistema expuesta en la red pública.

17.8.3 MENSAJERÍA ELECTRÓNICA

1. Establecer lineamientos para proteger los mensajes contra los accesos no autorizados, modificación o denegación de los servicios.
2. Supervisar que la dirección y el transporte de mensajes sean correctos.
3. Tomar en cuenta consideraciones legales como la de firmas electrónicas.

4. Encriptar los contenidos y/o información sensible que puedan enviarse por mensajería electrónica; utilizando firmas electrónicas reconocidas por el Estado Ecuatoriano u otras tecnologías evaluadas y aprobadas por el Gobierno Nacional.

17.9 FIRMA DIGITAL

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Pueden aplicarse a cualquier tipo de documento que se procese electrónicamente. Se implementan mediante el uso de una técnica criptográfica sobre la base de dos claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

17.9.1 TRANSACCIONES EN LÍNEA

1. Establecer procedimientos para garantizar todos los aspectos en la transacción como credenciales de usuario, confidencialidad de la transacción y privacidad de las partes.
2. Definir procedimientos para el uso de certificados de firmas electrónicas por las partes implicadas en la transacción.
3. Cifrar o encriptar el canal de comunicaciones entre las partes involucradas (por ejemplo, utilizando SSL/TLS).
4. Establecer protocolos seguros en la comunicación de las partes involucradas, por ejemplo, utilizando SSL/TLS).
5. Establecer procedimientos para que las transacciones se encuentren fuera del entorno de acceso público.
6. Utilizar los servicios de una entidad certificadora confiable.

17.9.2 INFORMACIÓN DISPONIBLE AL PÚBLICO

1. Establecer controles para que la información disponible al público se encuentre conforme a la normativa vigente.
2. Definir controles para que la información de entrada sea procesada completamente y de forma oportuna.
3. Establecer procedimientos para que la información sensible sea protegida durante la recolección, procesamiento y almacenamiento.

17.10 MANEJO DE LOS SOPORTES DE ALMACENAMIENTO

Pueden suponer una brecha importante en la seguridad de la información por lo que la norma propone un control específico para este tipo de soportes.

17.10.1 GESTIÓN DE LOS MEDIOS REMOVIBLES.

1. Establecer un procedimiento para la gestión de todos los medios removibles.
2. Tener autorización para la conexión de los medios removibles y registrar la conexión y retiro, para pruebas de auditoría.
3. Almacenar los medios removibles en un ambiente seguro, según las especificaciones de los fabricantes.
4. Evitar la pérdida de información por deterioro de los medios.

17.10.2 ELIMINACIÓN DE LOS MEDIOS

1. Identificar los medios que requieran eliminación segura.
2. Almacenar y eliminar de forma segura los medios que contienen información sensible, como la incineración, trituración o borrado de los datos.
3. Establecer procedimientos para selección del contratista que ofrece servicios de recolección y eliminación del papel, equipos y medios.
4. Registrar la eliminación de los medios para mantener pruebas de auditoría.

18 CONTROL DE ACCESO

Están orientadas a controlar y monitorizar los accesos a los medios de información de acuerdo con las políticas definidas por la organización.

18.1 POLÍTICA DE CONTROL DE ACCESO

1. Todos los sistemas de información que adquiera y/o desarrolle la ESPAM MFL deben contar con mecanismos de control y autenticación cifrados para el acceso a los mismos, por ejemplo: uso de cuentas de usuarios, contraseñas, doble autenticación, registro de acceso, permisos.
2. Gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.
3. Definir responsabilidades para la identificación, gestión y conservación de perfiles de los custodios de información.
4. La Dirección de Talento Humano o Coordinador de cada unidad solicitará a la UT la creación de credenciales de red (usuarios y contraseña), para el nuevo personal administrativo o docente.
5. La UT deberá generar y podrá actualizar las directrices que consideren adecuadas para realizar el respectivo control de acceso.
6. La UT controlará el acceso a la red y servidores de la ESPAM MFL, de acuerdo con las necesidades del usuario.
7. Los usuarios tendrán acceso a la red de datos mediante la autenticación de usuario y contraseña provistos por la UT.
8. El personal administrativo y docente no deberá revelar la clave de su cuenta de usuario de red a terceras personas.

9. Los usuarios de la red no deberán interrumpir las comunicaciones en la red de datos, o cambiar la configuración de la red utilizando cualquier tipo de software que monitoree, analice, o perturbe las actividades normales de la misma.
10. Los usuarios tienen prohibido acceder a datos en algún servidor a través de la red de datos para los cuales no estén autorizados.
11. Los usuarios no deben ingresar con una cuenta que no esté asignada para acceder a la red, a menos que estas actividades estén dentro del alcance de sus actividades.
12. Los usuarios no deberán evadir la autenticación de usuario o cualquier seguridad de algún equipo, red o cuenta de usuario propiedad de la ESPAM MFL.
13. Está prohibido que los usuarios revisen los recursos compartidos en la red, en busca de información no autorizada, para alterarla, copiarla, robarla o destruirla.
14. La UT empleará dispositivos de red para el monitoreo, bloqueo, enrutamiento o filtrado de tráfico, evitando el acceso a información confidencial que pueda ser enviada desde la red interna hacia el exterior.
15. Se prohíbe interferir con las actividades normales de cualquier usuario o negarle el acceso a algún servicio de red que él necesite para poder realizar sus labores.
16. Está prohibido utilizar algún programa, script, o comando para enviar mensajes de cualquier índole, con la intención de interferir o deshabilitar el equipo de algún usuario, sea esto localmente, a través de internet o alguna conexión remota.
17. La UT o administrador de redes no serán responsables por el contenido de los datos que circulen en la red, el usuario emisor será el único responsable por la información que envíe o intercambie con los demás usuarios.

18.2 CREDENCIALES DE ACCESO A LOS ACTIVOS DE INFORMACIÓN INSTITUCIONAL

1. Las credenciales de acceso a los activos de información son personales e intransferibles y no deben ser expuestas en sitios visibles.
2. La UT notificará a la Dirección de Talento Humano en caso de detectar que cualquier miembro de la Comunidad Politécnica, utiliza inadecuadamente sus credenciales de acceso entregándolas a cualquier persona, sean a usuarios internos o externos, como lo establece el acuerdo de confidencialidad.
3. Es responsabilidad de cada miembro de la comunidad politécnica acatar y cumplir todas las disposiciones y procedimientos establecidos, para mantener la confidencialidad en el uso de credenciales institucionales de acceso a los activos de información.

18.3 CONTROL DE ACCESO A LAS REDES Y SERVICIOS ASOCIADOS

Las conexiones no seguras a los servicios de red pueden afectar a toda la ESPAM MFL, por lo tanto, la UT controlará el acceso a los servicios de red internos como externos:

1. Identificar las redes y servicios de red a los cuales se permite el acceso.

2. Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
3. Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.
4. Todos los accesos deben poder ser sujetos de monitoreo y conservación permanente por parte de la UT.
5. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la institución, y no debe utilizarse para ningún otro fin.
6. Debe limitarse a los usuarios el acceso a portales, aplicaciones o servicios de la Internet y la Web que pudieren perjudicar los intereses y la reputación de la institución.
7. Se debe bloquear el acceso por medio de dispositivos fijos y/o móviles a aquellos 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 o que impacten negativamente en la productividad y trabajo de la institución y particularmente a los que atenten a la ética y moral.
8. La institución podrá en cualquier momento bloquear o limitar el acceso y uso de la Internet a los funcionarios o a terceros que accedan tanto por medio alámbrico como inalámbrico.

