ÍNDICE DE CONTENIDO

Pag.

POLÍTICAS DE GESTIÓN DE RIESGOS

POLÍTICAS DE GESTIÓN DE RIESGOS

1. OBJETIVOS

Identificar y minimizar la probabilidad de materialización de los riesgos que puedan afectar a los procesos críticos de la Escuela Militar de Ingeniería, soportados por el ambiente tecnológico.

Identificar y minimizar la probabilidad de materialización de riesgos que puedan afectar a los proyectos críticos.

2. NIVELES DE RESPONSABILIDAD

ROL O CARGO DEL RESPONSABLE	NIVEL DE RESPONSABILIDAD O FUNCIONES
Comité de Seguridad de la EMI.	• Aprobar esta política y otorgar lineamientos y criterios generales para la gestión de riesgos. • Aprobar acciones y planes de mitigación de riesgos críticos que puedan afectar a los procesos de Gestión Académica y Gestión Financiera.
Director Nacional de Informática.	• Revisar periódicamente el mapa de riesgos de tecnología que puedan afectar a los procesos críticos de la Escuela Militar de Ingeniería: Proceso de Gestión Académica y Proceso de Gestión Financiera. • Gestionar y dar seguimiento a la implementación de controles para mitigar los riesgos tecnológicos. • Definir los plazos de mitigación de cada riesgo y un responsable, basado en las sugerencias del CSIRT-EMI
Jefes de Departamento y/o Sección	• Ejecutar los planes de acción para mitigar los riesgos identificados.
CSIRT – EMI	• Administrar el universo de riesgos tecnológicos u operativos que pueden afectar a los procesos críticos de la Escuela Militar de Ingenieria. • Recomendar y asesorar a la Dirección Nacional de Informática y al Comité de Seguridad en la toma de decisiones o definición de directrices para mitigar riesgos críticos. • Presentar un informe periódico sobre la exposición de riesgo tecnológico. • Mantener informado de manera ejecutiva al Comité de Seguridad sobre riesgos importantes y sus métodos de mitigación.

3. DESCRIPCIÓN DE LA POLÍTICA

3.1 NORMAS Y DISPOSICIONES GENERALES

- ✓ Todos los miembros de la Dirección Nacional de Informática debe informar al CSIRT-EMI. la existencia de debilidades o amenazas que puedan afectar a los intereses de la Escuela Militar de Ingeniería.

- ✓ El CSIRT-EMI. tiene la obligación de detectar y sugerir controles para mitigar los riesgos identificados basándose en un plan de acción aprobado por la Dirección Nacional de Informática.

- ✓ En caso de existir riesgos críticos o que afecten significativamente a los procesos de Gestión Académica y/o Gestión Administrativa, el plan de acción debe aprobarlo el Comité de Seguridad.

- ✓ Los riesgos críticos que serán informados al Comité de Seguridad, deben presentar indicadores como costo, valor y retorno de inversión, con la finalidad de facilitar a los niveles directivos la toma de decisiones.

- ✓ En el Anexo A se detallan las escalas de: a) Probabilidad de ocurrencia de un riesgo; y, b) Impacto en caso de materialización del riego.

- ✓ No se definirá cuantitativamente el apetito de riesgo en términos económicos. Los límites de apetito de riesgo dependerán de cada proyecto y deberán ser mitigados todos aquellos riesgos que afecten a la operación Institucional y/o al cumplimiento de los objetivos principales de un proyecto.

- ✓ Cualquier lineamiento general o cambio en la priorización de mitigación de riesgo debe ser aprobada por el Comité de Seguridad.

ANEXO A: ESCALAS DE IMPACTO Y PROBABILIDAD RIESGOS INSTITUCIONALES

	Muy bajo	Bajo	Moderado	Alto	Muy alto
IMPACTO	**0,05**	**0,1**	**0,2**	**0,4**	**0,8**
Cualitativo	Pérdida o daño insignificante. No aumenta las quejas de los usuarios. No hay impacto negativo en el patrimonio.	Pérdida o daño menor. Aumentan las quejas de los usuarios. Impacto mínimo en el valor del patrimonio (activos)	Pérdida significativa. Reclamos de usuarios a gran escala. Potencial pérdida de valor en el patrimonio	Pérdida o daño mayor. Investigación formal del regulador y aplicación de multas. Pérdida que afecta el valor del patrimonio	Pérdida catastrófica. Riesgo inaceptable en el sector. Intervención de ente regulador. Produce quiebra de la entidad o pone en peligro su continuidad.
Cuantitativo	Pérdida financiera <=Bs.1000	Pérdida financiera > Bs.1000 <= Bs. 10.000	Pérdida financiera >Bs. 10.000 y <=Bs. 100.000	Pérdida financiera >Bs. 100.000 y <=Bs. 1.000.000	Pérdida financiera >Bs.1.000.000
Objetivos	Impacto insignificante en el logro de los objetivos.	Impacto menor que es fácilmente remediable.	Algunos objetivos son afectados	Algunos objetivos importantes no pueden ser alcanzados.	La mayoría de los objetivos no pueden ser alcanzados.
Reputación e imagen	El evento solo es de conocimiento de los ejecutivos directa involucrados	El evento es de conocimiento general de la organización	El evento es de conocimiento a nivel local	El evento es de conocimiento a nivel nacional	El evento es de conocimiento a nivel internacional
Afectación al recurso humano	Evento que no ocasionó lesiones u ocasionó lesiones con incapacidad de hasta 3 días	Evento que ocasionó incapacidad de 3 días a 1 mes	Evento que ocasionó incapacidad de 1 mes hasta 3 meses	Evento que ocasionó incapacidad de 3 a 6 meses	Evento que ocasionó pérdida de vidas humanas o incapacidad permanente.
Legal	Los activos no se ven expuestos a pérdidas ni comprometidos por vulnerabilidad de ámbito legal alguna. Las operaciones no se ven afectadas. Los pasivos y contingentes se incrementan en un nivel insignificante.	Los activos se ven expuestos a pérdida y comprometidos en un nivel menor debido a la explotación de alguna vulnerabilidad en el ámbito legal. Las operaciones se ven afectadas en un nivel menor. Los pasivos y contingentes se incrementan en un nivel no importante.	Los activos se ven expuestos a pérdida y comprometidos en un nivel moderado debido a algunas vulnerabilidades de ámbito legal. Las operaciones se ven afectadas de manera negativa en un nivel considerable. Los pasivos y contingentes se incrementan en un nivel importante.	Los activos se ven expuestos a pérdida y comprometidos en un nivel grave debido a la exposición de varias vulnerabilidades de ámbito legal. Las operaciones se ven afectadas negativamente en un nivel grave. Los pasivos y contingentes se incrementan de manera grave.	Los activos se ven expuestos a pérdida y comprometidos en un nivel critico debido a la explotación de varias vulnerabilidades de ámbito legal. Las operaciones de la organización fueron suspendidas. Los pasivos y contingentes se incrementan en un nivel crítico.

ANEXO B: ESCALAS DE PROBABILIDAD DE QUE UN RIESGO SE MATERIALICE.

	Muy baja	Baja	Moderada	Alta	Muy alta
Probabilidad	0,10	0,30	0,50	0,70	0,90
Significado	Nunca ha pasado	Ha pasado en alguna ocasión	Ha pasado contadas ocasiones	Pasa la mayoría del tiempo	Actualmente ocurre. / Siempre

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

Establecer los lineamientos necesarios que permitan resguardar la información institucional y los recursos tecnológicos relacionados a su gestión y consumo.

2. ALCANCE

La presente política regirá para todo el ambiente de tecnología de la información y sus actores, tanto operadores, administradores y beneficiarios de la Escuela Militar de Ingeniería.

3. DESCRIPCIÓN DE LA POLÍTICA

3.1. Normas y Disposiciones Generales

Es política de la Escuela Militar de Ingeniería, generar normas de seguridad para:

- ✓ Definir un marco direccional para iniciar y controlar la implementación de la seguridad de la información, así como para la distribución de funciones y responsabilidades**.**
- ✓ La gestión de activos informáticos para que estos reciban un apropiado nivel de protección.
- ✓ Asegurar a un nivel razonable que todos los medios de procesamiento y/o conservación de información cuenten con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado, así como permitan la continuidad de las operaciones.
- ✓ El funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.
- ✓ Asegurar a un nivel razonable que la información y la capacidad de procesamiento manual y automático, este disponible en el momento necesario para usuarios autorizados. Considerando la continuidad de la operación tecnológica que soporta los procesos institucionales.

- ✓ Asegurar que los datos y/o transacciones cumplan con los niveles de autorización correspondiente para su utilización y divulgación.
- ✓ El Registro e identificación inequívoca de los usuarios de los sistemas.
- ✓ Evitar casos de suplantación de identidad por medio de los recursos tecnológicos.
- ✓ Mantener registros de auditoría de los eventos ocurridos así como el responsable de su ejecución.
- ✓ Mantener niveles de operación razonables en los sistemas e infraestructura estratégica para la Universidad.
- ✓ La identificación de riesgos relacionados al ambiente tecnológico que no permitan soportar a la Escuela Militar de Ingeniería, en su cumplimiento de objetivos.

4. RESPONSABILIDADES

El Comité de Seguridad de la Información integrado por:

- ✓ Vice-rectorado
- ✓ Jefe del Departamento Administrativo Financiero
- ✓ Director de las Unidad Académicas.
- ✓ Director Nacional de Informática

- ✓ Este comité tendrá la responsabilidad de revisar y aprobar la Política de Seguridad de la Información de la Escuela Militar de Ingeniería, así como también; supervisar el Plan de Seguridad de la Información de manera ejecutiva mediante:

- ✓ La revisión anual del Plan Estratégico del Área Seguridad.
- ✓ La definición de proyectos de tecnologías que fortalezcan la Seguridad de la Información del Negocio (Servicio, Producto e Información).
- ✓ Aprobar el Manual de Gestión de Seguridad de la Información y el plan de difusión

respectivo, para lograr el compromiso de todos los usuarios de la Escuela Militar de Ingeniería.

La **Dirección Nacional de Informática**, elaborará las políticas necesarias para proteger la información generada en el ambiente tecnológico de la Escuela Militar de Ingeniería.

El **Director o Jefe de Cada Repartición**, cumplirá la función de notificar a todo el personal que ingresa a sus obligaciones, respecto del cumplimiento de las Políticas de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.

El **Responsable del Área Legal** brindará la asesoría necesaria en el ámbito legal y regulatorio, así mismo otorgará los lineamientos necesarios para no incurrir en incongruencias legales dentro del ámbito de seguridad de la información.

El **Área de Control Interno de TI**, es responsable de practicar auditorías periódicas sobre el cumplimiento de las normas y procedimientos asociados al Sistema de Gestión de Seguridad de la Información.

5. CONTROL DE CUMPLIMIENTO Y ACCIONES

En caso de existir incumplimiento de la presente Política de Seguridad de la Información por parte de un trabajador de la Escuela Militar de Ingeniería, se comunicará al departamento de RRHH para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a más de las responsabilidades civiles y penales a que hubiere lugar.

ANEXO “A”: TÉRMINOS Y DEFINICIONES

- ✓ **Política General:** Contiene principios generales de seguridad de la información sobre los cuales deben basarse las normas, procedimientos y estándares técnicos.
- ✓ **Norma**: Definiciones concretas sobre cada uno de los temas de seguridad que luego serán adaptados a cada recurso informático en particular.
- ✓ **Procedimientos**: Detalle de cursos de acción y tareas que deben realizar los usuarios para hacer cumplir las definiciones de las normas.
- ✓ **Estándares técnicos**: Conjunto de parámetros específicos de seguridad para cada una de las tecnologías informáticas utilizadas.
- ✓ **Confidencialidad**: La información solo puede ser conocida por las personas definidas.
- ✓ **Integridad:** La información solo puede ser creada y/o modificada por las personas autorizadas.
- ✓ **Disponibilidad:** La información esté disponible cuando lo necesite el usuario.
- ✓ **Evaluación de Riesgo**: Se entiendo por evaluación de riesgos a valoración de amenazas y vulnerabilidades relacionadas con la información y los procesos que la contienen en tres: disponibilidad, integridad y confidencialidad. La evaluación de riesgos es un proceso cíclico y debe ser llevado periódicamente.
- ✓ **Administración de Riesgos:** Es un proceso en que se identifica, controla y minimiza o elimina, a un costo aceptable, los riesgos de seguridad que pueden afectar a la información.
- ✓ **Comité de Seguridad de la Información:** Es un equipo integrado por representantes de las diferentes áreas de la organización, destinado a apoyar las iniciáticas de Seguridad de la Información.
- ✓ **Responsable de Seguridad de la Información:** Persona que se encarga de

supervisar el cumplimiento de la presente política de seguridad y asesorar en materia de seguridad de la información a los miembros de la organización.

- ✓ **Incidentes de Seguridad:** Es cualquier evento que comprometa la confidencialidad, integridad y disponibilidad de la información de la organización.

POLÍTICAS DE LA RESPONSABILIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

POLÍTICAS DE RESPONSABILIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

Administrar adecuadamente la Seguridad de la Información en la Escuela Militar de Ingeniería y establecer un marco gerencial para iniciar y controlar su implementación y establecer las funciones y responsabilidades. Garantizar la aplicación de medidas de seguridad adecuadas por terceros en el procesamiento de la información interna de la Escuela Militar de Ingeniería.

2. ALCANCE

La presente política regirá a todo el ambiente de tecnología de la información y sus actores, tanto operadores, administradores y beneficiarios de la Escuela Militar de Ingeniería.

3. DESCRIPCIÓN DE LA POLÍTICA

3.1 NORMAS Y DISPOSICIONES GENERALES

3.1.1 ORGANIZACIÓN INTERNA

Asignación de responsabilidades en materia de seguridad de la información. La Escuela Militar de Ingeniería deberá considerar los siguientes roles para llevar una adecuada administración de la Seguridad de la Información.

FUNCIONES RELACIONADAS CON SEGURIDAD DE LA INFORMACIÓN

FUNCIÓN	ROL
Respaldo de la Política de Seguridad	Comité de Seguridad
Seguimiento de la Política de Seguridad	Oficial de Seguridad
Clasificación de la Información	Dueño de Datos
Cumplimiento de la Política de Seguridad	Usuarios finales Terceros y/o Personal Contratado Personal de la Dirección Nacional de Informática.

3.1.1.1 Definición del Comité de Seguridad de la Información

La seguridad de la información es una responsabilidad compartida con todos los miembros de la Escuela Militar de Ingeniería, por lo cual se define un comité de seguridad de la Información que integra miembros de la alta dirección para el apoyo de las iniciativas de seguridad de la información.

El comité estará conformado por.