18.3.1 USO DEL INTERNET

1. El internet debe estar disponible para todos los miembros de la comunidad politécnica.
2. Se solicitará, mediante oficio a la UT, las credenciales de la red para tener acceso al servicio de internet.
3. El servicio de internet solo será utilizado por personal administrativo, docentes y estudiantes para fines laborales, consultas e investigaciones, accediendo a sitios de carácter académico y científico.
4. Los usuarios no deben ingresar a páginas con contenido no permitido, de entretenimiento u otros que no estén relacionados con las actividades laborales o académicas de la ESPAM MFL.
5. Los usuarios no deberán descargar videos, imágenes, música o programas gratuitos sin licencias que oferten en la web.
6. El uso de blogs, redes sociales, contenedores de video, entre otros, por parte de los miembros de la comunidad politécnica, está limitado según el perfil de los usuarios y, en forma ocasional, fuera de horario de trabajo, para que tal uso no interfiera en las labores diarias de estos.
7. Queda prohibido el difundir contenidos discriminatorios, despectivos, difamatorios o acosadores, así como cualquier otro contrario a la legalidad o la ética, así como el envío de mensajes no relacionados con los objetivos de la Institución, empleando la infraestructura de la ESPAM MFL.

18.3.2 USO DE LA RED INALÁMBRICA (WIFI)

1. La UT proveerá del servicio de red inalámbrica, a los docentes, áreas administrativas y a la comunidad estudiantil de la ESPAM MFL.
2. Los usuarios que cuenten con un dispositivo móvil, sea este un celular, Tablet o laptop, podrán acceder a la red inalámbrica, para realizar trabajos académicos como investigación y consultas.
3. Los usuarios tienen prohibido hacer uso del servicio de red inalámbrica para:
   a. Acosar, amenazar o intimidar a otras personas.
   b. Realizar acciones de rastreo, difusión de virus o acceder a recursos informáticos de la ESPAM MFL.
   c. Descargar programas, juegos, música, videos o imágenes inapropiadas.
   d. Enviar información personal como números de tarjetas, claves etc.
   e. Transferir información que viole el derecho de autor, material pornográfico, mensajes amenazantes u obscenos.
4. La UT no será responsable de la información que se transmita por la red inalámbrica, que realizan los estudiantes o docentes.
5. Los usuarios deberán tener cuidado de ingresar a sitios web no seguros o descargar información que pueda contener virus informáticos.

18.3.3 USO DE IMPRESORAS EN RED

1. Las impresoras conectadas en red, solo se utilizarán para trabajos relacionados con las actividades laborales del personal administrativo y docente.
2. Los usuarios no deberán utilizar las impresoras en red, para imprimir trabajos, imágenes o documentos personales.
3. Los usuarios deberán solicitar a la UT la configuración de la impresora en red a un nuevo equipo de cómputo, para poder acceder a este servicio.

18.3.4 SEGURIDAD DE REDES LAN E INALÁMBRICA

1. La UT podrá implementar filtros para todo el tráfico entre el Internet y la red LAN e inalámbrica de la ESPAM MFL, utilizando para el efecto herramientas especializadas.
2. La UT podrá activar el cifrado, autenticación y autorización en las redes LAN e inalámbricas para mantener limitado el acceso a estas.

18.3.5 SEGURIDAD DE REDES PRIVADAS VIRTUALES (VPN)

1. Toda conexión a la red de la ESPAM MFL mediante el uso de VPN será autorizada y monitoreada por la UT.
2. Implementar credenciales para acceder a los servicios mediante conexiones VPN.

18.3.6 REDES INALÁMBRICAS NO AUTORIZADAS

1. Está prohibida la instalación en la red de la ESPAM MFL de todo dispositivo (puntos de acceso, routers inalámbricos, entre otros) que no haya sido verificado y validado por la UT.
2. La UT podrá, retirar y desinstalar el servicio prestado por dispositivos no autorizados.

18.4 REGISTRO DE USUARIOS

1. Establecer un procedimiento formal, documentado y difundido, en el cual se evidencie detalladamente los pasos y responsables.
2. Definir el administrador de accesos que debe controlar los perfiles y roles.
3. Crear los accesos para los usuarios, para lo cual la institución debe generar convenios de confidencialidad y responsabilidad con el usuario solicitante; además, validar que el usuario tenga los documentos de ingreso con Recursos Humanos.
4. Modificar y eliminar los accesos de los usuarios.
5. Proporcionar accesos temporales a usuarios externos o terceros de acuerdo con el tiempo de su permanencia y limitados según las actividades para las que fueron contratados, de igual manera firmar un convenio de confidencialidad.
6. Suspender temporalmente los accesos de los usuarios en caso de vacaciones, comisiones, licencias, es decir, permisos temporales.
7. Mantener un registro de la gestión de accesos a aplicaciones y redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso; asimismo, disponer de los permisos de acceso que han sido asignados.

18.5 GESTIÓN DE CONTRASEÑAS PARA USUARIOS

1. Establecer un proceso formal para la asignación y cambio de contraseñas.
2. Garantizar que los usuarios cambien las contraseñas iniciales previas al primer ingreso al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
3. Generar contraseñas provisorias seguras para otorgar a los usuarios.

18.5.1 USO DE CONTRASEÑAS

1. Documentar, en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignados.
2. Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta.

3. Evitar contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables; por ejemplo: admin, administrador, administrador, user, usuario, entre otros.
4. Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas y evitar reutilizar o reciclar viejas contraseñas.
5. Controlar el cambio periódico de contraseñas de los usuarios.
6. Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte de la Unidad de Tecnología.

18.6 REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS

1 Realizar las depuraciones respectivas de los accesos de los usuarios, determinando un período máximo de 30 días; en casos de presentar cambios estructurales, esta gestión deberá hacerse inmediatamente que se ejecute el cambio organizacional.
2 Evidenciar los cambios sobre los derechos de acceso en archivos de log o registro de los sistemas, los cuales deben estar disponibles en caso de que se requieran.

18.7 CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN

1. Se definirán las funciones y restricciones para el uso de los sistemas informáticos institucionales, es decir, cada usuario solo podrá acceder a las funciones del sistema que le corresponden.
2. Suministrar protección contra acceso no autorizado por un programa utilitario, software del sistema operativo, software malicioso o cualquier otro software que pueda anular o desviar los controles de seguridad del sistema.
3. La Dirección de Talento Humano, solicitará a la UT la creación o eliminación de credenciales para el acceso a los sistemas informáticos por parte del personal administrativo o docente, así como el personal entrante o saliente de la institución.
4. Los usuarios no deberán compartir sus credenciales de autenticación para el ingreso a los sistemas informáticos institucionales, a personas no autorizadas.
5. La UT se encargará de depurar las credenciales de autenticación de acceso a los sistemas informáticos, de acuerdo con los registros proporcionados por la Dirección de Talento Humano, al haber movimientos de personal.
6. El Coordinador de la UT, designará a la persona autorizada y responsable de la Administración de las Bases de Datos, en este caso el analista/programador.
7. El administrador de la Base de Datos (BD), es la persona autorizada y responsable de acceder a la información contenida en las bases para realizar las siguientes actividades:
    a. Respaldar las BD´s de los Sistemas Informáticos Institucionales.
    b. Resolver problemas que los usuarios no pueden solucionar mediante la plataforma.
    c. Monitorear y diagnosticar los Sistemas Informáticos Institucionales.

8. El administrador de las BD´s no podrán eliminar información de los sistemas, salvo el caso que este dañada o pongan en riesgo el funcionamiento del sistema. Asimismo, no podrá sustraer, divulgar, destruir o suprimir información contenida en la BD, en caso de cometer alguno de estos delitos, será sancionado según las leyes ecuatorianas.

18.8 CONTROL DE ACCESO AL CÓDIGO FUENTE DE LOS PROGRAMAS

1. Asignar a un administrador de programas fuentes, quien tendrá en custodia los programas fuentes y deberá
2. Utilizar un manejador de versiones para los códigos fuente, proporcionar permisos de acceso a los desarrolladores bajo autorizaciones.
3. Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación o en producción).
4. Hay que asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador, sin un manejador de versiones.
5. Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
6. Establecer que el responsable de implantación en producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.
7. Desarrollar un procedimiento que garantice que cuando se migre a producción el módulo fuente, de preferencia se cree el código ejecutable correspondiente de forma automática de preferencia.
8. Evitar que la función de administrador de programas fuentes, sea ejercida por personal que pertenezca al área de desarrollo y/o mantenimiento.
9. Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
10. Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos como respaldos de información.
11. La actualización del código fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se deberá efectuar después de recibir la autorización apropiada.

18.9 FUGA DE INFORMACIÓN

1. Explorar los medios y comunicaciones de salida para determinar la información oculta.
2. Garantizar que un tercero no pueda deducir, extraer información de las comunicaciones, sistemas de modulación o de enmascaramiento, a partir de un comportamiento específico.
3. Adquirir o desarrollar programas acreditados o productos ya evaluados.

4. Realizar un monitoreo regular de las actividades del personal y del sistema.
5. Realizar un monitoreo del uso de los recursos en los sistemas de computador y transmisión de datos por la red.
6. Restringir el envío de información a correos externos no institucionales.
7. Prevenir y restringir el acceso no autorizado a la red.
8. Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.

19 CIFRADO

Están enfocados a la protección de la información en el caso de que un intruso pueda tener acceso físico a la información, se impone establecer un sistema de cifrado de la misma, para dificultar la violación de su confidencialidad o su integridad.

19.1 INTEGRIDAD DEL MENSAJE

1. Cuando una aplicación tenga previsto el envío de mensajes que contengan información reservada o confidencial, se implementarán los controles criptográficos determinados.

19.2 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS.

1. Identificar el nivel requerido de protección de datos que se almacenará en el sistema, considerando: el tipo, fortaleza y calidad del algoritmo de cifrado (encriptación) requerido.
2. Utilizar controles criptográficos para la protección de claves de acceso a: sistemas, datos y servicios. Las claves deberán ser almacenadas de manera codificada, cifrada (encriptada) en la base de datos y/o en archivos de parámetros.
3. La UT propondrán la asignación de funciones: Implementación de la Política de Controles, Administración de claves: gestión de claves, incluyendo su generación.

19.3 GESTIÓN DE CLAVES

Protección de claves cifradas (criptográficas):

1. Implementar un sistema de administración de claves cifradas (criptográficas) para respaldar la utilización por parte de la institución, de los dos tipos de técnicas criptográficas: técnicas de clave secreta (criptografía simétrica) y técnicas de clave pública (criptografía asimétrica).
2. Proteger todas las claves contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.
3. Proporcionar una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.
4. Distribuir la primera clave a los usuarios, incluyendo la forma de activar y confirmar la recepción de la clave. Luego, a través de un correo electrónico recibirá un

acceso al sistema, el cual validará la entrega de la clave y la obligatoriedad de cambiar dicha clave.

5. Incorporar funcionalidad para cambiar o actualizar las claves, incluyendo reglas sobre cuándo cambiarlas, cómo hacerlo y la forma en que los usuarios autorizados tendrán acceso a ellas.
6. Incorporar funcionalidad para tratar las claves perdidas. Bajo pedido del usuario que pierde una clave se generará una nueva, la entrega será a través del procedimiento definido para la entrega de la primera clave.
7. Permitir revocar las claves, incluyendo la forma de retirarlas o desactivarlas cuando las claves se han puesto en peligro o cuando un usuario se retira de la institución.
8. Incorporar funcionalidad para recuperar claves pérdidas o corruptas como parte de la gestión de continuidad de los servicios informáticos.
9. Registrar y auditar las actividades relacionadas con la gestión de claves.

19.4 SE DEBE GARANTIZAR:

1. Confidencialidad: uso de cifrado (encriptación) de la información para proteger información sensible o crítica, bien sea almacenada o transmitida
2. Integridad / autenticidad: uso de firmas electrónicas o códigos de autenticación de mensajes para proteger la autenticidad e integridad de información sensible o crítica transmitida o almacenada.
3. No-repudio: uso de técnicas de cifrado (criptográficas) para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.
4. Utilizar certificados electrónicos de Entidad de Certificación de Información reconocidas por el Estado Ecuatoriano para la firma de cualquier tipo de documento, mensaje de dato, transacción que se procese electrónicamente o para comunicaciones entre sistemas, aplicaciones y medios físicos.
5. Utilizar los certificados electrónicos emitidos bajo estándares por las Entidades de Certificación de Información, las cuales deben ser instituciones u organizaciones reconocidas, con controles y procedimientos idóneos establecidos para proporcionar el grado requerido de confianza.
6. Uso de los certificados electrónicos según el ámbito para la cual fue generado.

20 SEGURIDAD FÍSICA Y AMBIENTAL

Se centra en la necesidad de identificar y establecer medidas de control físicas para proteger adecuadamente los activos de información, para evitar incidentes que afecten a la integridad física de la información, interferencias no deseadas o posibles contingencias externas.

20.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS

1. Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de estos sin

la autorización de la UT, en caso de requerir este servicio, deberá notificarlo al mismo departamento por escrito y con visto bueno de su jefe de Área, con copia al Departamento de Almacén.

2. El Departamento de Almacén será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada.
3. El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones asignadas en la Institución.
4. Proteger el equipamiento de procesamiento de información crítica de la Institución, ubicándolas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.
5. Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático de la Institución.
6. Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, estos deberán ser notificados por escrito, con una semana de anticipación a la UT.

20.2 CONTROLES DE ACCESO FÍSICO

Mecanismos y sistemas implementados para controlar el acceso de personas a las instalaciones de la organización, por ejemplo: barreras, cámaras, alarmas, biométricos.

1. La institución deberá destinar un área apropiada para alojar los equipos de telecomunicaciones y servidores.
2. Prevenir e impedir accesos no autorizados, daños e interferencias a las sedes, instalaciones e información de la ESPAM MFL.
3. Supervisar la permanencia de los visitantes en las áreas restringidas y registrar la hora y fecha de su ingreso y salida.
4. Los sistemas de comunicaciones y servidores deberán estar protegidos con una infraestructura adecuada que cumplan las normas y estándares actuales, con el fin de evitar que los usuarios tengan libre acceso físico al área.
5. Se restringirá el acceso a las áreas que contengan información valiosa para la ESPAM MFL y las salas donde se alojan los equipos de telecomunicaciones y servidores.
6. El acceso de terceras personas deberá ser identificado, controlado y registrado en la bitácora, detallando el nombre, empresa o departamento, motivo, fecha/hora de ingreso y salida de las áreas restringidas, por el personal de la UT.
7. El Coordinador de la UT es el que autoriza el ingreso de personas internas o externas de la ESPAM MFL, a las áreas restringidas y acompañadas por personal de la Unidad de Tecnología, mediante aprobación de la máxima Autoridad.
8. El personal de la UT, personal administrativo de otros departamentos y terceras personas, deberán portar su credencial institucional, al momento de ingresar a las áreas restringidas.