- ✓ Vice-rectorado
- ✓ Jefe del Departamento Administrativo Financiero
- ✓ Directores de Unidades Académicas
- ✓ Director Nacional de Informática

3.1.1.2 Responsabilidades del Comité de Seguridad de la Información

Este comité tendrá la responsabilidad de revisar y aprobar la Política de Seguridad de la Información de la Escuela Militar de Ingeniería, así como también; supervisará el Plan de Seguridad de la Información de manera ejecutiva mediante:

- ✓ La revisión anual del Plan Estratégico del Área Seguridad
- ✓ La definición de proyectos de tecnologías que fortalezcan la Seguridad del Información del Negocio (Servicio, Producto e Información).
- ✓ Aprobar el Manual de Gestión de Seguridad de la Información y el plan de difusión respectivo, para lograr el compromiso de todos los usuarios de la Escuela Militar de Ingeniería.

3.1.1.3 Definición del Dueño de Datos

Son todos los responsables de cada uno de los procesos y sistemas de información que mantiene la Escuela Militar de Ingeniería.

El oficial de Seguridad conjuntamente con cada Jefe de Departamento y/o Sección de la

Escuela Militar de Ingeniería, son los responsables de identificar los dueños de datos y hacer conocer a los mismos sus responsabilidades. En esta identificación se debe determinar también:

- ✓ Información.
- ✓ Dueño de Datos.
- ✓ Recursos informáticos que procesan la información.
- ✓ Proceso Involucrado con la información.

3.1.1.4 Responsabilidades del Dueño de Datos

- ✓ Deberá identificar toda la información confidencial que corresponda a su área de responsabilidad directa, cualquiera sea su forma y medio de conservación, para proceder a clasificarla de acuerdo a lo establecido en la Política de Gestión de activos.

- ✓ Deberá autorizar el acceso a su información a toda persona o grupo que requiera. Este acceso contemplará los privilegios respectivos (lectura, escritura, actualización y eliminación).

- ✓ Podrá delegar su función a personal idóneo, pero conservaran la responsabilidad del cumplimiento de la misma. Además, deberán verificar la correcta ejecución de las tareas asignadas. La delegación de funciones debe quedar documentado por el propietarios e informadas al Oficial de Seguridad de dicha delegación.

3.1.1.5 Definición del Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI)

La Escuela Militar de Ingeniería, como toda organización maneja un flujo continuo de información que mueve gran número de las actividades de la institución, razón por la cual se ha conformado el Área de Seguridad de la Información, cuyos objetivos son:

- ✓ Desarrollar un grupo formal de administración de Seguridad en la Escuela Militar de Ingeniería, que trabaje en establecer mecanismos y políticas de seguridad que minimicen los riesgos potenciales.

- ✓ Disminuir el número y criticidad de los problemas de seguridad.
- ✓ Difundir la cultura de la seguridad de la información a los usuarios finales.
- ✓ Desarrollar procedimientos de seguridad en las distintas plataformas de la Escuela Militar de Ingeniería.
- ✓ Potenciar la formación de Recursos Humanos en el Área de Seguridad de la Información.
- ✓ Definir una adecuada Gestión de Incidentes de Seguridad de la Información.

3.1.1.6 Responsable del Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI)

- ✓ Deberá apoyar al Oficial de Seguridad en la ejecución del plan de Seguridad de la Información.
- ✓ Deberá participar en la implementación de los proyectos establecidos en el plan de Seguridad de la Información aprobados por el comité de Seguridad.
- ✓ Deberá investigar y dar seguimiento a los incidentes de seguridad de la información.
- ✓ Deberá estar en constante innovación y capacitación en temas relacionados con la Seguridad de la Información.
- ✓ Deberá establecer procedimientos de Auditoria a través de los cuales se efectúen controles permanentes del correcto cumplimiento de las medidas en el presente manual.
- ✓ Deberá realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente política.

3.1.1.7 Definición del Oficial de Seguridad

El oficial de seguridad tiene a su cargo la definición y el mantenimiento del Manual de Gestión de Seguridad de la Información y el asesoramiento a todo el personal de la

Escuela Militar de Ingeniería para su implementación.

3.1.1.8 Responsabilidades del Oficial de Seguridad

- ✓ Deberá implementar un plan para concientizar a la administración acerca de la importancia de dar seguridad según la criticidad de la información manejada en cada servicio.

- ✓ Deberá llevar a cabo el mantenimiento, aprobación, actualización, distribución y monitoreo del Manual de Gestión de Seguridad de la Información en base a los requerimientos futuros presentados por nuevos servicios.

- ✓ Deberá implementar los proyectos de seguridad que se planteen en el Plan de Seguridad de la Información de la Escuela Militar de Ingeniería.

- ✓ Deberá participar en la investigación y recomendaciones de productos de seguridad para la implementación de las medidas de seguridad en la Escuela Militar de Ingeniería.
- ✓ Deberá dar soporte a los usuarios en los procesos de:

    - o Identificación de la información sensible.

    - o Identificación de las medidas de seguridad necesarias en cada sistema para cumplir con el Manual de Gestión de Seguridad de la Información.

    - o Implementar dichas medidas.

- ✓ Deberá analizar e informar cualquier evento que atente contra la seguridad de la información al Director de la Dirección Nacional de Informática, así como monitorear periódicamente que solamente los usuarios autorizados tengan accesos a los sistemas.

- ✓ Deberá verificar la validez del plan aprobado para la Seguridad de la Escuela Militar de Ingeniería mediante un testeo constante.

- ✓ Deberá someter al plan de seguridad en una mejora continua.

- ✓ Llevar un registro actualizado de contactos de todos los administradores de los servicios de la Escuela Militar de Ingeniería.

3.1.1.9 Definición de los Administradores de los Servicios

Se considera a las personas encargadas de llevar la administración de las aplicaciones, servidores, bases de datos y equipos de comunicación existentes en la Escuela Militar de Ingeniería.

3.1.1.10 Responsabilidades de los Administradores de los Servicios

- ✓ Deberán implementar las medidas de seguridad dadas en el Manual de Gestión de Seguridad de la Información a fin de garantizar la seguridad de su servicio.
- ✓ Deberá participar activamente en las capacitaciones y actualizaciones periódicas para conocer el Manual.
- ✓ Deberá apoyar a los proyectos que se planteen en torno al tema de seguridad de la información.
- ✓ Deberá ser parte del desarrollo e implementación del Plan de Seguridad de la Escuela Militar de Ingeniería.

3.1.1.11 Definición de Usuario final

Se considera a todo el personal de la Escuela Militar de Ingeniería y/o terceros que hacen uso de las aplicaciones y la información con el objetivo de poder cumplir con sus correspondientes funciones.

3.1.1.12 Responsabilidades del Usuario Final

- ✓ Deberá cumplir con todas las medidas de seguridad definidas en el Manual de Gestión de Seguridad de la Información.
- ✓ Deberá participar activamente de las capacitaciones periódicas para conocer el Manual de Gestión de Seguridad de la Información.

3.1.1.13 Autorización para Instalaciones de Procesamiento de Información

- ✓ La inclusión de nuevos servicios para el procesamiento de la información deberá ser autorizada por el dueño de datos involucrado y por la Dirección Nacional de Informática

- ✓ El Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), deberá identificar e implementar controles de seguridad necesarios contra posibles vulnerabilidades introducidos por la implementación de nuevos sistemas e infraestructura que procese información.

3.1.1.14 Acuerdos de confidencialidad

- ✓ Todos los administradores de servicios deberán firmar un Acuerdo de Confidencialidad.

- ✓ Todo el personal que trabaja en el Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), deberá obligatoriamente firmar un Acuerdo de Confidencialidad, estos incluyen personal de planta, becarios de investigación y tesistas. (Ver Plantillas "Acuerdo de Confidencialidad")

3.1.1.15 Revisión Independiente de la Seguridad de la Información

El Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), realizará revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de Información, con el fin de verificar y garantizar que las prácticas de la Escuela Militar de Ingeniería reflejen adecuadamente sus disposiciones.

3.1.2 TERCEROS

3.1.2.1 Identificación de Riesgos Derivados del Acceso de Terceros

En caso que sea necesario que un tercero tenga acceso a información o servicios tecnológicos internos de la Escuela Militar de Ingeniería, el Oficial de Seguridad y el responsable de la información o servicios tiene la responsabilidad de documentar y realizar una evaluación de riesgos para definir los controles necesarios, tomando en cuenta los siguientes aspectos:

- ✓ El tipo de accesos que requiere.
- ✓ El motivo por el que solicita el acceso.
- ✓ El valor de la información.
- ✓ Los controles que tomará la tercera parte.
- ✓ La incidencia del acceso en la seguridad de la información de la Escuela Militar de Ingeniería.

No se otorgará acceso a terceros a la información, hasta que se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdos de confidencialidad que definan las condiciones para la conexión o acceso.

3.1.2.2 Requerimientos de Seguridad en Contratos y Acuerdos con Terceros

Los contratos o acuerdos con terceros que se efectúen deben tomar en cuenta:

- ✓ Cumplimiento de la Política de Seguridad de la Información de la Escuela Militar de Ingeniería
- ✓ Protección de los activos de la Escuela Militar de Ingeniería, incluyendo:
    - o Procedimientos para proteger los bienes de la Escuela Militar de Ingeniería, abarcando los activos físicos, la información y el software.
    - o Controles para garantizar la recuperación o destrucción información y los activos al finalizar el contrato o acuerdo, o durante la vigencia del mismo.
- ✓ Definición de nivel de servicios esperado y del nivel de servicio aceptable.
- ✓ Acuerdos de control de acceso que contemplen:
    - o Métodos de accesos permitido, y el control uso de identificadores únicos.
    - o Procesos de autorización y privilegios de usuarios.
    - o Requerimiento para mantener actualizada una lista de individuos autorizados

a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

- ✓ Procesos claros y detallados para la administración de cambios.
- ✓ Controles que garanticen la protección contra software malicioso.
- ✓ Acuerdos de confidencialidad en los contratos.

3.1.2.3 Requerimientos de Seguridad en Contratos de Tercerización

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de PC del Organismo, contemplarán además de los puntos especificados en ("Requerimientos de Seguridad en Contratos o Acuerdos con Terceros"), los siguientes aspectos:

- ✓ Acuerdo de confidencialidad.
- ✓ Forma en que se cumplirán los requisitos legales aplicables.
- ✓ Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.
- ✓ Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos de la Escuela Militar de Ingeniería
- ✓ Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible de la Escuela Militar de Ingeniería.
- ✓ Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
- ✓ Niveles de seguridad física que se asignarán al equipamiento tercerizado.
- ✓ Derecho a la auditoría por parte de la Escuela Militar de Ingeniería, sobre los aspectos tercerizados en forma directa o a través de la contratación de este servicio.

- ✓ Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.
- ✓ Si el servicio que se va contratar es la instalación y/o configuración de servidores, equipos de comunicación y/o aplicación, se deberá pedir al tercero que se realice un hardening de seguridad que debe de contemplar como mínimo.
    - o Definición de accesos a los servicios.
    - o Cambio de configuraciones por defecto.
    - o Cambio o eliminación de archivos de instalación.
    - o Ocultamiento de versions.
    - o Cambio o eliminación de usuarios y claves por defecto.
    - o Desinstalación de servicios innecesarios.
    - o Configuración de Firewall.
    - o Eliminación de accesos a recursos innecesarios

4. CONTROL Y CUMPLIMIENTO DE SANCIONES

En caso de existir incumplimiento de la presente Política de Seguridad de la Información por parte de un trabajador de la Escuela Militar de Ingeniería, se comunicará al Departamento de Recursos Humanos para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a más de las responsabilidades civiles y penales a que hubiere lugar.

ACUERDO DE CONFIDENCIALIDAD

Yo……por el presente dejo constancia de haber recibido accesos de seguridad e información confidencial de la Escuela Militar de Ingeniería, comprometiéndome a aceptar y cumplir con todas las políticas, normas y estándares de seguridad informática de la Escuela Militar de Ingeniería y, específicamente, a:

- ✓ No utilizar la información para fines contrarios a los intereses de la Escuela Militar de Ingeniería.
- ✓ El intento de ganar acceso a recursos asignados al mismo será considerado “intento de violación al sistema” en el cual la Escuela Militar de Ingenieria se reserva los derechos de tomar acciones pertinentes al caso.
- ✓ No divulgar información obtenida de los sistemas de la Escuela Militar de Ingeniería.
- ✓ No revelar la contraseña otorgada.
- ✓ Modificar la contraseña al sospechar que esta haya sido descubierta.
- ✓ Aceptar las responsabilidades sobre el uso de mi cuenta de usuario.
- ✓ Utilizar el sistema de la Escuela Militar de Ingeniería únicamente para fines aprobados por esta.
- ✓ No permitir la utilización de la cuenta de usuario por terceros.
- ✓ No realizar instalación de ningún tipo de software no homologado por la Escuela Militar de Ingeniería.
- ✓ Aceptar que toda la información conservada en los equipos informáticos (archivos y correos electrónicos residentes en servidores de datos centralizados y/o estaciones de trabajo) es de propiedad de la Escuela Militar de Ingeniería, por lo que podrá ser administrada y/o monitoreada por los responsables del área de sistemas de acuerdo con las pautas de seguridad definidos.
- ✓ Efectuar la destrucción de todo mensaje cuyo origen es desconocido, y asumir la responsabilidad por las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. en estos casos, no se deben contestar dichos mensajes

y debe ser enviada una copia al administrador de seguridad para que efectué las tareas de seguimiento e investigación necesarias.

- ✓ Desconectarse de la estación de trabajo correspondiente cada vez que finalice con las tareas que en ella desarrolla, a fin de evitar el uso de la la clave por otra persona.

En caso de incumplimiento de las obligaciones contenidas en este documento reconozco el derecho de la Escuela Militar de Ingeniería, para reclamar las indemnizaciones respectivas a través de todas las acciones judiciales contempladas en las leyes vigentes y presentar inclusive las acciones penales a que hubiere lugar de acuerdo con los dispuesto en la Ley 1322 de Propiedad Intelectual en Bolivia.

La terminación del presente acuerdo, por cualquier causa, no me libera de las obligaciones de confidencialidad adquiridas en virtud del mismo, respecto a la información que le haya sido revelada hasta la fecha de la terminación.

Usuario……

Fecha de entrega:……/……/……

Firma de Usuario

C.I……

POLÍTICAS DE GESTIÓN DE ACTIVOS

POLÍTICAS DE GESTIÓN DE ACTIVOS

1. OBJETIVO

Alcanzar y mantener una protección adecuada de los activos e información de la Universidad.

2. ALCANCE

La presente política regirá para todo el ambiente de tecnología de la información y sus actores, tanto operadores, administradores y beneficiarios de la Escuela Militar de Ingeniería.

3. DESCRIPCIÓN DE LA POLÍTICA

3.1 Normas y Disposiciones Generales

3.1.1 Inventario

- ✓ Todas las áreas de la Dirección Nacional de Informática deben llevar un inventario de los activos tecnológicos que manejan.

    - El Departamento de Asistencia Técnica, deberá mantener un inventario actualizado de las PC's e impresoras instaladas dentro de la Escuela Militar de Ingeniería. (Ver estándar: Inventario de equipos computacionales e impresoras).

    - El Departamento de Tecnologías de la Información, deberá mantener un inventario de los servidores, y equipos de comunicación activos existentes en la Escuela Militar de Ingeniería. (Ver estándar: Inventario de Servidores y Equipos de comunicación).