9. El departamento de Talento Humano informará a la UT, las personas que no tienen relación laboral con la ESPAM MFL, para proceder a revocar los permisos de acceso.
10. Se debe definir y autorizar el personal que tendrá acceso a las salas de telecomunicaciones y servidores, para mover, cambiar o extraer los equipos de estos sitios, mediante identificaciones y formularios de entrada/salida, notificando al departamento correspondiente y al personal de seguridad de la ESPAM MFL que se encuentra en la entrada y salida del campus.

20.3 PROTECCIÓN FÍSICA

1. Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
2. Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán controles de autenticación para autorizar y validar todos los accesos. Se mantendrá un registro protegido para permitir auditar todos los accesos.
3. Las puertas de acceso a la sala de servidores o Data Center deben ser de vidrio transparente, con el fin de facilitar el control de los equipos.
4. Revisar y actualizar semestralmente los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el responsable de la Unidad Organizativa de la que dependa.
5. La UT con todas sus áreas deberán contar con un plano actualizado de las instalaciones eléctricas y de comunicación.
6. La sala de servidores y telecomunicaciones se deben definir como áreas restringidas, las mismas que deben contar con un sistema de control de acceso del personal del UT, por ejemplo: sistema biométrico, tarjetas magnéticas, otros.
7. El Data Center debe recibir limpieza por lo menos una vez a la semana, para evitar la acumulación de polvo, el mismo que puede provocar ineficiencia o daños a equipos servidores y de telecomunicaciones.
8. La sala de servidores, telecomunicaciones y el cableado estructurado, deben estar diseñados bajo las normas y estándares actuales que ayuden a preservar la vida útil de los equipos que se alojan en los mismos.
9. Se deberán realizar mantenimientos cada tres meses a los sistemas de protección y eléctricos de las áreas restringidas.
10. Se deberán realizar inventarios y controles de los equipos servidores y de telecomunicaciones que encuentren distribuidos en los diferentes edificios de la ESPAM MFL.
11. Se deberá revisar y comprobar el voltaje de la toma eléctrica donde se requiera conectar un equipo de cómputo.

12. El personal autorizado de acceder al Data Center, deben controlar las condiciones ambientales como temperatura y humedad, para verificar que no afecte al funcionamiento del equipamiento.
13. Los equipos servidores y de telecomunicaciones (Data Center), deberán recibir mantenimiento físico por lo menos dos veces al año.

20.4 INSTALACIÓN DE EQUIPOS DE COMPUTO

La instalación del equipo de cómputo deberá seguir las siguientes acciones:

1. Los equipos de cómputo para uso interno se instalarán en lugares adecuados, lejos de polvo, luz solar y tráfico de personas.
2. Las instalaciones eléctricas y de comunicaciones, deben estar fijas o protegidas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.
3. Las instalaciones se apegarán estrictamente a los requerimientos de los equipos de cómputo, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
4. No se permitirán instalaciones improvisadas o sobrecargadas.
5. La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca la Unidad de Tecnología.

20.5 MANTENIMIENTO DE LOS EQUIPOS

1. Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
2. Ejecutar el plan de mantenimientos preventivo y correctivo de equipos de cómputo periódicos a los equipos y dispositivos, de acuerdo con las especificaciones y recomendaciones del proveedor.
3. Realizar el mantenimiento de los equipos únicamente con personal calificado y autorizado por la UT.
4. Conservar los registros de los mantenimientos preventivos, correctivos y fallas relevantes o sospechosas.
5. Establecer controles apropiados para realizar mantenimientos programados y emergentes.
6. Gestionar mantenimientos planificados con hora de inicio, fin, impacto y responsables y poner previamente en conocimiento de administradores y usuarios finales.
7. Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

20.6 SEGURIDAD DEL CABLEADO

1. Proteger el cableado de la red contra la interceptación o daño.

2. Separar los cables de energía de los cables de comunicaciones.
3. Identificar y rotular los cables de acuerdo con las normas locales o internacionales para evitar errores en el manejo.
4. Disponer de documentación, diseños/planos y la distribución de conexiones de: datos alámbricos/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc.
5. Controlar el acceso a los módulos de cableado de conexión (patch panel) y cuartos de cableado.
6. Proteger el tendido del cableado troncal (backbone).

20.7 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

1. Custodiar los equipos y medios que se encuentren fuera de las instalaciones de la institución. Tomar en cuenta las instrucciones del fabricante para la protección de los equipos que se encuentran fuera de estas instalaciones.
2. Firmar acta de compromiso, de esta manera, el custodio del equipo de cómputo tiene la responsabilidad del cuidado de este y/o pérdida de información, mientras el equipo esté fuera de la institución.

20.8 SUSTRACCIÓN O PÉRDIDAS DE EQUIPOS DE CÓMPUTO

1. La UT llevará un inventario físico para control interno del departamento, que se lo realizará junto con el Plan de Mantenimiento Preventivo – Correctivo.
2. La UT al asignar equipos de cómputo lo realizará mediante "Acta de Entrega/Recepción", que quedará como evidencia óptica de la aceptación de responsabilidad sobre el equipo por parte del usuario.
3. El equipo de cómputo quedará bajo el custodio del área o persona que lo usa, el mismo que será responsable de proteger el bien.
4. El Área de Redes y Telecomunicaciones y el Data Center, así como las áreas que cuenten con equipos de misión crítica deberán contar con un sistema de vigilancia de control de acceso mediante cámaras o equipo biométrico, que ayude a obtener evidencia de accesos físicos a las instalaciones e identificar los responsables de la desaparición de los equipos.
5. El Usuario es el responsable por la pérdida o destrucción del equipo de cómputo, por mal uso de este, salvo el caso que sea por causas naturales, así mismo, será responsable terceras personas que tengan acceso al equipo que realicen actividades de mantenimiento o reparación.
6. El Usuario es el responsable del equipo de cómputo y sus accesorios, deberá notificar por escrito al jefe inmediato y a la máxima autoridad de la ESPAM MFL, sobre el extravío, robo o desaparición de este, actuando de acuerdo con el Art. 77 del Reglamento General para la Administración, Utilización, Manejo y Control de los bienes y existencias del sector público.
7. El equipo de cómputo asignado al usuario, en el caso de extraviarse o sufrir daños por el uso, será de responsabilidad del departamento o del usuario administrativo/docente; es decir, quien esté a cargo del mismo deberá restituir o

reemplazar el equipo por otro, de acuerdo a lo mencionado en el Art.77 del Reglamento General para la Administración, Utilización, Manejo y Control de los bienes y existencias del sector público.

20.9 SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACIÓN DE LOS EQUIPOS

1. Destruir, borrar o sobrescribir los dispositivos que contienen información sensible utilizando técnicas que permitan la no recuperación de la información original.
2. Evaluar los dispositivos deteriorados que contengan información sensible antes de enviar a reparación, borrar la información o determinar si se debería eliminar físicamente el dispositivo.

20.10 EQUIPO DE USUARIO DESATENDIDO

1. Implementar medidas para que, en un determinado tiempo, de acuerdo con la información crítica que maneje, si el usuario no está realizando ningún trabajo en el equipo, este se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave.
2. Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
3. Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

21 SEGURIDAD EN LA OPERATIVIDAD

Se trata de asegurar la operación correcta y segura de las instalaciones de procesamiento de información.

21.1 GESTIÓN DE CAMBIOS

1. Evaluar el impacto de dichos cambios.
2. Aprobar de manera formal los cambios propuestos.
3. Planificar el proceso de cambio.
4. Realizar pruebas del cambio.
5. Comunicar el detalle de cambios a todas las personas involucradas.
6. Identificar responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de estos.
7. Establecer responsables y procedimientos formales del control de cambios en los equipos y software. Los cambios deben efectuarse únicamente cuando haya razón válida para el negocio, como: cambio de versión, corrección de vulnerabilidades, costos, licenciamiento, nuevo hardware, etc.

21.2 SEPARACIÓN DE LAS INSTANCIAS DE DESARROLLO, PRUEBAS, CAPACITACIÓN Y PRODUCCIÓN

1. Definir y documentar diferentes entornos para desarrollo, pruebas, capacitación y producción. Para el caso que no se pueda definir diferentes entornos con recursos físicos independientes, se debe mantener diferentes directorios con su respectiva versión y delegación de acceso.
2. Aislar los ambientes de desarrollo, pruebas, capacitación y producción.
3. Controlar la instalación y uso de herramientas de desarrollo de software y/o acceso a bases de datos y redes en los equipos informáticos, salvo que sean parte de las herramientas de uso estándar o su instalación sea autorizada de acuerdo a un procedimiento expresamente definido.
4. Implantar ambientes de prueba, iguales en capacidad, a los ambientes de producción.
5. Utilizar sistemas de autenticación y autorización independientes para las diversas instancias o ambientes.
6. Definir perfiles de usuario para las diferentes instancias o ambientes.
7. Aislar los datos sensibles de los ambientes de desarrollo, pruebas y capacitación.
8. Permitir al personal de desarrollo de software el acceso al entorno de producción, únicamente en caso de extrema necesidad, con la autorización explícita correspondiente.
9. Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

21.3 CONTROLES CONTRA CÓDIGO MALICIOSO

1. Prohibir el uso de software no autorizado por la institución. Elaborar un listado del software autorizado.
2. Establecer procedimientos para evitar riesgos en la obtención/descarga de archivos y software desde o a través de redes externas o por cualquier otro medio.
3. Instalar y actualizar periódicamente software de antivirus y contra código malicioso.
4. Mantener los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles.
5. Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la institución.
6. Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos o en archivos recibidos a través de redes no confiables.
7. Redactar procedimientos para verificar toda la información relativa a software malicioso.
8. Emitir boletines informativos de alerta con información precisa.
9. Concienciar al personal acerca del problema de los virus y cómo proceder frente a los mismos.

10. Contratar con el proveedor de Internet o del canal de datos los servicios de filtrado de: virus, spam, programas maliciosos, en el perímetro externo.
11. No abrir los archivos o ejecutar programas adjuntos a mensajes de correo electrónico sin verificar primero con un programa de detección de virus.
12. No utilizar formatos ejecutables en los archivos comprimidos, dado que este formato facilita la propagación del virus.
13. Usar software licenciado para su uso por la organización, de acuerdo con las disposiciones específicas establecidas en el contrato.

21.4 RESPALDO DE LA INFORMACIÓN

La UT generará y gestionará los respaldos de los activos de información críticos, así como de la información crítica institucional de los diferentes departamentos Académicos y Administrativos de la ESPAM MFL.

1. Los responsables de la UT junto con el propietario de la información determinarán los procedimientos para el resguardo y contención de la información.
2. Es responsabilidad de cada miembro de la comunidad politécnica realizar respaldos de la información que genera, inherente a las actividades institucionales.
3. La UT deberá generar y podrá actualizar el procedimiento para "Generar y Gestionar los respaldos de los activos de información críticos e información crítica institucional".
4. Definir el procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención.
5. Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo con los requisitos del negocio de la institución.
6. Establecer procedimientos de los medios de respaldo, una vez concluida su vida útil recomendada por el proveedor y la destrucción de estos medios.
7. Proporcionar un grado apropiado de protección física y ambiental.
8. Se deben realizar respaldos periódicamente de la información importante y relevante, contenida en la base de datos que generan los sistemas de información institucional.
9. Establecer procedimientos regulares de verificación y restauración de los medios de respaldo para garantizar sean confiables para uso de emergencia.
10. Considerar los respaldos a discos y en el mismo sitio si se tiene suficientes recursos, ya que, en caso de mantenimientos de los sistemas de información, es más rápida su recuperación.
11. Los usuarios deberán proteger y cuidar los medios o unidades de almacenamiento (CD´s o DVD´s, Tarjetas de Memoria, Pen drives, otros) que estén bajo su responsabilidad y que contengan información confidencial e importante.
12. Proteger la información confidencial por medio de encriptación.
13. Los usuarios podrán solicitar asesoría o capacitación a la UT en el procedimiento para respaldar la información.

14. Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y salvaguardar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

21.5 REGISTRO DE EVENTOS

Los sistemas de información generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir:

1. Identificación del usuario.
2. Fecha y hora de inicio y terminación.
3. Identidad o ubicación de la terminal, si se hubiera dispuesto identificación automática para la misma.
4. Registros de intentos exitosos y fallidos de acceso al sistema.
5. Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

21.6 CONTROL DE LAS VULNERABILIDADES TÉCNICAS

1. Disponer de un inventario completo y actual de los activos de software. El inventario servirá para dar soporte a la gestión de la vulnerabilidad técnica e incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue y las personas de la institución responsables del software.
2. Identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y mantener la concienciación sobre ellas para el software y otras tecnologías, con base en la lista de inventario de activos.
3. Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente.
4. Definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes.
5. Identificar los riesgos asociados a una vulnerabilidad potencial y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y/o la aplicación de otros controles.
6. Evaluar los riesgos asociados con la instalación de un parche para cubrir vulnerabilidades. Los riesgos impuestos por la vulnerabilidad se deberán comparar con los riesgos de instalar el parche.
7. Apagar los servicios o capacidades relacionadas con la vulnerabilidad.
8. Adaptar o agregar controles de acceso; por ejemplo, cortafuegos (firewalls), en las fronteras de la red.
9. Aumentar el monitoreo para detectar o prevenir los ataques reales.

10. Resolver y restaurar el servicio afectado por el incidente debido a la par de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes.
11. Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto.
12. Monitorear y evaluar a intervalos regulares las vulnerabilidades técnicas, para garantizar eficacia y eficiencia.

22 SEGURIDAD EN LAS TELECOMUNICACIONES

El intercambio de información se realiza a través de redes de telecomunicaciones, por tal motivo, corresponderá establecer los controles adecuados para proteger tanto las comunicaciones externas a la organización como las que viajan a través de las redes de la propia organización.

22.1 CONTROLES DE LAS REDES

1. Se realizará el monitoreo de la red inalámbrica mediante análisis de tráfico, detectando usos indebidos del servicio y así mantener en buen funcionamiento la red.
2. Se bloqueará páginas web de redes sociales, entretenimiento u otras, para evitar el consumo excesivo de ancho de banda del internet.
3. Se dará mantenimiento a los equipos y puntos de acceso a la red inalámbrica.
4. Separar el área de redes del área de operaciones, cuando la capacidad y recursos lo permitan.
5. Designar procedimientos y responsabilidades para la gestión de equipos remotos como el caso de redireccionamiento de puertos y accesos por VPNs, incluyendo el área de operaciones y el área de usuarios finales.
6. Establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por las redes públicas, redes locales e inalámbricas; así como la disponibilidad de las redes.
7. Garantizar la aplicación de los controles mediante actividades de supervisión.
8. Disponer de un esquema de red de los enlaces de datos, Internet y redes locales, así como la documentación respectiva.