- ✓ Todo PC's e impresoras de la Escuela Militar de Ingeniería, equipos activos y servidores deberán estar etiquetados para su identificación y control de inventario. Este etiquetado será realizado por el Departamento de Activos Fijos.

- ✓ El Departamento de Asistencia Técnica y el Departamento de Tecnologías de la

Información conjuntamente con Activos Fijos deberán controlar periódicamente y actualizar el inventario de sus respectivos equipos cada que exista una movilización y/o nueva adquisición.

- ✓ Cada área de la Dirección Nacional de Informática deberá identificar la información que son procesados por los sistemas informáticos y clasificarlos, para luego realizar un inventario de esta información y mantenerlo actualizado. (Ver estándar: Inventario de Información).

- ✓ Cada área de la Dirección Nacional de Informática, deberá definir el inventario de servicios que presta a la Escuela Militar de Ingeniería y mantenerlo actualizado. (Ver estándar: Inventario de Servicios)

- ✓ El Departamento de Asistencia Técnica e Departamento de Tecnologías de la Información, deberá establecer procedimientos para la movilización, adquisición y dar de baja (de manera técnica) los equipo a su cargo.

3.1.2 Clasificación de la Información

Cada área de la Dirección Nacional de Informática conjuntamente con el dueño de datos y el Oficial de Seguridad deberán clasificar la información según los siguientes tres criterios:

3.1.2.1 Confidencialidad

a) **Público:** Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea de la Escuela Militar de Ingeniería o no.

b) **Reservada – uso interno:** Información que puede ser conocida y utilizada por todos los empleados de la Escuela Militar de Ingeniería y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la Escuela Militar de Ingeniería.

c) **Reservada – Privada:** Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la

Escuela Militar de Ingeniería.

d) **Reservada – Confidencial:** Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la Escuela Militar de Ingeniería, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo.

3.1.2.2 Integridad

a) Información cuya modificación no autorizada puede prepararse fácilmente, o no afecta la operatividad de la Escuela Militar de Ingeniería.

b) Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la Escuela Militar de Ingeniería.

c) Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la Escuela Militar de Ingeniería.

d) Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la Escuela Militar de Ingeniería.

3.1.2.3 Disponibilidad

a) Información cuya inaccesibilidad no afecta la operatoria de la Escuela Militar de Ingeniería durante un mes.

b) Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para la Escuela Militar de Ingeniería.

c) Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la Escuela Militar de Ingeniería.

d) Información cuya inaccesibilidad permanente durante 2 horas podría ocasionar pérdidas significativas a la Escuela Militar de Ingeniería.

- ✓ Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

- **Criticidad Baja:** ninguno de los valores asignados superan el 1.
- **Criticidad Media**: alguno de los valores asignados es 2
- **Criticidad Alta:** alguno de los valores asignados es 3

✓ Sólo el Dueño de datos puede asignar o cambiar su nivel de clasificación.

✓ El Dueño de datos con apoyo del administrador del servicios deberá identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deberán tener acceso a la misma.

✓ En adelante se mencionará como “información clasificada” (o “datos clasificados”) a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

✓ El Dueño de datos deberá definir los criterios utilizados para la depuración de datos y su periodicidad.

4. Control de Cumplimiento y Sanciones

En caso de existir incumplimiento de la presente Política de Seguridad de la Información por parte de un trabajador de la Escuela Militar de Ingeniería, se comunicará a la Departamento de Recursos Humanos para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a más de las responsabilidades civiles y penales a que hubiere lugar.

INVENTARIO DE EQUIPOS COMPUTACIONALES E IMPRESORAS

Equipos Computacionales

No	Propietario	Localización			Ti	Componentes					Aplicacion	Sistema	Mem o	Pr	Garantí	Observaciones
		Edifici	Departamento	Ár		Nombr	Mar	Model	Se	Activ						

Impresoras

No.	Propietario	Localización			Tipo	Marca	Modelo	Serie	Activos	Garantía	Observaciones
		Edificio	Departamento	Ár							

INVENTARIO DE SERVIDORES Y EQUIPOS DE COMUNICACIÓN

Servidores

- ✓ Nº
- ✓ Nombre del servidor
- ✓ Dependencia
- ✓ Datos del Administrador o Nombre y Apellidos o Extensión
  - Número de Celular
- ✓ Datos del Backup
  - Nombre y Apellidos
  - Extension
  - Número de Celular
- ✓ Servicios que presta
- ✓ Dirección IP
- ✓ Sistemas Operativos
  - Nombre del Sistema Operativo
  - Versión
- ✓ Marca
- ✓ Hardware del Servidor
  - Type/Parte Number
  - Modelo
  - N/S
  - Descripción
- ✓ Procesador
  - Número
  - Tipo
  - Velocidad (GHz)
- ✓ Memoria
- ✓ Disco Interno
  - Número o Tamaño o Tipo
  - Configuración
- ✓ Disco Interno

- Número o Tamaño o Tipo
- Configuración

✓ Tarjeta de Red
- Número
- Velocidad

✓ Ubicación Física
- Lugar
- Rack
- Blade Center
  - Número de Blade Center
  - Cuchilla

Expiración de Garantía

✓ Fecha de Inicio de producción

✓ Respaldos
- ¿Respalda?
- Tamaños de respaldos (aproximado)
- Medio de respaldo
- Periodo de respaldo

✓ Criticidad

✓ Observaciones

DISPOSITIVOS DE RED

Dirección IP	Hostname	Ubicación	Modelo	Versión	Serie	Numero de Parte	Tipo de Dispositivo	Criticidad	Garantía	Observación

INVENTARIO DE INFORMACIÓN

Nº	Información	Clasificación (0-3)				Propietario	Localización	Medio o formato de almacenamiento	Observación
		Confidencialidad	Integridad	Disponibilidad	Categoría				

INVENTARIO DE SERVICIOS

Nº	Área	Servicio	Descripción del Servicio	Administrador del servidor	Criticidad del Servicio

POLÍTICA DE LA SEGURIDAD FÍSICA EN LAS INSTALACIONES

POLÍTICA DE LA SEGURIDAD FÍSICA EN LAS INSTALACIONES

1. OBJETIVO

Mantener una adecuada protección física de los equipos, soportes de procesamiento, transmisión y conservación de la información de la Escuela Militar de Ingeniería.

2. ALCANCE

La presente política regirá para todo el ambiente de tecnología de la información y sus actores, tanto operadores, administradores y beneficiarios de la Escuela Militar de Ingeniería.

3. DESCRIPCIÓN DE LA POLÍTICA

3.1 Normas y Disposiciones Generales

3.1.1 Consideraciones Generales

El área de Infraestructura de Escuela Militar de Ingeniería, deberá contar con un estándar para la Sala de Servidores, tomando en cuenta:

- ✓ Un sistema de climatización adecuada para el buen funcionamiento de los equipos.
- ✓ Sistemas de detección de humo y calor.
- ✓ La protección contra accesos no autorizados.
- ✓ Cableado de red y eléctrico (Ejemplo: organización y etiquetado).
- ✓ Sistema Eléctrico (ejemplo: energía redundante, UPS's (Uninterrumpible Power Supply), generadores, etc.)
- ✓ Todos los servidores de la Escuela Militar de Ingeniería deberán ubicarse en la sala de servidores y colocarlos en racks. Si algún administrador no colocara su servidor en dicho lugar, este debe presentar por escrito los motivos y justificación de esto al Responsable del equipo de la Sala de Servidores.
- ✓ Se deberá realizar revisiones periódicas, al menos una vez al año, sobre el estado del cableado de red y sobre su organización.

3.1.2 Control de Accesos

El Departamento de Asistencia Técnica de Informática deberá establecer un equipo de trabajo que se encargará de velar por el buen estado, funcionamiento y la buena presentación de la Sala de Servidores. Este equipo debe estar compuesto por:

- Responsable del equipo de la Sala de Servidores.
- Responsable de red.
- Responsable de la parte eléctrica.
- Responsable del aire acondicionando.
- Responsable de mantenimiento de servidores.

- ✓ Los Jefes de Departamento y/o Secciones de la Escuela Militar de Ingeniería y el Oficial de Seguridad deberán elaborar un listado del personal autorizado para ingresar a la Sala de Servidores. Estrictamente se debe apuntar a las personas que por el rol de sus funciones tiene que ingresar cotidianamente. Este listado deberá estar a cargo del Responsable del equipo de la sala de servidores y el Oficial de Seguridad.
- ✓ Las nuevas solicitudes de acceso a la sala de servidores, deberán ser evaluadas por el Oficial de Seguridad.
- ✓ Los miembros del equipo de la Sala de Servidores deberá entregar al personal autorizado una clave única, la que le permitirá ingresar a la sala de servidores y ser registrada en el Sistema de Control de Accesos.
- ✓ Los miembros del equipo de la Sala de Servidores y el Oficial de Seguridad deberá implementar controles para vigilar que el acceso a la sala de servidores sea efectivamente por el personal autorizado.
- ✓ El personal del Departamento de Asistencia Técnica deberán portar un identificativo para realizar el mantenimiento de software o equipo en las diferentes instalaciones de la Escuela Militar de Ingeniería.

- ✓ Los tours de visitas a la sala de servidores, deben ser realizadas con la presencia de al menos un personal de la Dirección Nacional de Informática.

3.1.3 Factores Ambientales

- ✓ El equipo de la sala de servidores deberá gestionar mantenimiento periódico para:
- ✓ UPS`s
- ✓ Aire acondicionado de la sala de servidores.
- ✓ Generador eléctrico del edificio de Escuela Militar de Ingeniería.
- ✓ Servidores
- ✓ Se deberá prohibir el ingreso de alimentos y bebidas en la sala de servidores.

3.1.4 Instalaciones Eléctricas

- ✓ Las áreas de trabajo y a los equipos que son considerados vitales en la Escuela Militar de Ingeniería deberán estar conectadas a un UPS y a un generador.
- ✓ Previo a la instalación de equipos informáticos en la sala de servidores el área del Departamento de Tecnologías de la Información de la Escuela Militar de Ingeniería deberá realizar cálculos de la carga eléctrica requerida en la instalación, de los tableros de distribución, así como de los circuitos y conexiones que deben soportar la carga adicional proyectada.

3.1.5 Movilización de Equipos

- ✓ Debe existir procedimientos formales para la movilización o adquisición de equipo computacionales.
- ✓ Las movilizaciones de equipos computacionales deberán ser informadas y autorizadas por el personal del Departamento de Asistencia Técnica.

3.1.6 Guardia

El personal de Guardia deberá registrar la orden de salida de los equipos para su movilización fuera de las instalaciones de la Escuela Militar de Ingeniería.

3.1.7 Ordenadores Portátiles y Teletrabajo

- ✓ Los equipos portátiles usados por los administradores deben ser de propiedad de la Escuela Militar de Ingeniería.
- ✓ Los administradores no puede portar información sensible de la Escuela Militar de Ingeniería en medios extraíbles como: discos, pen drive, teléfonos celulares, etc, fuera de las instalaciones de la Escuela Militar de Ingeniería.
- ✓ Los administradores no puede trabajar con equipos portátiles personales ni portar información de la Escuela Militar de Ingeniería en los mismos.

4. Control de cumplimiento y sanciones

En caso de existir incumplimiento de la presente Política de Seguridad de la Información por parte de un trabajador de la Escuela Militar de Ingeniería, se comunicará al Departamento de Recursos Humanos para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a más de las responsabilidades civiles y penales a que hubiere lugar.

POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES Y OPERACIONES

POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES Y OPERACIONES

1. OBJETIVO

Asegurar la integridad, confidencialidad y disponibilidad de la información en su transmisión y recepción tanto en una red interna como externa.

2. ALCANCE

La presente política regirá para todo el ambiente de la Direccion Nacional de Informática y sus actores, tanto operadores, administradores y beneficiarios de la Escuela Militar de Ingeniería.

3. DESCRIPCIÓN DE LA POLÍTICA

3.1 Normas y Disposiciones Generales

3.1.1 Consideraciones Generales

- ✓ Todos los equipos de comunicación, servidores y aplicaciones deberán contar con soporte de direccionamiento Dual Stack (IPv4 e IPv6).
- ✓ IPv6 deberá estar habilitado en todos los servicios de la Universidad tanto internos como externos.

3.1.2 Responsabilidades y Procedimiento de Operación

- ✓ Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta política y sus cambios serán autorizados por el Oficial de Seguridad.
- ✓ Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:
  - o Monitoreo de red y servidores
  - o Administración de la W-LAN, LAN y WAN

- Administración de equipo de seguridad (Firewall, Switch de Core, IPS y IDS)
- Administración de Servidores
- Administración de servicios informáticos
- Alta y baja de cuenta de usuario en todos los sistemas
- Verificación de accesos
- Respaldos
- Mantenimiento de servidores
- Mantenimiento de equipo computacionales
- Mantenimiento de equipos de red
- Manejo de incidentes de seguridad
- Recuperación de información
- Control de cambios

✓ En cada uno de los procedimientos se deberán especificar cuales son los responsable de realizar las tareas en cada procedimiento.

✓ Se deberá establecer estándares de configuración segura para las diferentes plataformas bases como son: servidores (Windows, Linux, Solaris y Aix), equipos de comunicación de red y bases de datos.

3.1.3 Control de Cambio en las Operaciones

✓ Se deberá cumplir el proceso de control de cambios para cualquier cambio que se requiera realizar en: infraestructura, sistema, configuración en servidores, WAN, LAN y la incorporación de nuevos servicios tecnológicos.

✓ Se definirán procedimientos y estándares para cada área de la Direccion Nacional de Informática, para el control de los cambios en los ambientes operativos y de

comunicación.

Todo cambio deberá ser evaluado en aspectos técnicos y de seguridad.

- ✓ El Oficial de Seguridad, controlará que los cambios en los componentes operativos y de comunicación no afecten la información y seguridad de los mismos.
- ✓ Cada Jefe de Departamento y/o Sección, tiene la responsabilidad de evaluar el impacto operativo de su área debido a los cambios previstos y verificará su correcta implementación.
- ✓ Los procedimientos de control de cambios deberán contemplar lo siguiente:
  - o Identificación y registros de cambios significativos.
  - o Evaluación del posible impacto.
  - o Evaluación de riesgos.
  - o Aprobación formal de los cambios propuestos.
  - o Planificación del proceso
  - o Pruebas del nuevo escenario.
  - o Comunicación de cambios a todos los involucrados.
  - o Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto a los mismos.
  - o Regirse a la Política de Control de Cambios establecida.

3.1.4 Separación de los Recursos de Desarrollo, Pruebas y Operación

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo. Para ello, se tendrán en cuenta los siguientes controles:

- ✓ Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios.

- ✓ Separar las actividades de desarrollo y prueba, en entornos diferentes.

- ✓ Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.

- ✓ Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas.

- ✓ Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.

- ✓ Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.

- ✓ El personal de desarrollo no tendrá acceso al ambiente operativo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

- ✓ Todo servicio deberá ser probado y verificado su funcionamiento en un ambiente de pruebas.

- ✓ Los servicios que se estén probando para su operación también deberán pasar pruebas de seguridad.

3.1.5 Planificación y Aceptación del Sistema

- ✓ Cada Jefe de Departamento de la Dirección Nacional de Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los servicios en operación y proyectará las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta los nuevos requerimientos de los servicios así como las tendencias actuales y proyectadas en el procesamiento de la información de la Escuela Militar de

Ingeniería, para el período estipulado de vida útil de cada componente.

- ✓ Los Jefes de Departamento y/o de Secciones informarán las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

- ✓ El equipo de control de cambio deberán especificar los criterios de aceptación para un nuevo sistema o servicio tecnológico a implementar en la Escuela Militar de Ingeniería. Debe considerar los siguientes puntos:

    - o Verificar el impacto en el desempeño y requerimientos de capacidad en los equipos informáticos.

    - o Garantizar la recuperación ante errores.

    - o Garantizar la implementación acorde a las normas de seguridad establecidas.

    - o Asegurara que la nueva implementación no afectaran negativamente a los sistemas existentes.

    - o Considerar el efecto en la seguridad de la Escuela Militar de Ingeniería con la nueva implementación.

3.1.6 Protección Contra Software Malicioso

- ✓ El Departamento de Asistencia Técnica y el Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), deberán definir e implementar controles de detección y prevención contra código maliciosos.

- ✓ El Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), desarrollará procedimientos adecuados para concientizar a los usuarios en materia de seguridad y control de accesos a los sistemas.

- ✓ Estos controles deberán considerar las siguientes acciones:

- Prohibir el uso de software no autorizado por la Escuela Militar de Ingeniería.
- Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.
- Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles.
- Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Escuela Militar de Ingeniería, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

3.1.7 Respaldos

Los administradores de los servicios y sus backup deberán mantener documentos actualizados de políticas y manuales de administración, configuración y manejo del software instalado en los servidores y equipos de comunicación, y usuarios finales para la adecuada administración de los mismos. Estos documentos deberán especificar:

- ✓ Fecha de creación.
- ✓ Versión del documento.
- ✓ Cambios efectuados.
- ✓ Datos informativos de la persona que los elaboró.
- ✓ Aprobación.
- ✓ Departamento de Tecnologías de la Información, debe proveer a los administradores de servicios un sistema de respaldos como: CD's, cintas, servidor de respaldos o cualquier otro medio de almacenamiento.
- ✓ Los administradores de los servicios deberán respaldar el código, datos, base

de datos, configuraciones antes de aplicar cualquier cambio.

- ✓ Solo los administradores de los servidores y sus backup tiene acceso al lugar de almacenamiento de los respaldos dentro de la Escuela Militar de Ingeniería o fuera de ella.

- ✓ Se deberá tener un lugar alterno para guardar los respaldos físicamente, este lugar debe estar fuera de las instalaciones del edificio de la Escuela Militar de Ingeniería.

- ✓ El lugar alterno de respaldos deberá contar con la infraestructura, medidas de seguridad y ambientales necesarias para mantener una adecuada organización y clasificación de las copias de respaldos.

- ✓ Cada administrador deberá priorizar la información según su nivel de importancia, (aplicando los ítems mencionados en la Política de Gestión de Activos), y su comportamiento para determinar la frecuencia de respaldos.

- ✓ Se deberá trasladar de manera inmediata los respaldos residentes en el disco del computador del administrador a dispositivos secundarios como CD's, cintas, o cualquier otro tipo de almacenamiento en forma inmediata luego de haber realizado esta tarea.

- ✓ La copia de respaldos si tuviere un uso excesivo deberá reemplazarse periódicamente, antes de que el mismo medio magnético de almacenamiento que la contiene llegue a deteriorarse.

- ✓ Al momento en que los medio de respaldos (cintas magnéticas, CD's, etc) deban desecharse, estos deberán ser destruidos de forma segura para evitar copias o recuperación de la información almacenada.

- ✓ Los administradores de los servicios y sus backup deberán verificar el funcionamiento de los medio de almacenamiento antes de realizar el respaldo.

- ✓ Las copias de respaldo deberán conservase en armarios de acceso restringido.

- ✓ El administrador principal y su backup deberán realizar pruebas periódicas para

verificar la validez y funcionalidad de las mismas.

- ✓ Toda la información respaldada será clasificada y etiquetada. En su medio de almacenamiento debe incluir: nombre del archivo, versión, aplicación o sistema al que pertenece la información, fecha de respaldo, persona que hizo el respaldo, ubicación física para su almacenamiento.

- ✓ Los administradores de los servicios deberán llevar un registro de la información respaldada para su fácil localización.

- ✓ Se deberá manejar políticas y procedimientos para la administración, generación y pruebas y respaldos de información.

3.1.8 Administración de Servidores

- ✓ El responsable de cada dependencia de la Escuela Militar de Ingeniería, donde se administren servidores, debe asignar un administrador principal y de bakcup para los equipos.

- ✓ Los administradores son los responsables de establecer el manual de administración y configuración de sus servicios, y solicitar y documentar los permisos que son necesarios para el funcionamiento del servicio.

- ✓ Cuando se implemente un nuevo servicio en producción, el administrador tiene la responsabilidad de solicitar al Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), un Reporte de vulnerabilidades de equipo.

- ✓ El Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), debe realizar el escaneo de vulnerabilidades a los servidores de la Escuela Militar de Ingeniería y este debe entregar el reporte respectivo a cada administrador.

- ✓ El administrador y su backup debe dar respuesta a este reporte con un informe de los huecos de seguridad arreglados.

- ✓ Se debe establecer una línea base del comportamiento de los servidores y equipos de comunicación para su monitorización.

- ✓ Todos los servidores y equipos de comunicación deben estar monitoreados por el administrador de la red. Como mínimo deben monitorearse:
- ✓ Disponibilidad del Servicio que presta el servidor
  - o Disco
  - o Procesador
  - o Memoria
- ✓ Los informes de monitoreo deben ser enviados al administrador del servicio cada mes o cuando se presente una situación anormal en el mismo.
- ✓ Para el monitoreo de la integridad del sistema de archivos de los servidores se debe instalar un HIDS (Sistema de Detección de Intrusos de Host). Se puede utilizar osiris para Windows y Linux.
- ✓ El administrador de la LAN conjuntamente con el administrador de cada servidor deben planificar cada 6 meses una depuración de permisos de red tanto de intranet como de internet para los servidores que administran.
- ✓ La solicitud de permisos de red hacia los servidores deben ser solicitados por el administrador o el backup del mismo.
- ✓ Los administradores de servidores deben como mínimo configurar sus servidores bajo el estándar técnico establecido (ver estándar: Línea base de servidores)
- ✓ El administrador de servidores debe informar al administrador del antivirus la presencia de código malicioso que no es detectado por el antivirus de la Escuela Militar de Ingeniería.
- ✓ El administrador del antivirus debe reportar lo antes mencionado al proveedor de antivirus y dar un plan de acción al administrador.
- ✓ Todos los servidores en producción deben estar en una de las vlan’s de servidores internos o externos (DMZ Zona Desmilitarizada).

- ✓ En caso de que no sea posible esto, el administrador de servidores se responsabiliza por la seguridad del mismo.

- ✓ Internet. En caso de ser estrictamente necesario este acceso se lo realizará a través de un mecanismo seguro como una red privada virtual o un canal dedicado.

- ✓ El administrador debe revisar periódicamente los log de auditoría de su servidor.

- ✓ Cuando existan un cambio de administradores, se debe realizar la capacitación respectiva al nuevo administrador y se debe realizar la entrega de manuales de administración y configuración.

- ✓ Además, el nuevo administrador debe proceder a realizar el cambio de claves de los usuarios de administración, eliminar usuarios personales del anterior administrador y depuración de permisos.

- ✓ En los servidores de pruebas se debe implementar todos los puntos anteriores de esta sección.

3.1.9 Gestión de Seguridad en la red

3.1.9.1 Red Interna

- ✓ La Dirección Nacional de Informática deberá establecer estándares para el etiquetad y cableado estructurado de voz y datos.

- ✓ El Departamento de Tecnologías de la Información, deberá establecer estándares de configuración para los dispositivos de red (firewall, router, switch) con los niveles de seguridad definidos para cada servicio.

- ✓ El Departamento de Asistencia Técnica deberá configurar los nuevos equipos computacionales bajo el estándar establecido (ver estándar: Configuración de equipos computacionales).

- ✓ No está permitido el uso de módems en PC's que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Escuela Militar de Ingeniería y las autorizaciones por parte del administrador, con el fin de prevenir

la intrusión de hackers.

- ✓ Toda estación de trabajo deberá estar asociado a una Vlan dependiendo de sus funciones.

- ✓ En los segmentos de red de servidores internos y externos se debe establecer obligatoriamente Listas de Control de Accesos (ACL's) tomando en cuenta el principio del mínimo privilegio.

- ✓ Si un usuario final necesita acceder a servicios externos de la Escuela Militar de Ingeniería, que se encuentran restringidas (como ftp, vpn's, escritorio remoto, etc), este debe realizar la solicitud (ver plantilla: Solicitud de Permisos).

- ✓ El personal del Departamento de Asistencia Técnica serán encargado de: primeramente validar la necesidad de lo solicitado y realizar la asignación del permiso en caso de que se requiera.

- ✓ Si un administrador de servicios necesita permisos adicionales a los ya establecidos en sus servidores, el único personal autorizado para solicitarlos es el administrador del servicio o su backup.

- ✓ Ellos deberán solicitar el permiso (ver plantilla: Solicitud de Permisos). Estas solicitudes deberán ser atendidas por el administrador de la LAN o su backup, quienes son los únicos autorizados para asignar permiso de servidores.

- ✓ El administrador de la Red LAN debe tener documentado la asignación de IP's públicas a los servidores, equipos computacionales y de red, tomando en cuenta:

    - o Justificación del uso de la IP pública.

    - o Vigencia de la asignación de la IP pública.

    - o Permisos asignados a dicha IP pública.

    - o Justificación de los permisos asignados.

- ✓ El Oficial de Seguridad deberá revisar cada tres meses la documentación de

IP's Publicas asignadas y sus permisos asociados.

3.1.9.2 Acceso Remoto

- ✓ Los accesos remotos a sistemas informáticos de uso interno deben estar debidamente autorizados por el administrador del sistema y el Oficial de Seguridad.
- ✓ Se debe permitir acceso remoto (desde la red externa) a los servidores, solamente a personal autorizado e identificados dentro de la Escuela Militar de Ingeniería, como son administrador y backup de un determinado servicio.
- ✓ Para el acceso remoto a los servidores se debe utilizar protocolos seguros como SSH V2 para servidores Linux, Solaris, AIX, WMWare ESX, Roocks y MAC y mstsc para servidores Windows.
- ✓ Para la administración remota de los servidores mediante aplicaciones Web, se deberá obligatoriamente habilitar SSL en la aplicación web (HTTPS).
- ✓ En caso de ser necesario el acceso de terceros a la administración de un determinado servidor, el administrador de dicho servidor y el Oficial de Seguridad son los responsables de autorizar el acceso.
- ✓ Las conexiones externas remotas deben ser autorizadas por el Oficial de Seguridad.
- ✓ Las conexiones externas remotas se las debe establecer por medio del servicio de VPN.

3.1.9.3 Red Inalámbrica

El Departamento de Tecnologías de la Información, deberá establecer los Manuales de Configuraciones para Access Point.

- ✓ El administrador de la red inalámbrica deberá desarrolla un Manual para usuario final en el que se presente paso a paso como unirse a la red inalámbrica y los posibles problemas que puedan haber.
- ✓ Las redes WLAN deben ser asignadas a una subred dedicada y no compartidas con una red LAN.

- ✓ La red WLAN es considerada insegura, por lo que todo el tráfico entre ella y la red corporativa debe ser filtrada. Estos filtrados deben ser aplicados principalmente a la red de servidores, por lo que no se permitirá la administración de servidores desde la red inalámbrica.

- ✓ El acceso a la administración de los Accesos Point ya sea por ssh o via web deben ser permitida solo al personal autorizado.

- ✓ El Access Point deberá estar configurado obligatoriamente con una clave segura (ver estándar: Creación de contraseñas para usuarios) mediante el mecanismo de acceso WPA (Wi-Fi Protected Access) para las red inalámbricas de uso específico como son:
  - Escuela Militar de Ingeniería
  - Dirección Nacional de Informática
  - Video Conferencia
  - Salas de Reuniones

- ✓ Las claves de las redes inalámbricas protegidas podrán ser cambiados por petición de un representante del Departamento y/o Sección a la que pertenece la red.

- ✓ El administrador de la red inalámbrica deberá cambiar las claves de acceso a la red cada 3 meses e informarle a cada departamento.

- ✓ Realizar inspecciones físicas periódicas y emplear herramientas de gestión de red para revisar la red rutinariamente y detectar la presencia de puntos de acceso no autorizados.

- ✓ La instalación de un Access Point sin autenticación deberá ser solicitada al Jefe de Sección de la Dirección Nacional de Informática.

- ✓ Conjuntamente con el Oficial de Seguridad y el Jefe del Departamento de Tecnologías de la Información, deberá evaluar los riesgos a los que está expuesta la información que va a fluir en este canal inseguro. Si el riesgo es aceptable el administrador de la WLAN procederá a instalar el Access Point sin

autenticación, caso contrario se habilitará la autenticación.

3.1.9.4 Monitoreo

- ✓ El administrador de la red deberá estar monitoreando:
  - Los equipos activos de red
  - Los enlaces de: Internet, centros regionales o asociados, videoconferencia y voz sobre IP.
- ✓ Cada administrador de los servicios y equipos activos deberá proporcionar al administrador de la red la información que se solicite en la plantilla Configuración de Alarmas (ver anexo: Plantillas: Solicitud de Información para Configuración de Alarmas) para ser registrado en el monitoreo y aviso de alarmas que ofrece las herramientas de monitoreo.
- ✓ El administrador de la red deberá configurar en la herramienta de monitoreo que los avisos de alarmas llegue por correo electrónico o SMS.
- ✓ Los tipos de alarmas que se deberán configurar son los siguientes:
  - Ping: saturación
  - Traps: anomalías
  - Host down: pérdida de conectividad
  - Almacenamiento: almacenamiento saturado
- ✓ El monitoreo deberá ser habilitado las 24 horas x 7 días por los enlaces, equipos activos y servidores.
- ✓ El administrador de la red deberá evaluar la capacidad de los enlaces semestralmente, con los administradores de las aplicaciones involucradas.
- ✓ El administrador de la red deberá contactarse inmediatamente con el proveedor del servicio cuando haya pérdida de enlace (ver anexo: Asignaciones: Proveedores de Enlaces)

4. Control de cumplimiento y sanciones

En caso de existir incumplimiento de la presente Política de Seguridad de la Información por parte de un trabajador de la Universidad, se comunicará al Departamento de Recursos Humanos para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a más de las responsabilidades civiles y penales a que hubiere lugar.