22.1.1 CONTROL DEL ENRUTAMIENTO EN LA RED

1. Configurar políticas de control de acceso para el enrutamiento en la red, basándose en los requerimientos de la institución.
2. Las puertas de enlace de la seguridad (gateway) se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes internas y externas, si se emplean tecnologías proxy y/o de traducción de direcciones de red.

3. Las instituciones que utilizan proxys y quienes definen las listas de control de acceso (LCA), deben estar conscientes de los riesgos en los mecanismos empleados, a fin de que no existan usuarios o grupos de usuarios con salida libre y sin control, en base a las políticas de la institución.

22.1.2 LIMITACIÓN DEL TIEMPO DE CONEXIÓN

1. Utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.
2. Configurar espacios de tiempo predeterminados para procesos especiales (transmisiones de datos o archivos, obtención de respaldos, mantenimientos programados, entre otros.)
3. Restringir los tiempos de conexión a las horas normales de oficina, si no se requiere tiempo extra u operaciones de horario prolongado.
4. Requerir la autenticación a intervalos determinados cuando lo amerite.
5. Proporcionar accesos temporales para ciertas operaciones (mediante tickets o tokens electrónicos temporales)

22.2 MECANISMO DE SEGURIDAD ASOCIADOS A SERVICIOS EN RED

1. Incorporar tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red.
2. Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, etc.
3. Definir procedimientos para la utilización de los servicios de red para restringir el acceso a los servicios de red cuando sea necesario.
4. Instalar periódicamente las actualizaciones de seguridad.

22.3 SEGREGACIÓN DE LAS REDES

1. Realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentren los activos críticos para la institución.
2. Dividir las redes en dominios lógicos de red, dominios de red interna, dominios de red externa e inalámbrica.
3. Documentar la segregación de red, identificando las direcciones IP que se encuentran en cada segmento de red.
4. Configurar la puerta de enlace (gateway) para filtrar el tráfico entre dominios y bloquear el acceso no autorizado.
5. Controlar los flujos de datos de red usando las capacidades de enrutamiento/conmutación (listas de control de acceso).
6. La separación de las redes debe ejecutarse en base a la clasificación de la información almacenada o procesada en la red, considerando que el objetivo es dar mayor protección a los activos de información críticos en función del riesgo que éstos podrían presentar.

7. Separar redes inalámbricas procedentes de redes internas y privadas, para evitar el acceso a terceros y de usuarios externos a las redes privadas internas.

23 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Se trata de garantizar la integridad de la seguridad de la información en los sistemas.

23.1 ANÁLISIS Y ESPECIFICACIONES DE LOS REQUERIMIENTOS DE SEGURIDAD

1. Debemos incluir requisitos para la seguridad de la información en la fase de especificación de condiciones para sistemas de información.
2. Definir los controles apropiados, tanto automatizados como manuales. En esta definición deben participar personal del requerimiento funcional y personal técnico que trabajarán en el sistema.
3. Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que estos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas por falla o falta de seguridad.
4. Si se adquieren productos, los contratos con el proveedor deben contemplar los requisitos de la seguridad identificados.

23.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS

1. Verificar que los cambios sean propuestos por usuarios autorizados y se respete los términos y condiciones que surjan de la licencia de uso, en caso de existir.
2. Elaborar el informe de paso de pruebas a producción, que deberá contener el detalle de los cambios y acciones a ejecutar, tanto de software, bases de datos y hardware.

23.3 SEGURIDAD EN ENTORNOS DE DESARROLLO

1. Incorporar controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.
2. Utilizar controles de sesión en los sistemas.
3. Utilizar funciones de agregar, modificar y borrar para implementar los cambios en los datos. El borrado a través de los sistemas será siempre un borrado lógico de los datos.
4. Crear registros de auditoría, al insertar y actualizar datos; y, si se requiere según el sistema, se mantendrá el registro (logs) de consultas de datos.
5. Crear el procedimiento y/o herramientas para la revisión periódica de los registros de auditoría para detectar cualquier anomalía en la ejecución de las transacciones.
6. Identificar, crear y utilizar programas para la recuperación de datos después de fallas, con el fin de garantizar el procesamiento correcto de los datos.

7. Utilizar controles para mantener integridad de registros y archivos.
8. Utilizar controles para protección contra ataques por desbordamiento/exceso en el buffer.
9. Definir y ejecutar periódicamente, procedimientos de recuperación de sistemas, que verifiquen la ejecución de los sistemas en caso de una falla o desastre, esto estará a cargo del administrador técnico de la aplicación o sistema.
10. Definir y aplicar procesos de control de cambios para la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

23.4 CONTROL DEL SOFTWARE OPERATIVO

1. Asignar un responsable de la implantación de cambios por sistema, quien tendrá como funciones principales:
    - Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
    - Se debe asegurar que los aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo con las normas y procedimientos vigentes.
2. Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del área encargada del testeo y del usuario final.
3. Rechazar la implementación en caso de encontrar defectos
4. Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones para el paso a producción, el informe de pruebas previas y el informe de paso a producción.
5. Disponer del informe de paso a producción, el cual contendrá información de todos los cambios a realizar y el plan de contingencia.
6. Guardar o instalar únicamente los ejecutables y cualquier elemento necesario para la ejecución de un software en el ambiente de producción.
7. Llevar un registro de auditoría de las actualizaciones realizadas.
8. Retener las versiones previas del sistema, como medida de contingencia.
9. Denegar permisos de modificación a los desarrolladores, sobre los programas fuentes bajo su custodia.
10. Entregar acceso físico o lógico al ambiente producción únicamente para propósitos de soporte, cuando sea necesario y con aprobación del responsable del área de Tecnologías de la Información, esto se realizará tanto para usuarios internos de la dirección como para proveedores.

23.5 REVISIÓN TÉCNICA DE LAS APLICACIONES DESPUÉS DE LOS CAMBIOS EN EL SISTEMA OPERATIVO

1. Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
2. Probar que los cambios realizados retornen la funcionalidad esperada.

3. Realizar las pruebas inmediatamente después de realizar el cambio y durante la ventana de mantenimiento definida para el cambio.
4. Identificar si existen problemas con los cambios, para aplicar el plan de contingencia o realizar el retorno al estado anterior al cambio.

23.6 RESTRICCIÓN DEL CAMBIO DE PAQUETES DE SOFTWARE

1. Disponer de la autorización del responsable del área de Tecnologías de la Información que apruebe el cambio
2. Analizar los términos y condiciones de la licencia, si es del caso, a fin de determinar si las modificaciones se encuentran autorizadas.
3. Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.
4. Conservar el software original que se va a cambiar y los cambios se deberán aplicar a una copia claramente identificada
5. Probar y documentar en su totalidad todos los cambios, de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software.

23.7 EXTERNALIZACIÓN DEL DESARROLLO DE SOFTWARE

1. Definir acuerdos de licencias, acuerdos de uso, propiedad de código y derechos conferidos.
2. Definir los requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
3. Verificar el cumplimiento de las condiciones de seguridad requeridas.
4. Definir acuerdos de custodia de las fuentes del software o convenios de fideicomiso (y cualquier otra información requerida) en caso de quiebra de la tercera parte.
5. Realizar pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

23.8 ACEPTACIÓN DEL SISTEMA

1. Considerar procedimientos de recuperación y planes de contingencia.
2. Se debe asegurar que la instalación del nuevo sistema no afecte negativamente los sistemas existentes, especialmente en períodos pico de procesamiento.
3. Considerar el efecto que tiene el nuevo sistema en la seguridad global de la institución.
4. Capacitar sobre el funcionamiento y utilización del nuevo sistema.
5. Para nuevos desarrollos, se debe involucrar a los usuarios y a todas las áreas relacionadas, en todas las fases del proceso, para garantizar la eficacia operativa del sistema propuesto.