CONFIGURACIÓN DE EQUIPOS COMPUTACIONALES

Instalación y configuración de básica de equipos computacionales

- ✓ Instalación del sistema Operativo con ultimo Services Pack
  - Excepcion: aplicaciones que no son soportadas por el ultimo Service Pack
- ✓ Instalación de Drives de Audio, Video y red.
- ✓ Instalación de Antivirus y actualización.
- ✓ Instalación de Software básico.
  - Microsoft Office.
  - Adobe Profesional
  - Win zip.
  - Win rar.
- ✓ Activación de Firewall
- ✓ Activación de IP v4 y IP v6.
- ✓ Configuración de nombre del equipo y nombre de dominio (ver estándar: Nombre de equipo y grupo de trabajo).
- ✓ Configuración de Zona horario (GT +5)
- ✓ Configuración del Proxy en caso de ser necesario.
- ✓ Configuración del Nombre de equipo compuesto por:
  - Edificio o Unidad Académica
  - Departamento o Sección.
  - Número.
- ✓ Configuración del Grupo de trabajo: emi.edu.bo

LÍNEA BASE DE SERVIDORES

- ✓ Instalación y configuración Básica de Servidores
- ✓ Instalación del Sistema Operativo con la última actualización del sistema.
- ✓ Instalación de Antivirus y su actualización.
- ✓ Activación y configuración del Firewall.
- ✓ Configuración del nombre del equipo.
- ✓ Configuración estática de la red.
- ✓ Configuración de zona horaria.
- ✓ Desinstalación de Software y servicios innecesarios.
- ✓ Eliminación de archivos de instalación.
- ✓ Eliminación de cuentas por defecto.
- ✓ Cambiar el nombre del usuario de administración.
- ✓ Establecer contraseña segura para las cuentas de administración según estándar. Creación de contraseñas para administración (Política de Control de Accesos Lógicos)
- ✓ Documentar los servicios levantados en el equipo y el software instalado.

PLANTILLA

SOLICITUD DE INFORMACIÓN PARA CONFIGURACIÓN DE ALARMAS

DATOS GENERALES **Fecha _____**

Administrador Principal

Nombres Completos_____

Dirección de Correo Electrónico_____

Número de Teléfono Móvil_____

Administrador de Backup

Nombres Completos_____

Dirección de Correo Electrónico_____

Número de Teléfono Móvil_____

Servidor

Dirección IP interna	**Dirección IP externa**

Servicios a monitorear

Servicios a monitorear	**Puertos**	**Tipo de Alarma**

FORMATO DE SOLICITUD DE PERMISOS – SEGURIDAD EMI.

NOMBRE DEL RESPONSABLE……

JUSTIFICACIÓN……
……
……
……

PERIODO DE TIEMPO……..

DESCRIPCIÓN

IP ORIGEN	IP DESTINO	PUERTO
.....	.....	.....

ASIGNACIONES

PROVEEDORES DE ENLACES

ENLACE	PROVEEDOR	CONTACTO	TELEFÓN0
Terrestre	VIVA	Claudio Chacón	68215973
Terrestre	ENTEL	Patricio Andrade	72548632
Terrestre	TIGO	Gustavo Alarcón	73312483
Terrestre	AXES	Efrain Encarnación	68459731
Satelital	ENTEL	Patricio Andrade	71269842

POLÍTICAS DE CONTROL ACCESOS LÓGICOS

POLÍTICA DE CONTROL ACCESOS LÓGICOS

1. OBJETIVO

Proteger la información institucional, normando el acceso a través de los sistemas informáticos, considerando: perfiles, permisos, cuentas, contraseñas y protectores de pantalla.

2. ALCANCE

Las normas definidas en esta política cubren toda la información que se encuentra almacenada y gestionada en activos tecnológicos. Su cumplimiento es de carácter obligatorio para quienes necesitan hacer uso de a la misma.

3. RESPONSABILIDADES

- ✓ El Oficial de Seguridad Información estará a cargo de:
  - Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información.
  - Definir pautas de utilización de los activos de información institucionales para los usuarios de la Dirección Nacional de Informática.
  - Participar en el comité de control de cambios y aprobar o rechazar un cambio luego de poseer un informe de impacto de las áreas involucradas en el cambio.
  - Verificar el cumplimiento del procedimiento de control de cambios
  - Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, protección de puertos, subdivisión de redes, control de conexiones a la red, etc.
  - Autorizará el acceso remoto a la administración de servicios críticos de la Escuela Militar de Ingeniería y a datos sensibles, verificando que se adopten

todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes.

- ✓ Los administradores de los servicios junto con el Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), estarán encargados de identificar los riesgos a los cuales se expone la información con el objeto de:
  - o Definir el plan de acción que permita mitigar los riesgos encontrados en: los controles de accesos y autenticación.
  - o Definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.
- ✓ El Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, realizarán auditorias periódicas a los sistemas, los mismo que tendrán acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.
- ✓ El Departamento de Recursos Humanos se encargará de:
  - o Notificar al Oficial de Seguridad el cambio de rol, o la salida o ingreso de un empleado para que los administradores de los servicios procedan a eliminar/crear inmediatamente accesos y permisos a los sistemas informáticos.
  - o Emitir un reporte mensual al Oficial de Seguridad en el que se detalle todos los ingresos y salidas de personal.

4. DESCRIPCIÓN DE LA POLÍTICA

4.1 Normas y Disposiciones Generales

4.1.1 Consideraciones Generales

- ✓ Los Jefes de Departamento y/o secciones de la Escuela Militar de Ingeniería conjuntamente con el Dueño del Servicio tienen la responsabilidad de crear procesos formales para la gestión de usuarios de los sistemas informáticos, en los

cuales se debe considerar:

- Definición de roles y perfiles

✓ El rol está definido por la función que cumple un usuario dentro de un sistema.

✓ El perfil es la descripción detallada de las transacciones que un usuario puede realizar en un sistema. En definitiva son los privilegios con los que cuenta un usuario.

- Procedimiento de autorización, acceso y nivel de privilegios en los sistemas.

- Procedimiento de entrega de usuarios y claves a los sistemas de manera adecuada y segura.

✓ Cada administrador de servicios conjuntamente con el Dueño del Servicio deberán definir el flujo de autorización y procedimiento de creación de usuarios considerando: las solicitudes y autorizaciones, roles y perfiles.

✓ El nombre de usuario debe estar creado según el estándar definido (Ver estándar: Creación de cuentas).

4.1.2 Gestión de Accesos de Usuarios

4.1.2.1 Registro de Usuarios

✓ Los Jefes de Departamento de la Dirección Nacional de Informática, conjuntamente con el Dueño del Servicios deben definir el flujo de autorización para el acceso y el nivel de privilegios en los sistemas.

✓ El otorgamiento de roles y perfiles de usuario deberá ser definido de acuerdo al principio del mínimo privilegio.

✓ Todo el personal de la Escuela Militar de Ingeniería, tendrá asignado un nombre único de usuario y contraseña para acceder a los sistemas informáticos permitidos según su perfil. Si existe alguna excepción, esta debe ser autorizada por el Oficial de Seguridad.

- ✓ Los administradores de servicios deberán otorgar acceso a los diferentes sistemas siempre que el solicitante posea la respectiva autorización.

- ✓ Los administradores de cada servicio deberá mantener actualizado sus registros de usuario. Así como una bitácora relacionada a accesos lógicos de los mismos. Se debería mantener opciones y reportes automáticos para obtener los listados necesarios de las cuentas y privilegios de los usuarios en los sistemas.

4.1.3 Gestión de privilegios

- ✓ Cada aplicación debe gestionar el nivel de privilegios que tienen los usuarios dentro del sistema informático.

- ✓ Todo el personal de la Escuela Militar de Ingeniería, debe estar asociado a un rol/perfil en los sistemas informáticos de acuerdo a las actividades que realiza.

- ✓ Es responsabilidad de los administradores de servidores y servicios, la correcta administración de las cuentas de acceso, el otorgamiento de privilegios de acuerdo a las autorizaciones que se especifiquen en el flujo de autorización.

4.1.4 Seguimiento y Auditoria

- ✓ Los servicios de TI serán auditados por el Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI),.

- ✓ Se deberá activar el registro de auditoría en los servicios, servidores, equipos de comunicación y sistemas críticos, para aquellos usuarios que mantengan privilegios administrativos.

- ✓ Los registros de auditoria deberán ser eliminados periódicamente, para que no afecten el rendimiento de los servicios.

4.1.5 Gestión de Contraseñas de Usuario

- ✓ Se debe aplicar el estándar de creación de contraseñas seguras para el acceso de usuarios finales a los diferentes sistemas. (ver estándar: Creación de Contraseñas para usuarios finales).

- ✓ Se debe aplicar el estándar de creación de contraseñas seguras para el acceso a la administración de los sistemas, servidores o equipos de comunicación (ver estándar: Creación de Contraseñas para administración).

- ✓ Las claves de acceso a los sistemas deben ser protegidas mediante controles criptográficos.

- ✓ Los sistemas críticos: Sistema de Gestión Académica y Administrativa deben estar configurados de tal manera que:

    - o Permitan al usuario cambie su clave obligatoriamente cuando ingresa por primera vez al sistema.

- ✓ Se debe utilizar un sistema de gestión de usuarios que permita:

    - o Bloquear al usuario en la aplicación por 15 minutos luego de 3 intentos fallidos.

    - o Cambiar la contraseña al menos cada 6 meses para los usuarios finales, con excepción del sistema Administrativo que debe ser cambiado cada 3 meses. Y cada 3 meses para las cuentas administradores de servicios, servidores o equipos de comunicación.

    - o Verificar la robustez de las contraseñas según estándar establecido

- ✓ Se debe cambiar inmediatamente la contraseña al sospechar o detectar que ha sido comprometida.

- ✓ Todo el personal de Escuela Militar de Ingeniería, debe mantener sus equipos de trabajo diario como: PC, PORTATIL con contraseña de acceso segura cuando no estén trabajando en ellas.

4.1.6 Revisión de los Derechos de Acceso de los Usuarios

- ✓ Los Jefes de Departamento de la Dirección Nacional de Informática serán responsables de ejecutar una depuración de los derechos y privilegios de acceso de los colaboradores a su cargo, tanto en los sistemas informáticos,

dispositivos de red, bases de datos, servidores. Esto se lo debe realizar mínimo dos veces al año

- ✓ Los administradores de servicios deberán reportar trimestralmente al Oficial de Seguridad los derechos y privilegios de acceso de los usuarios con altos privilegios en los activos de información.

5. CONSECUENCIAS Y SANCIONES

En caso de existir incumplimiento de la presente Política de Seguridad de la Información por parte de un trabajador de la Escuela Militar de Ingeniería, se comunicará al Departamento de Recursos Humanos para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a más de las responsabilidades civiles y penales a que hubiere lugar.

CREACIÓN DE CARACTERES

- La contraseña debe tener una longitud mínima de seis caracteres.
- La contraseña debe ser una combinación de letras y números.
- La contraseña no debe estar conformada por nombres o palabras comunes.

CREACIÓN DE CONTRASEÑAS PARA ADMINISTRACIÓN

- La contraseña debe tener una longitud mínima de ocho caracteres.
- La contraseña debe ser una combinación de letras mayúsculas, minúsculas números y caracteres especiales.
- La contraseña no debe estar conformada por nombres o palabras comunes.

CREACIÓN DE CUENTAS

El nombre de usuario estará conformado por:

- ✓ Letra del primer nombre.
- ✓ Letra del segundo nombre.
- ✓ Apellido.
- ✓ En caso que ya exista el nombre de usuario agregar secuencia de números.
- ✓ Ejemplo
    - **Usuario:** Erick Rolando Palenque Rios
    - **Cuenta de Usuario:** erpalenque (si ya existe el usuario se cabiaria erpalenque1).

POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

1. OBJETIVO

- ✓ Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas informáticos.
- ✓ Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

2. ALCANCE

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base.

3. RESPONSABILIDADES

- ✓ El Oficial de Seguridad, definirá los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.
- ✓ El Oficial de Seguridad definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos.
- ✓ Así mismo, el Oficial de Seguridad las siguientes funciones:
    - o Definir los procedimientos de administración de claves.
    - o Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
    - o Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

- Control Interno realizará auditorias para verificar el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

4.- DESCRIPCIÓN DE LA POLÍTICA

4.1 Normas y disposiciones generales

4.2 Requisitos de seguridad de los sistemas informáticos

4.3 Consideraciones generales

- ✓ La definición de requerimientos deben estar regidos por la Política institucional de definición de requerimientos para sistemas de información.
- ✓ Los sistemas informáticos deben contar con un módulo de gestión de la aplicación, en el que se contemple:
    - o Gestión de usuarios (creación, eliminación, desactivación de usuarios, entre otros)
    - o Gestión de privilegios

4.3.1 Análisis y especificaciones de los requisitos de seguridad.

4.3.1.1 Etapa de Análisis

- ✓ Se debe incorporar los requerimientos referentes al cumplimiento con la normativa local (CPE, Ley 164 de Telecomunicaciones, Tecnologías de Información y comunicación, Ley 195 Agenda Patriótica, Ley 1322 Derechos de Propiedad intelectual, etc.).
- ✓ Se debe identificar el tipo de información que se trasmitirá y procesará (pública, privada, datos financieros, contraseñas, etc).
- ✓ La aplicación debe proporcionar registros de auditoría.

4.3.1.2 Etapa de Diseño

- ✓ En esta etapa se definirá el diseño de autorización (definición de roles, permisos y privilegios de la aplicación).

- ✓ Se debe realizar el diseño de la forma de autenticación de los usuarios así como los mecanismos para evitar posibles ataques.

4.3.1.3 Etapa de Codificación

- ✓ En esta etapa se realizará la identificación de los tipos de vulnerabilidades las cuales se las puede dividir en dos:
  - o Vulnerabilidades clásicas: dentro de estas vulnerabilidades tenemos errores de manejo de sesiones, desbordamiento, denegación de servicios.
  - o Vulnerabilidades funcionales: estas vulnerabilidades se refieren a la funcionalidad de la aplicación con respecto a los requerimientos de la aplicación (Que haga lo que tiene que hacer)
- ✓ Se verificará que los datos de entrada sean los mismos que los de salida.

4.3.1.4 Etapa Testing

- ✓ Se deberá evaluar los controles definidos en las etapas anteriores.
- ✓ Se debe crear un proceso formal de testing de seguridad para probar la aplicación con escenarios no planificados incluyendo:
  - o Valores fuera de rango
  - o Valores de tipo incorrecto
  - o Acciones fuera de orden

4.3.2 Procesamiento Correcto en las Aplicaciones

4.3.2.1 Validación de Datos

- ✓ Elaborar procedimientos formales para la validación de los datos de entrada, procesamiento y salida de los sistemas.
- ✓ Una vez culminadas las pruebas a los sistemas se debe elaborar un informe formal de todas las actividades realizadas y los resultados obtenidos.

4.3.3 Seguridad de los Archivos del Sistema

4.3.3.1 Controles del Software en Explotación

- ✓ Toda aplicación desarrollada por el Departamento de Desarrollo de Sistemas o por un tercero tendrá un único Responsable técnico designado formalmente por el Jefe del Departamento de Desarrollo de Sistemas.