23.9 PROTECCIÓN DE LOS DATOS DE PRUEBA DEL SISTEMA

1. Identificar por cada sistema, los datos que pueden ser copiados de un ambiente de producción a un ambiente de pruebas.
2. Efectuar pruebas de los sistemas en el ambiente de pruebas, sobre datos extraídos del ambiente de producción.
3. Solicitar autorización formal para realizar una copia de la base de datos de producción como base de datos de prueba.
4. Identificar los datos críticos que deberán ser modificados o eliminados del ambiente de pruebas.
5. Aplicar los mismos procedimientos de control de acceso que existen en la base de producción.
6. Registrar la copia y la utilización de la información para futuras auditorías.
7. Controlar que la modificación, actualización o eliminación de los datos operativos (de producción) serán realizados a través de los sistemas que procesan esos datos, y de acuerdo con el esquema de control de accesos implementado en los mismos.
8. Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo. En el caso de que esta función no pueda ser separada del área de Desarrollo, se aplicarán controles adicionales de acuerdo con la separación de funciones.

24 RELACIONES CON PROVEEDORES

En caso de que empresas o personal externo a la organización tengan acceso a los sistemas de información o a los recursos que manejan activos de información, se deberá establecer, de modo formal, las condiciones para el uso de dichos activos y supervisar el cumplimiento de dichas condiciones

24.1 MONITOREO Y REVISIÓN DE LOS SERVICIOS, POR TERCEROS

1. Identificar los sistemas sensibles o críticos que convenga tener dentro o fuera de la institución.
2. Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos.
3. Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionadas con el servicio prestado.

24.2 GESTIÓN DE LOS CAMBIOS EN LOS SERVICIOS OFRECIDOS POR TERCEROS

1. Establecer un proceso de gestión de cambios en los servicios ofrecidos por terceros, en el desarrollo de aplicaciones, provisión de servicios de hardware, software, redes, otros.

2. Coordinar el proceso de cambio cuando se necesita realizar cambios o mejoras a las redes y uso de nuevas tecnologías en los servicios ofrecidos por terceros.
3. Coordinar el proceso de cambio cuando se realice cambio de proveedores, cambio de ubicación física en los servicios ofrecidos por terceros.

25 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Se persigue garantizar que los registros de incidencias y las debilidades en la seguridad de la información y de sus sistemas, se comuniquen de manera pertinente, como medio que posibilite la debida corrección.

1. Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, previstos en el apartado de amenazas y vulnerabilidades de este documento.
2. Comunicar los incidentes a través del responsable de la Unidad Organizativa tan pronto como sea posible
3. Registrar pistas de auditoría y evidencia similar para:
   a. Análisis de problemas internos.
   b. Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial.
   c. Negociación de compensaciones por parte de los proveedores de software y de servicios.
4. Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
   a. Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
   b. Documentación de todas las acciones de emergencia emprendidas en forma detallada.
   c. Comunicación de las acciones de emergencia al titular de la Unidad Organizativa y revisión de su cumplimiento.
   d. Constatación de la integridad de los controles y sistemas de la UNC en un plazo mínimo.

25.1 RESPONSABILIDADES Y PROCEDIMIENTOS

1. Identificar y clasificar los diferentes tipos de incidentes de seguridad de la información.
2. Identificar y analizar las posibles causas de un incidente producido.
3. Planificar e implementar acciones correctivas para evitar la recurrencia del incidente.
4. Notificar a todos los funcionarios afectados por el incidente de la restauración del equipo, sistema o servicio afectado, una vez esté solucionado el incidente.
5. Recolectar y asegurar pistas de auditoría y toda la evidencia relacionada con el incidente.

6. Determinar el costo promedio por incidente.
7. Determinar el número de incidentes recurrentes.
8. Determinar la frecuencia de un incidente recurrente.

25.2 REPORTE SOBRE LAS DEBILIDADES EN LA SEGURIDAD

1. Notificar a su Coordinador inmediato y este a la Unidad de Tecnología de la debilidad o vulnerabilidad detectada.
2. Registrar la fecha, hora, apellidos y nombres del funcionario que detectó la debilidad o vulnerabilidad, descripción de la debilidad, descripción de posibles incidentes de seguridad que pudieran ocurrir producto de esta debilidad. El responsable de llevar este reporte denominado "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es la Unidad de Tecnología.
3. La Unidad de Tecnología deberá tomar las medidas pertinentes para prevenir o eliminar la vulnerabilidad o debilidad detectada.

25.3 RECOLECCIÓN DE EVIDENCIAS

1. Desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la institución.
2. Hay que asegurar que los sistemas de información cumplan con las normas legales para la producción de evidencia, para lograr la admisibilidad, calidad y cabalidad de esta.
3. Se debe proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debe estar supervisado por personal de confianza y se debe registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué Herramientas o programas se utilizaron.

26 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La organización debe saber responder a una interrupción en sus actividades, proteger sus procesos críticos y garantizar una pronta reanudación de sus funciones.

26.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
2. Identificar los activos involucrados en los procesos críticos de los servicios informáticos, así como de las actividades que se deben realizar.
3. Garantizar la continuidad incorporando los procesos generados en la estructura de la institución.

4. Documentar el proceso de respaldo y restauración de la información.
5. Documentar todos los procesos de los servicios de procesamiento de datos, incluyendo la interrelación con otros sistemas.
6. Documentar los contactos de soporte, necesarios en caso de incidentes.
7. Documentar los procedimientos para reinicio y recuperación del sistema en caso de fallas.
8. Documentar los registros de auditoría y de la información de registro del sistema.

26.2 CONTINUIDAD DEL NEGOCIO Y EVALUACIÓN DE RIESGOS

1. Definir los procesos y actividades de los servicios y aplicaciones
2. Entender las complejidades e interrelaciones existentes entre equipamiento, personas, tareas, departamentos, mecanismos de comunicación y relaciones con proveedores externos, los cuales pueden prestar servicios críticos que deben ser considerados.
3. Identificar y valorar el impacto de las interrupciones de los procesos, aplicaciones y servicios de los servicios informáticos, para cuantificar y calificar los impactos y saber sus efectos.
4. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información.
5. Logística: responsable de reunir todos los medios para ayudar a la puesta en operación de las actividades.
6. Recuperación: puesta en servicio de la infraestructura.
7. Desarrollar los procedimientos indicando el objetivo y el alcance, considerando las actividades y los tiempos de recuperación.
8. Difundir y capacitar al personal responsable en los conceptos que contemplan la continuidad de los servicios informáticos.
9. Seleccionar los sitios alternos y de almacenamiento externo.
10. Duplicado de los registros tanto físicos como electrónicos
11. Incorporar RAID en los discos de los servidores
12. Contratos de mantenimiento preventivo y correctivo.
13. Estrategia adecuada de respaldos
14. Seguros para los activos

27 CUMPLIMIENTO

Este apartado refiere a la necesidad del cumplimiento del marco normativo y de todo requisito de seguridad que en él esté implícito. La organización optimizará su efectividad a través del recurso de una auditoría sobre las infraestructuras y las aplicaciones.

27.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE

1. Organizar e inventariar todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para cada programa de software, servicio informático y en general todo activo de información que utiliza la institución.
2. Considerar las normas y leyes más generales relacionadas a la gestión de los datos e información electrónica en el gobierno. A saber:
3. Constitución de la República del Ecuador
4. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
5. Ley Orgánica de Transparencia y Acceso a la Información Pública
6. Ley del Sistema Nacional de Registro de Datos Públicos
7. Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva
8. Ley Orgánica y Normas de Control de la Contraloría General del Estado
9. Decreto Ejecutivo No. 1014 uso de Software Libre en la Administración Pública.
10. Decreto Ejecutivo No. 1384 sobre Interoperabilidad Gubernamental en la Administración Pública.

27.2 DERECHOS DE PROPIEDAD INTELECTUAL

1. Adquirir software únicamente a proveedores reconocidos para garantizar que no se violen derechos de propiedad intelectual. Si el Software es Libre Opensource se considerará los términos de las licencias públicas generales.
2. Implementar mecanismos para concienciar sobre las políticas para proteger derechos de propiedad intelectual y las acciones disciplinarias para el personal que las viole. Se aplica al software libre como al privativo.
3. Mantener registros apropiados de los activos de información para proteger los derechos de propiedad intelectual. Se aplica al software libre como al privativo.
4. Custodiar evidencia de la propiedad de licencias o suscripciones, contratos, discos maestros, manuales y toda la información relevante del software que se utiliza.
5. Controlar y asegurar que no se exceda el número máximo de usuarios permitidos para un programa de software. Se aplica al software libre como al privativo, donde corresponda.
6. Cumplir los términos y condiciones de uso para el software y la información, obtenidos de la Internet o proveedores.
7. Controlar que no se duplique, convierta en otro formato, ni extraiga contenidos de grabaciones de audio y video, si no está expresamente permitido por su autor o la persona que tenga los derechos sobre el material.
8. Controlar que no se copie total ni parcial software privativo, códigos fuente y la documentación de programas de software con derechos de propiedad intelectual. Excepto los programas de software libre con términos de sus licencias públicas.
9. Exigir a los funcionarios que utilicen solo software desarrollado, provisto o aprobado por la institución.

10. Definir y aplicar una licencia pública general al software desarrollado por la institución o contratado a terceros como desarrollo, para proteger la propiedad intelectual.

27.3 PROTECCIÓN DE REGISTROS DE LA ORGANIZACIÓN

1. Clasificar los registros electrónicos y físicos por tipos, especificando los periodos de retención y los medios de almacenamiento, como discos, cintas, entre otros.
2. Mantener la documentación y especificaciones técnicas de los algoritmos y programas utilizados para el cifrado y descifrado de archivos y toda la información relevante relacionada con claves, archivos criptográficos o firmas electrónicas, para permitir el descifrado de los registros durante el periodo de tiempo para el cual se retienen.
3. Establecer un procedimiento para revisar el nivel de deterioro de los medios utilizados para almacenar los registros. Los procedimientos de almacenamiento y manipulación se deberán implementar según las recomendaciones del fabricante.
4. Establecer un procedimiento para garantizar el acceso a los datos e información registrada, tanto el medio como el formato, durante todo el periodo de retención.
5. Establecer un procedimiento para cambiar o actualizar la tecnología del medio en el cual se almacenan los activos de información y registros de acuerdo con las innovaciones tecnológicas disponibles en el mercado.
6. Los sistemas de almacenamiento de datos se deberán seleccionar de manera que los datos requeridos se puedan recuperar en el periodo de tiempo y en formatos legibles, dependiendo de los requisitos que se deben cumplir.

27.4 PROTECCIÓN DE LOS DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL

La Unidad de Tecnología deberá controlar la aplicación de la política de protección de datos y privacidad de la información personal.

27.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS

1. Restringir importaciones y/o exportaciones de hardware y software de computadores para la ejecución de funciones criptográficas; o diseñados para adicionarles funciones criptográficas.
2. Restringir el uso de encriptación, y especificar y documentar los ámbitos en dónde se aplicarán tales procesos (ej., comunicaciones, firma de documentos, trasmisión de datos, entre otros).
3. Restringir métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información encriptada mediante hardware o software para brindar confidencialidad al contenido.
4. Garantizar el cumplimiento con las leyes y los reglamentos nacionales antes de desplazar información encriptadas o controles criptográficos a otros países.

27.6 COMPROBACIÓN DEL CUMPLIMIENTO TÉCNICO

1. Verificar el cumplimiento técnico bien sea manualmente (con soporte de las herramientas de software apropiadas, si es necesario) por un ingeniero de sistemas con experiencia, y/o con la ayuda de herramientas automáticas que generen un informe técnico para la interpretación posterior por parte del especialista técnico.
2. Analizar los sistemas operativos para asegurar que los controles de hardware y software se han implementado correctamente. Este tipo de verificación del cumplimiento requiere experiencia técnica especializada.
3. Ejecutar o contratar pruebas de penetración y evaluaciones de la vulnerabilidad, las cuales pueden ser realizadas por expertos independientes especialmente contratados para este propósito. Ello puede ser útil para detectar vulnerabilidades en el sistema y verificar qué tan efectivos son los controles evitando el acceso no autorizado debido a estas vulnerabilidades. Las pruebas de penetración y las evaluaciones de vulnerabilidad no deben sustituir las evaluaciones de riesgos.

28 REGISTROS

FORMATO	NOMBRE	LOCALIZACIÓN	RESPONSABLE	DISPOSICIÓN
DIGITAL (PDF)	Reglamento de Aseguramiento de la Información V02	http://www.espam.edu.ec/web/informativo/reglamentacion.aspx	Unidad de Tecnología	Público
FISICO (FOLLETO)	Reglamento de Aseguramiento de la Información V02	• Secretaría General • Unidad de Tecnología	• Secretaría General • Unidad de Tecnología	Público

29 CONTROL DE CAMBIOS.

Tipo de documento:	Reglamento	Código:	RAI-UT-V02
Título del documento:	REGLAMENTO DE ASEGURAMIENTO DE LA INFORMACIÓN		
Colaboradores:	Ing. Andrés Zambrano, Ing. Juan Muñoz, Ing. Julio Molina, Ing. Marón Vera, Ing. Míriam Lectong, Mgtr. César Moreira, Mgtr. Jéssica Vélez, Mgtr. Néstor Mora, Mgtr. Javier Intriago y Mgtr. Patricio Zambrano		
Elaborado por: Firmado electrónicamente por: ROBERTO CARLOS ORMAZA MEDINA Ing. Roberto Ormaza Medina	Revisado por: Firmado electrónicamente por: ANGEL GEOVANNY GARCIA MONTES Lic. Geovanny García Montes	Aprobado por: Firmado electrónicamente por: MIRYAM ELIZABETH FELIX LOPEZ Dra. C. Miryam Félix López	

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
V02	19/10/2023	Segunda Versión: Bajo lineamientos en la NORMA ISO/IEC 27001

CERTIFICO: Que el presente Reglamento de Aseguramiento de la Información (basado en la norma ISO 27001), fue conocido y aprobado en primera instancia a través de Resolución RHCP-SO-02-2023-N°046, de fecha 03 de marzo de 2023; y, aprobado en segundo y definitivo debate a través de Resolución RHCP-SE-18-2023-Nº005, de fecha 19 de octubre de 2023, en la Décimo Octava Sesión Extraordinaria del Honorable Consejo Politécnico de la ESPAM MFL.

Firmado electrónicamente por:
JULIO CESAR ORMAZA SUAREZ

Ab. Julio César Ormaza Suárez
SECRETARIO GENERAL