- ✓ Los programadores o analistas de desarrollo y mantenimiento de aplicaciones no pueden acceder a los ambientes de producción.

- ✓ Todas las modificaciones que se realicen a algún sistema informático en el ambiente de producción deben estar regidas por la Política de Control de Cambios.

4.3.3.2 Protección de Datos de Pruebas del Sistema

- ✓ Los datos que son utilizados para pruebas no pueden ser datos de las bases de datos que se encuentran en producción.

- ✓ Si se realizan copias de bases de datos operativas se deberá autorizar formalmente y llevar un registro de las autorizaciones realizadas.

4.3.3.3 Control de acceso al código fuente de los programas

- ✓ En la Dirección Nacional de Informática debe existir una persona responsable de administrar y custodiar los programas fuentes, la misma que debe:

- ✓ Proveer los programas fuentes solicitados para su modificación.

- ✓ Llevar un registro formal y actualizado de todos los programas fuentes en uso en el que se debe incluir (nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y estado: en modificación, en producción).

- ✓ Administrar las distintas versiones de una aplicación.

- ✓ Asegurar que un mismo programa fuente no sea modificado simultáneamente por

más de un desarrollador.

- ✓ Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, caso contrario se deberá rechazar el pedido.

- ✓ El administrador de programas fuentes no puede modificar el código de los programas fuente bajo su custodia.

- ✓ Todo programa ejecutable en producción debe tener un único programa fuente asociado a este.

- ✓ Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.

- ✓ Se debe realizar copias de respaldo de los programas fuentes cumpliendo requisitos de seguridad especificados en la sección Política de seguridad en las comunicaciones y operaciones.

4.3.4 Seguridad de los Procesos de Desarrollo y Soporte

4.3.4.1 Procedimientos de Control de Cambios

- ✓ Se debe mantener un control de versiones para todas las actualizaciones de software.

- ✓ La documentación se debe mantener actualizada para cada cambio implementado, tanto en los manuales de usuario como en la documentación operativa.

- ✓ Los requisitos de seguridad que debe cumplir el software deben ser revisados por el Oficial de Seguridad.

- ✓ Los propietarios de la información deberán autorizar los cambios si estos afectan al procesamiento de la información de un determinado sistema.

- ✓ Las actividades relativas al cambio deben efectuarse en el ambiente de

desarrollo.

- ✓ Se debe garantizar que la discontinuidad de las actividades sea mínima durante la implementación de cambios y que los procesos involucrados no sean alterados.

- ✓ Regirse a la Política de Control de Cambios

4.3.5 Externalización del desarrollo de software

4.3.5.1 Para la Tercerización del Desarrollo de Software

- ✓ Se establecerán acuerdos de Licencias, propiedad de código y derechos conferidos (Derechos de propiedad intelectual)

- ✓ Si se intercambia información que es confidencial, se deberá generar un documento/acuerdo de confidencialidad entre la Escuela Militar de Ingeniería y el proveedor de servicios, ya sea como parte del contrato de tercerización en sí o un acuerdo de confidencialidad por separado.

- ✓ Se debe verificar el cumplimiento de las condiciones de seguridad contempladas en la política de responsabilidad de la seguridad de la información.

- ✓ Se establecer como requerimiento a la calidad del código.

- ✓ Se establecerá procedimientos para la certificación de la calidad del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.

- ✓ Deben regirse a las política establecidas por el área de Soluciones de Negocio:

    - o Política de documentación de desarrollo de sistemas de información (programación)

    - o Política de documentación de proyectos de desarrollo y/ó implementación de sistemas de información

- Política de definición y revisión de pistas de auditoría
- Política de seguridad de la información en servicios tercerizados
- Política de definición de multas y sanciones
- Política de documentación de acuerdo de responsabilidad.

5. Consecuencias y sanciones

En caso de existir incumplimiento de la presente Política de Seguridad de la Información por parte de un trabajador de la Escuela Militar de Ingeniería, se comunicará al Departamento de Recursos Humanos para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a más de las responsabilidades civiles y penales a que hubiere lugar.

POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

1. OBJETIVO

Establecer procedimientos para el reporte de incidentes, para garantizar que los incidentes, eventos y debilidades en la seguridad de los sistemas informáticos se comuniquen oportunamente y sean atendidos de la mejor manera.

Garantizar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad.

Establecer responsabilidades y procedimientos para el manejo de incidentes de seguridad informática de manera efectiva.

2. ALCANCE

La presente política regirá para todo el ambiente de tecnología de la información y sus actores, tanto operadores, administradores y beneficiarios de la UTPL.

3. DESCRIPCIÓN DE LA POLÍTICA

3.1 Normas y Disposiciones Generales

3.1.1 Consideraciones Generales

- ✓ El CSIRT, debe hacer conocer al personal de la Escuela Militar de Ingeniería, los contactos a los que puede comunicarse para el reporte de incidentes de seguridad informática.
- ✓ Es responsabilidad del CSIRT, es hacer conocer al personal de la Escuela Militar de Ingeniería, sobre la existencia del Equipo de respuesta a incidentes de seguridad informática (CSIRT).
- ✓ El CSIRT-EMI debe elaborar y publicar los datos estadísticos acerca de los incidentes de seguridad que se producen en la Escuela Militar de Ingeniería.
- ✓ La Seccion de Soporte Técnico de la Dirección Nacional de Informática escala al CSIRT- EMI todos los incidentes de los usuarios que coincidan con la categorización de incidentes del CSIRT-EMI y que no consten en el catálogo de

servicios de Soporte Técnico.

- ✓ Todas las actividades concernientes al manejo de incidentes se realizan en base a los procedimientos definidos para el manejo de incidentes.

- ✓ Por ningún motivo se debe utilizar métodos ilegales para la resolución de un incidente, se debe tomar en cuenta que estos métodos no ocasionen acciones legales posteriores en contra de la Escuela Militar de Ingeniería.

- ✓ Es importante tomar en cuenta la asesoría legal para las acciones a realizar en incidentes relacionados a: suplantación de identidad, acceso a información confidencial e incidentes relacionados con ingeniería social.

- ✓ Toda la información relativa a los incidentes reportados, deben ser manejada con total confidencialidad, la clasificación de la información se realiza de acuerdo a la Política de Gestión de Activos.

- ✓ Se debe tomar en cuenta mecanismos para la recolección de evidencia durante el proceso de respuesta a incidentes, lo que servirá de recurso necesario, en el caso de instancias legales.

3.1.2 Categorización de Incidentes

En el Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), se ha catalogado como incidente a cualquier evento que esté directamente relacionado con los sistemas y servicios de la Escuela Militar de Ingeniería de acuerdo a las siguientes categorías:

CATEGORIZACIÓN DE INCIDENTES CSIRT- EMI

SEVERIDAD (GRAVEDAD)	CLASE DE INCIDENTE	TIPO DE INCIDENTE
Grave - Medio - Leve	Código Malicioso	• Virus • Worm • Trojan
Medio - Leve	Denegación de Servicios (Disponibilidad)	• Ataques DOS (denegación de servicios) • Ataques Dsos (denegación de servicios distribuidos)
Leve	Contenido Abusivo	Acoso
Grave - Medio - Leve	Recopilación de Información	Ingeniería Social
		Suplantación de Identidad
		Scanning (Escaneo)
		Detección de Vulnerabilidades
Medio - Leve	Intentos de Intrusión	Explotación de Vulnerabilidades Conocidas
		Intentos de acceso a un sistema
Grave - Medio - Leve	Ataques de Autenticación	Ataques por fuerza bruta Exploits
Grave - Medio - Leve	Mal uso de Recursos Tecnológicos	Violación de Políticas
Grave - Medio - Leve	Acceso no Autorizado	Accesos no autorizados Robo de Información Borrado de Información Alteración de la Información

3.1.3 Comunicación de Incidentes y Eventos en la Seguridad de la Información

3.1.3.1 Reporte de Incidentes de Seguridad

Todo el personal Escuela Militar de Ingeniería, debe conocer los procedimientos para realizar el reporte de incidentes, eventos y vulnerabilidades de seguridad de la información que puedan tener impacto en la seguridad de los sistemas que administra (Ver Procedimiento: Reporte de Incidentes).

- ✓ Todo el personal Escuela Militar de Ingeniería debe informar de cualquier incidente o evento de seguridad informática al Área de Soporte Técnico de acuerdo al proceso establecido.

  (Ver Procedimiento: Reporte de Incidentes – Sección: Usuarios que reportan a Soporte Técnico).

- ✓ Los Administradores de Servidores deben realizar el reporte de incidentes y eventos de seguridad informática directamente al Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), de acuerdo a los procedimientos definidos. (Ver Procedimiento: Reporte de Incidentes – Sección: Administradores de Servidores que reportan al CSIRT- EMI).

3.1.3.2 Reporte de vulnerabilidades de Seguridad

El reporte de vulnerabilidades es responsabilidad del Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), en el que a través de escaneos de vulnerabilidades y test de penetración se hace conocer al administrador de servidores el estado de seguridad de los equipos que administra.

- ✓ Todos los administradores de servidores y usuarios de sistemas deben notificar cualquier debilidad observada en los sistemas que administra.

- ✓ El Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), previo acuerdo con los administradores de servidores deberá establecer un cronograma para realizar el escaneo de vulnerabilidades y test de penetración a los servidores de la Escuela Militar de Ingeniería, de acuerdo a servidores críticos

y no críticos.

- ✓ Los administradores pueden solicitar que se realice el escaneo al equipo que administran en base al formato establecido. (Ver Estándar: Formulario para solicitar el Escaneo de Vulnerabilidades).

3.1.3.3 Responsabilidades del Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI)

Es responsabilidad del Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), de:

- ✓ Realizar el envío de reportes y escaneos de vulnerabilidades de los servidores de la Escuela Militar de Ingeniería de acuerdo al cronograma previamente establecido con los administradores.

- ✓ El monitoreo de IDS e IPS se lo realizará de forma diaria, en el caso de que se registren alertas críticas, se enviará al Administrador del equipo, un reporte en el que se indique, vulnerabilidades críticas, puertos abiertos, y las alternativas de solución. Esto se realizará utilizando el formato de reporte correspondiente. (Ver Estándar: Formulario para el Reporte de Vulnerabilidades y Formulario de Reporte de Incidentes).

- ✓ Reportar los incidentes de seguridad que sean notificados al área por entes internos o externo a los respectivos implicados con el incidente.

- ✓ Coordinar el plan de acción para mitigar el incidente con el administrador del servicio afectado y/o los involucrados.

- ✓ Dar seguimiento a la ejecución del plan de acción establecido para los incidentes de seguridad y reportar su avance semanalmente al Oficial de Seguridad.

3.3.3.4 Escaneos de Vulnerabilidades a los Sistemas

- ✓ Los escaneos de vulnerabilidades a los sistemas, deben ser realizados de acuerdo a:

  - o Sistemas Críticos

Se realizará el escaneo de vulnerabilidades a los sistemas críticos cada tres (3) meses y cuando el administrador lo solicite.

- Sistemas no Críticos

Se realizará el escaneo de vulnerabilidades a los sistemas no críticos cada seis (6) meses, y cuando el administrador lo solicite.

- ✓ La criticidad de los sistemas es definida por los Jefes de Departamento y/o Secciones.

3.3.3.5 Responsabilidades del Administrador de Servidores

- ✓ Los administradores de servidores, al momento de recibir el reporte de vulnerabilidades enviado, tienen un plazo máximo de cinco días para comunicar al Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), que recibieron el reporte y que el mismo será atendido en el plazo señalado por los administradores.

- ✓ Los administradores de servidores deben notificar al Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), sobre el avance del plan de acción para remediar y corregir los incidentes o vulnerabilidades reportadas.

- ✓ Por ninguna circunstancia los administradores pueden proceder a realizar pruebas de las posibles vulnerabilidades encontradas en los sistemas de producción, si se requiere estas pruebas, se deben ser hechas en un ambiente de pruebas.

- ✓ El administrador en base a la información recibida con el apoyo del Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), debe descartar las vulnerabilidades que se considere como falsos positivos.

Para las demás vulnerabilidades se deberá dar solución en base a las sugerencias descriptas en el reporte enviado.

- ✓ El administrador de servidores puede solicitar la colaboración del Centro de

Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), para la revisión e indicaciones de los reportes de vulnerabilidades y cualquier otra información, concerniente al tema de Seguridad.

- ✓ Si el Administrador no envía los reportes en el tiempo indicado se procederá con las siguientes acciones:

  - **Informe Enviado al Jefe de Departamento o Sección**

    - ✓ Si en los treinta (30) días siguientes a la emisión de los reportes, no se emite la respuesta al informe enviado, se enviará nuevamente el reporte, adjuntando un oficio dirigido al Jefe de Departamento o Sección.

    - ✓ Luego del informe emitido al Jefe de Departamento o Sección, el administrador tiene un plazo de veinte (20) días laborables para enviar el informe con las correcciones realizadas.

  - **Notificación enviada por parte de Dirección Nacional de Operaciones**

    Si luego de enviar la notificación al Jefe de Departamento o Sección, no se ha recibido respuesta a los reportes enviados, se enviará un oficio firmado por la Dirección Nacional de Informática, en la que se deslinda la responsabilidad del Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), y en la que el único responsable de cualquier incidente de seguridad con los equipos es el administrador del mismo.

3.3.4 Gestión de Incidentes y Mejoras en la Seguridad de la Información

3.3.4.1 Respuesta de Incidentes

- ✓ Una vez que se reciba un reporte de incidente de seguridad en el Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), el afectado recibirá un acuse de recibo indicando que el reporte ha sido recibido y será resuelto en el menor tiempo posible.

- ✓ La respuesta a Incidentes por parte del Departamento de Asistencia Técnica de la Dirección Nacional de Informática y el Centro de Respuestas a Incidentes de

Seguridad Informática (CSIRT - EMI), debe realizarse en base a los procedimientos establecidos. (Ver Procedimiento: Respuesta de Incidentes de Seguridad Informática)

- ✓ Una vez resuelto el incidente, se enviará un informe ejecutivo al personal que informó del incidente y a la Dirección Nacional de Informática, o Jefes De Departamentos y/o Secciones que requieran la información del incidente.

- ✓ Se debe realizar un informe técnico, el mismo que será realizado en base al formato establecido, este informe queda archivado en el Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), y es entregado en el caso de que sea requerido por la parte afectada (Ver Estándar: Formulario de Respuesta a Incidentes). Se debe informar constantemente acerca de la resolución del incidente a las personas que reportaron el mismo. Si la persona lo solicita se envía el reporte técnico de la resolución del incidente, caso contrario, solamente se envía el informe ejecutivo de resolución del incidente reportado.

- ✓ Los reportes de incidentes y vulnerabilidades, y los informes ejecutivos son de carácter confidencial.

- ✓ Se deberá enviar mensualmente al Oficial de Seguridad y a la Dirección Nacional de Informática, las estadísticas de los incidentes y vulnerabilidades atendidas por el Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI).

4. CONTROL DE CUMPLIMIENTO Y SANCIONES

En caso de existir incumplimiento de la presente Política de Seguridad de la Información por parte de un trabajador de la Escuela Militar de Ingeniería, se comunicará al Departamento de Recursos Humanos para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a más de las responsabilidades civiles y penales a que hubiere lugar.

REPORTE DE INCIDENTES DE SEGURIDAD INFORMÁTICA

Usuarios que reportan a Soporte Técnico

- El usuario debe ponerse en contacto con personal del Departamento de Asistencia Técnica de la Dirección Nacional de Informática para reportar los incidentes de seguridad.

- El Departamento de Asistencia Técnica de la Dirección Nacional de Informática, atenderá los reportes de incidentes de seguridad que se encuentran en su base de conocimiento, caso contrario, el reporte se escala al Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI),.

Administradores de Servidores que reportan al Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI),

Los incidentes de seguridad informática pueden ser reportados por los siguientes medios:

- El formulario debe ser enviado al Equipo Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI),. (Ver Estándar Técnico: Reporte de Incidentes)

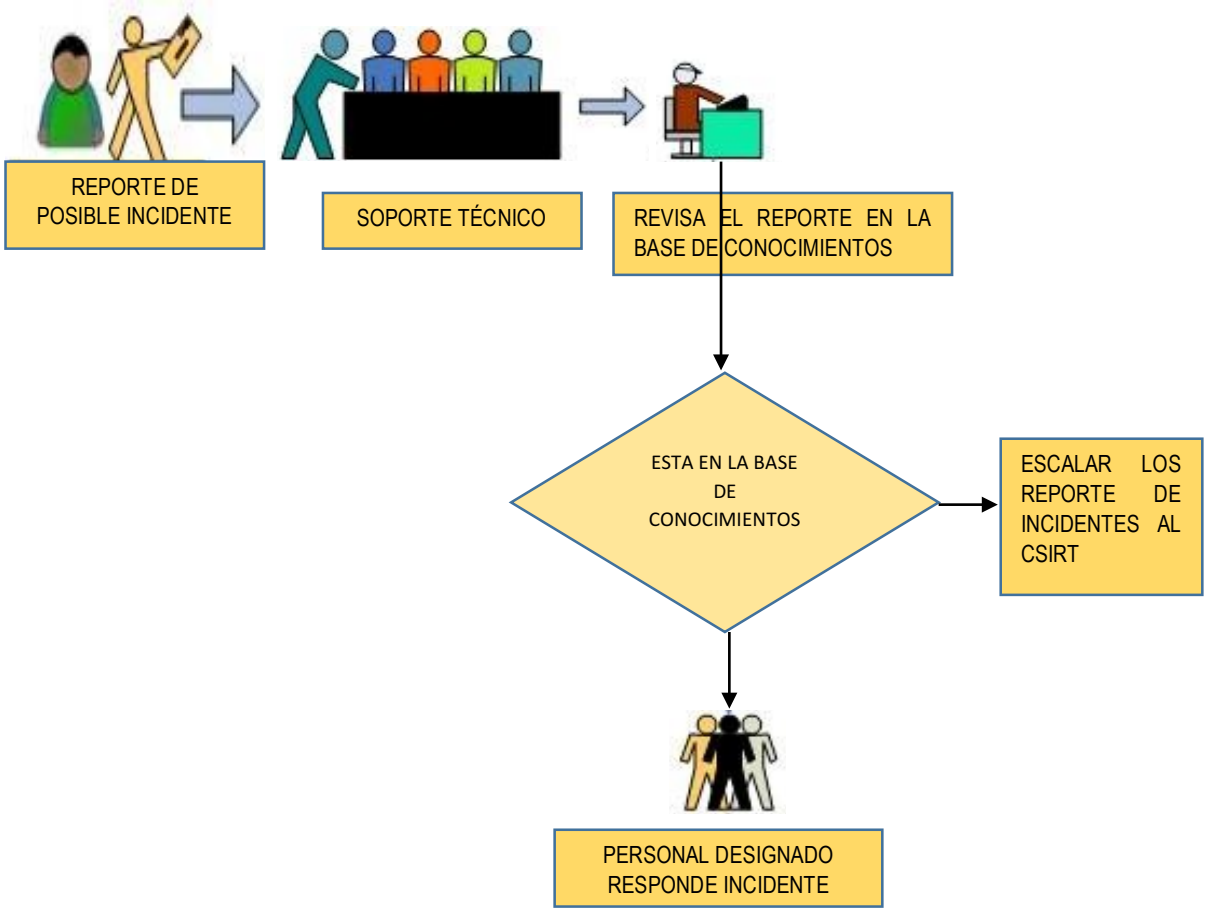
- Personalmente.

- Via Web a crear: www.emi.edu.bo/csrit-emi (Sección: Reporta tu Incidente)

Una vez que se ha recibido el reporte de incidente en el Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), se envía al usuario un acuse de recibo de que el informe se recibió y será atendido en el menor tiempo posible.

- Luego de recibir el reporte de incidente por parte del usuario, el Departamento de Asistencia Técnica de la Dirección Nacional de Informática, revisará si el incidente reportado está en la base de conocimientos y brindar la solución al incidente reportado.

- Si el incidente no está en la base de conocimiento de la Departamento de Asistencia Técnica escala al Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI),.



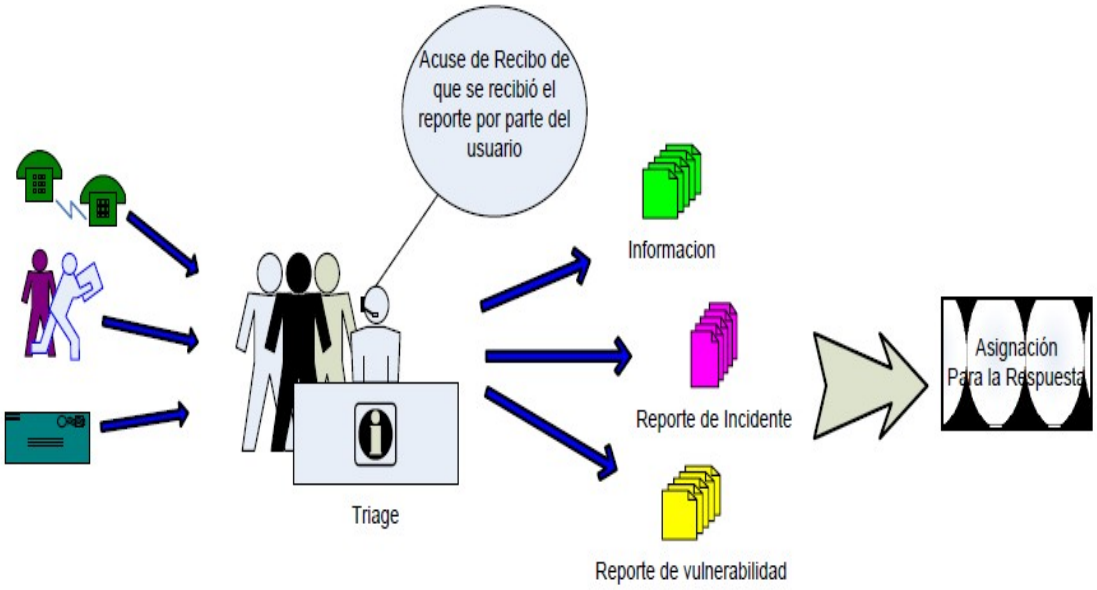
Respuesta al Incidente – CSIRT - EMI

- Cuando se reciba el reporte de incidentes en el Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), se debe realizar el procedimiento definido en para la Gestión de Incidentes, el primer proceso a realizar es triage de la

información recibida.

- En el proceso de triage se determina si el reporte recibido corresponde a un incidente, vulnerabilidad o información general.

✓ Si se determina que es un incidente, se asigna el tiempo y recursos para su atención y respuesta.



Proceso de Respuestas a incidentes

- Si el reporte corresponde a una vulnerabilidad, se brinda información y colaboración para mitigar el problema, (búsqueda de parches, e información general).

- Los procesos que se realizan durante la respuesta al incidente deben ser realizados en base al procedimiento para la Gestión de Incidentes realizada.

FORMULARIO DE NOTIFICACIÓN DE INCIDENTES

REPORTE CSIRT

Fecha:

Información de Contacto

Nombre:	Nombre de quién reporta el incidente
Dependencia:	
Correo Electrónico:	
Extensión:	

Equipos o Servicios Afectados

Indique los equipos, servicios o personas afectadas por el incidente

Explique brevemente el Trabajo que desarrolla en el Equipo que usted maneja, (indique: Sistema Operativo, Programas Instalados, etc.):

Origen del Incidente

Realice una breve descripción de la forma en la que descubrió el incidente

Antecedentes

Indique un resumen de cómo descubrió el incidente Si es necesario incluya una sección de anexos.

NOTA:
Toda la información que usted reporte será manejada de manera confidencial, la información recibida solamente será publicada bajo su consentimiento.

Información de Contacto CSIRT- EMI Email: csirt-emi@emi.edu.bo

Teléfono: 2437891 ext. 152

PLANILLA DE SOLICITUD DE ESCANEO DE VULNERABILIDADES

Este formulario, es utilizado por los administradores, para solicitar el escaneo de vulnerabilidades a los equipos que administran.

Este reporte debe ser enviado al CSIRT – EMI csirtemi@emi.edu.bo

Información de Contacto

Nombre:	
Dependencia:	
Correo Electrónico:	
Extensión:	

Información del Equipo a ser analizado

"Tabla de Registro de Equipo"			
Servidor			
Dirección IP			
Sistema O.		**Fecha**	
Observaciones			

Información adicional:

En esta Sección indique los riesgos o vulnerabilidades que ha identificado.

Id	Vulnerabilidad

SECCIÓN DE RESPUESTA POR PARTE DEL CSIRT- EMI.

Esta sección es utilizada por el CSIRT- EMI.

"Tabla de registro de Vulnerabilidades"			
Servidor			
Dirección IP		**Nombre de dominio**	
Sistema O.		**Fecha**	

Puerto	Protocolo	Servicio	Detalles del servicio

Id	Vulnerabilidad	Correctivo	Estado

FORMULARIO PARA EL REPORTE DE VULNERABILIDADES

Este formulario, es utilizado por el CSIRT – EMI, para realizar el reporte de vulnerabilidades a los Administradores de Servidores.

PLANTILLA DE REPORTE DE VULNERABILIDADES

REPORTE VUL.

Fecha:

Información de Contacto

Nombre:	
Dependencia:	
Correo Electrónico:	
Extensión:	

El reporte adjunto tiene como finalidad, darle a conocer el estado de su equipo en cuanto a vulnerabilidades y puertos abiertos.

Solicitamos su colaboración, en cuanto a la revisión de la información adjunta.

Cualquier información que usted requiera, no dude en contactarse con el Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI),.

Solicitamos revisar el estado de su equipo y cerrar los puertos que no utilice, luego de esto se realizará un nuevo escaneo para determinar el estado actual del equipo.

Nota:

Se adjunta el reporte de vulnerabilidades.

DATOS DEL EQUIPO Y PUERTOS ESCANEADOS

Observaciones:

En esta sección indique en forma resumida, los puertos abiertos que reportan vulnerabilidades más críticas.

"Tabla de registro de Vulnerabilidades"			
Servidor			
Dirección IP			
Sistema O.		**Fecha**	

Puertos Escaneados	Protocolo	Servicio	Detalles del Servicio

Información Adicional

En esta sección indique en forma resumida, cualquier información adicional en cuanto a las alertas encontradas, si es necesario realice un mayor detalle de las mismas, indicando las posibles soluciones.

SECCIÓN DE RESPUESTA POR PARTE DEL ADMINISTRADOR

La tabla que se indica a continuación debe ser enviada al Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), indicando los correctivos tomados para cada una de las alertas reportadas.

"Tabla de Registro de Vulnerabilidades "			
Servidor			
Dirección IP			
Sistema O.		**Fecha**	
Vulnerabilidad	**Protocolo**	**Correctivo**	**Estado**

Importante

El plazo para que usted responda este reporte es de cinco días laborables, si en este tiempo no se es enviado el reporte con los correctivos al Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI), se enviará una notificación al Jefe de Departamento y/o Sección posteriormente, si no se recibe respuesta en un plazo de tres días, se enviará un aviso firmado por Dirección Nacional de Operaciones.

FORMULARIO DE RESPUESTA DE INCIDENTES

Fecha Ingreso de Reporte: REPORTE: CSIRT#

Fecha de Respuesta:

Información General

Nombre de las personas que envían este informe	
Correo Electrónico:	csirtemi@emi.edu.bo
Extensión:	543

Resumen del Incidente:

Indique un breve resumen del incidente atendido

Observaciones:

Indique cualquier información referente al incidente atendido.

RESPUESTA AL INCIDENTE

Tipo de Incidente: Escoja la opción que considere aplicable.

Acceso no autorizado		**Denegación de Servicios**	
Acceso no autorizado	☐	Tiempos de respuesta muy bajos sin razones aparentes	☐
Robo de Información	☐		
Alteracion de la información	☐	servicios internos inaccesibles sin razones aparentes	☐
Intentos recurrentes de acceso no autorizado	☐		
Abuso y/o mal uso de servicios informaticos que requieren autenticación	☐	Servicios externos inaccesibles sin razones aparentes	☐
Mal uso de Recursos Tecnologicos		**Código Malicioso**	
Violación de normas de acceso a internet	☐	Vírus	☐
Mal uso de correo electrónico	☐	gusanos	☐
Violación de normas y políticas de Seguridad	☐	troyanos	☐
		spam	☐
	☐	pishing	☐

Causas del Incidente:

1. **Resolución del Incidente**

Detalle toda la información referente a los pasos seguidos para la resolución del incidente.

2. **Soluciones para el Incidente Reportado**

(Indique si utilizó alguna metodología o soluciones anteriores)

3. **Medidas que se Deben Tomar Para Evitar que el Incidente Suceda Nuevamente:**

Indique las medidas de seguridad a implementar para que no ocurran incidentes similares.

_____ _____

Jefe del CSIRT – EMI **Sub Jefe CSIRT - EMI**

_____

Firma de persona que facilite datos para resolver incidente

POLÍTICA DE CUMPLIMIENTO

POLÍTICA DE CUMPLIMIENTO

1. OBJETIVO

Cumplir con las disposiciones legales y contractuales establecidas en la constitución de nuestro país a fin de evitar sanciones administrativas a la Escuela Militar de Ingeniería y/o al empleado que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

2. ALCANCE

Esta Política se aplica a todos los sistemas informáticos, normas, procedimientos, documentación, así como al personal de la Escuela Militar de Ingeniería.

3. RESPONSABILIDAD

- ✓ El Oficial de Seguridad cumplirá las siguientes funciones:
  - Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.
  - Realizar revisiones periódicas de todas las Secciones de la Dirección Nacional de Informática a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
  - Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.

4. DESCRIPCIÓN DE LA POLÍTICA

4.1 Cumplimiento de Requisitos Legales

4.1.1 Identificación de la Legislación Aplicable

- ✓ La Escuela Militar de Ingeniería por ser una institución educativa está sujeta al respeto y cumplimiento de las leyes señaladas en la Constitución Política y

demás normativas, en especial la relativa a:

- Ley de Comercio electrónico
- Derechos de propiedad Intelectual
- Código de Trabajo
- Nueva ley de Educación
- Código Tributario
- Código Penal
- Ley de Telecomunicaciones

4.1.2 Derechos de Propiedad Intelectual.

- ✓ Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software y datos que defina el uso legal de productos de información y de software.
- ✓ Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
- ✓ Todo software utilizado por la Escuela Militar de Ingeniería debe tener su respectivo registro de Licencia a excepción del software libre.
- ✓ Se verificará que sólo se instalen en los equipos de la Escuela Militar de Ingeniería, productos con licencia y software autorizado.
- ✓ El Departamento de Asistencia Técnica, deberá mantener un registro de las licencias de software con las que cuenta la Escuela Militar de Ingeniería.
- ✓ Se deberá conservar pruebas de evidencia de propiedad de licencias, discos maestros, manuales, etc.
- ✓ Se deberá elaborar y divulgar un procedimiento relacionado con la eliminación o

transferencia de software a terceros.

- ✓ Implementar controles para evitar el exceso del número máximo permitido de usuarios al uso de las licencias.

5. CONSECUENCIAS Y SANCIONES

En caso de existir incumplimiento de la presente Política de Seguridad de la Información por parte de un trabajador de la Escuela Militar de Ingeniería, se comunicará al Departamento de Recursos Humanos para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a más de las responsabilidades civiles y penales a que hubiere lugar.

POLÍTICA LICENCIAMIENTO DE SOFTWARE

POLÍTICA DE LICENCIAMIENTO DE SOFTWARE

1. OBJETIVO

Regularizar el uso y gestión de licencias de software en la Escuela Militar de Ingeniería Escuela Militar de Ingeniería

2. NIVELES DE RESPONSABILIDAD

ROL O CARGO DEL RESPONSABLE	NIVEL DE RESPONSABILIDAD O FUNCIONES
Gestión de Servicios	• Mantener inventarios actualizados de: o Licencias existentes en la Universidad. o Licencias entregadas a usuarios. o Licencias disponibles. o • Generar reportes periódicos de gestión de licencias • Definir lineamientos y perfiles para la asignación de licencias. • • Ejecutar procesos de: o Relevamiento de información. o Regularización de licencias. o Concienciación e información a usuarios finales. o • Brindar soporte al software base de los equipos asignados por la Escuela Militar de Ingeniería. • Implementar un sistema automatizado de gestión de licencias mediante las herramientas existentes. • Gestionar los convenios de software existentes con proveedores e informar sobre los mismos a los interesados en solicitar la adquisición de licencias. • Monitorear periódicamente el uso, instalación y gestión de licencias de software en los computadores institucionales. • Presentar trimestralmente a la Dirección de TI informes sobre el estado de licenciamiento y las brechas existentes. ▪ Es responsable de la correcta gestión de licencias en la Universidad.

ROL O CARGO DEL RESPONSABLE	NIVEL DE RESPONSABILIDAD O FUNCIONES
Control Interno, Calidad, Seguridad y Riesgos de TI.	• Ejecutar revisiones anuales de cumplimiento de políticas y normas de licenciamiento. • Informar a la dirección de TI cualquier brecha existente que se detecte como resultado de los exámenes de auditoría.
Departamento solicitante de licencias	• La unidad o departamento solicitante de licencias deberá gestionar de su presupuesto, el pago de los costos implicados en licencias de software.
Usuario final	• Cumplir con la política de licenciamiento. • Es responsable del software instalado en el computador que utilice. • Gestionar el soporte y capacitación de las aplicaciones que utilice y no formen parte del software base.

3. DESCRIPCIÓN DE LA POLÍTICA

3.1 Normas y disposiciones generales

Con el objetivo de cumplir con la regulación existente en el ámbito de software, la Escuela Militar de Ingeniería, extiende la presente política de licenciamiento dirigida a todos los, Departamentos, Secciones, Unidades Académicas y Reparticiones.

- ✓ Los Departamentos, Secciones, Unidades Académicas y Reparticiones, con ayuda de la Dirección Nacional de Informática, deberán identificar los perfiles de software necesarios para soportar la operación de la Escuela Militar de Ingeniería.

- ✓ La Dirección Nacional de Informática con el Departamento de Asistencia Técnica, implementará un estándar de software base para el usuario final, el mismo que se considera la plataforma (sistema operativo) y programas básicos para desarrollar labores generales de cada usuario.

- ✓ En caso de existir la necesidad de instalar software en los equipos de la Escuela Militar de Ingeniería, el usuario final o custodio deberá solicitar a la

Dirección Nacional de Informática al Departamento de Asistencia Técnica, la instalación del mismo previa autorización de su Departamentos, Secciones, Unidades Académicas y Reparticiones.

- ✓ Cada vez que sea necesario adquirir, renovar o cambiar un software el usuario final debe llenar la plantilla de "Solicitud de Adquisición de Licencias de Software" la misma que tiene que estar firmada por el Usuario Solicitante / Jefe inmediato / Jefe de Departamento o Sección y presentar este requerimiento en el Departamento de Asistencia Técnica para su validación y gestión técnica.

- ✓ El solicitante de la adquisición, renovación o cambio de software será responsable de la gestión de compra que esto implique.

- ✓ En caso de existir programas de software no licenciados, no regularizados o no pertenecientes al perfil aprobado por la dirección de su dependencia en un computador de la Institución, la responsabilidad final y el derecho de repetición recaerán sobre el custodio del equipo.

- ✓ La asignación de licencias de software a un empleado de la Escuela Militar de Ingeniería se realizará en base a las funciones que éste desempeñe, para lo cual se realizará una validación de dos elementos:

- ✓ Verificación del perfil de software al que pertenece.

- ✓ Autorización de la Jefatura inmediata y de la Dirección Nacional de Informática.

- ✓ Dirección Nacional de Informática, y el Departamento de Asistencia Técnica, proveerá únicamente software que ha sido adquirido legalmente, con el fin de satisfacer todas sus necesidades, en un tiempo determinado y en cantidades suficientes. El uso de los programas que se obtienen a partir de otras fuentes, puede implicar amenazas en la seguridad de la información de la Escuela Militar de Ingeniería, por lo que dicho uso está estrictamente prohibido.

- ✓ Dirección Nacional de Informática, y el Departamento de Asistencia Técnica no estará autorizada para realizar instalaciones de software adquiridos por Escuela Militar de Ingeniería a equipos no pertenecientes al inventario de Activos Fijos-

Escuela Militar de Ingeniería.

- ✓ La Dirección Nacional de Informática, y la Sección de Soporte Técnico ejecutará procesos de revisión del software instalado en los equipos institucionales y en caso de detectar software no regularizado, se informará a las autoridades sobre este incumplimiento.

- ✓ La Dirección Nacional de Informática, y la Sección Soporte Técnico, se encargará de comunicar con la debida anticipación la caducidad de las licencias inventariadas a los líderes de cada Área.

- ✓ El Departamento de Asistencia Técnica de la Dirección Nacional de Informática no es responsable del soporte o capacitación de software especializado y/o software no básico.

- ✓ Los equipos computacionales de la Escuela Militar de Ingeniería deben mantener instalado únicamente software regularizado por su, Departamento, Sección y la Dirección Nacional de Informática, en base a su perfil.

- ✓ Todo equipo computacional asignado a los empleados de la Escuela Militar de Ingeniería o cualquiera de sus reparticiones relacionadas, debe ser utilizado por el usuario final o custodio cumpliendo las normas y políticas de Licenciamiento de la Escuela Militar de Ingeniería.

- ✓ La Escuela Militar de Ingeniería no se hace responsable bajo ningún concepto del software no licenciado o regularizado que se encuentre instalado en los equipos institucionales, considerando que la existencia de este tipo de software en un equipo institucional, representa una violación a la presente política.

3.2 Restricciones y Prohibiciones

- ✓ Instalar software sin licencia en los equipos de la Escuela Militar de Ingeniería.

- ✓ Instalar software legalizado por Escuela Militar de Ingeniería en equipos que no son propiedad de la Escuela Militar de Ingeniería.

- ✓ Utilizar programas de generación de códigos de licenciamiento, ya que son

ilegales y contravienen la Política Institucional de Seguridad de la Información "Control de cumplimiento y acciones".

4. ANEXOS

- ✓ Estándar de perfiles para licenciamiento.
- ✓ Software Autorizado por Perfil.
- ✓ Solicitud de Adquisición de Licencias de Software.
- ✓ Extracto de Política Institucional de Seguridad de la Información.

5. GLOSARIO DE TÉRMINOS

- ✓ **Licencia de software:** es un contrato entre el titular del derecho de autor (propietario) y el usuario del programa informático (Universidad), el cual se definen con precisión los derechos y deberes de ambas partes.

  Una licencia de software otorga al usuario derecho legal a utilizar un software.

- ✓ **Custodio o usuario de un equipo computacional:** Empleado de la Universidad que tiene el control físico o tenencia del equipo computacional y es el responsable de vigilar o proteger el activo tecnológico en mención.

- ✓ **Sistema Operativo:** Es un conjunto de programas encargados de controlar y coordinar el uso del hardware entre diferentes programas de aplicación y los diferentes usuarios. Por lo que constituye la interfaz para interactuar entre el HW y usuario; gestionando procesos básicos de un sistema informático.

- ✓ **Derecho de Repetición:** Es el derecho que tiene el prestador del servicio para reclamar la Indemnización o resarcimiento del pago ante terceros a causa de la inobservancia al presente instructivo.

POLÍTICA
GESTIÓN DEL SERVICIO

POLÍTICA GESTIÓN DE SERVICIOS

1. OBJETIVOS

Establecer los lineamientos necesarios que permitan el manejo eficiente de la gestión y soporte de los servicios de tecnología hacia el usuario.

2. ALCANCE

La política regirá para todo el ambiente de tecnología de información y sus actores operadores de los servicios, así como los usuarios y clientes de Escuela Militar de Ingeniería.

3. NIVELES DE RESPONSABILIDAD

ROL O CARGO DEL RESPONSABLE	NIVEL DE RESPONSABILIDAD FUNCIONES
Mesa de Servicio	• Registrar, dar seguimiento y solución a todas las solitudes e incidentes reportados a la mesa de servicios. • Clasificar y priorizar las solicitudes de servicio en incidentes reportados a la mesa de servicios. • Entregar un ticket al usuario para el seguimiento de su solicitud. • Comunicar a los usuarios los medios por lo que se puede reportar las solicitudes e incidentes referentes. • Realizar la gestión de incidentes, problemas y niveles de servicio. • Monitorear la solución de solicitudes, incidentes y problemas y proponer la mejora contínua de los servicios. • Gestión y monitoreo de los niveles de servicio acordados con el cliente. Cumplir con los niveles de servicios comprometidos y acordados con los clientes. • Renovar los acuerdos de nivel de servicio con el cliente, aplicando los alcances que se llegaren acordar con el mismo. • Reportar a los clientes y Rectorado de la Escuela Militar de Ingeniería, el desempeño del servicio según los niveles de servicio acordados. ✓ Realizar periódicamente encuestas para medir el nivel de satisfacción del usuario. Proponer las mejoras correspondientes para incrementar el nivel de satisfacción.

Centro de Respuestas a Incidentes de Seguridad Informática (CSIRT - EMI),	• Ejecutar revisiones anuales de cumplimiento de políticas y normas de la gestión del servicio. ✓ Informar a la dirección de TI cualquier brecha existente que se detecte como resultado de los exámenes de auditoría.
Dirección Nacional de Informática	• Ejecutar revisiones anuales de cumplimiento de políticas y normas de la gestión del servicio. ✓ Informar cualquier brecha existente que se detecte como resultado de los exámenes de auditoría.
Usuario	• Cumplir con la política de gestión del servicio. • Comunicarse a la mesa de servicios tecnológica por los medios indicados. • Reportar a la mesa de servicio tecnológica la solicitud o incidencia del servicio afectado, así como confirmar el cierre del ticket en cuanto se tenga la solución. • Apoyar a la mesa de servicios tecnológica proporcionando información necesaria para el registro y solución de su solicitud o incidencia. ✓ Solicitar el número de ticket de la solicitud o incidente reportado. • Responder a las encuestas que realice la mesa de servicios tecnológica referente al soporte de los servicios.
Cliente	• Cumplir con la política de gestión del servicio. • Es responsable de acordar conjuntamente con el dueño del servicio tecnológico, los niveles de servicio y condiciones que regirán en el acuerdo de nivel de servicio.

4. DESCRIPCIÓN DE LA POLÍTICA

La Escuela Militar de Ingeniería orientada a mejorar el soporte de los servicios tecnológicos, advierte la necesidad crear un único punto de contacto hacia los servicios de TI, con ello se implementa la Mesa de Servicios Tecnológicos basada en las mejores prácticas de la gestión del servicio ITIL.

4.1 Normas y Disposiciones Generales / Procedimiento

✓ El único punto de contacto entre el usuario y el área de tecnología para reportar solicitudes e incidentes referentes a los servicios que se oferten en el catálogo de servicios de TI, es la mesa de servicios tecnológicos.

✓ Los medios de comunicación hacia la mesa de servicios tecnológicos son mail, telefónica o personalmente.

✓ La mesa de servicios tecnológicos atenderá en los horarios habituales de la

Escuela Militar de Ingeniería, cualquier extensión en cuanto al mismo será gestionado con la Dirección Nacional de Informática según las clausulas establecidas en los acuerdos de nivel de servicio pactados con el cliente.

- ✓ Toda solicitud de servicio o incidente de soporte de los servicios tecnológicos deberán ser registrados en el Sistema para monitoreo, control y gestión de su solución.

- ✓ La mesa de servicios tecnológicos, a través del Sistema, entrega un número de ticket al usuario que le permita realizar el seguimiento de su solicitud o incidente.

- ✓ El ticket registrado o cerrado en el Sistema es enviado vía mail al correo institucional del usuario.

- ✓ El usuario es responsable de colaborar con la mesa de servicios tecnológicos en la realización de un checklist o lista de verificación y proporcionar toda la información requerida ya sea verbal, física o digital, dependiendo del requerimiento, para realizar la documentación de su solicitud o incidente y gestionar la solución de su ticket.

- ✓ Toda solicitud de servicio o incidente reportado es categorizado y priorizado según el acuerdo de nivel de servicio pactado con el cliente.

- ✓ Todo ticket reportado a la mesa de servicios tecnológicos será resuelto según priorización.

- ✓ Los técnicos que conforman la mesa de servicios realizarán la gestión de incidentes, problemas y niveles de servicio según los procedimientos aprobados por la dirección de la Dirección Nacional de Informática y conforme a los acuerdos de niveles de servicio pactados con el cliente.

- ✓ La gestión que realiza la mesa de servicio, así como el proceder de los técnicos que la conforman, se ajustarán al marco de referencia ITIL de las mejores prácticas de gestión de servicios de TI.

- ✓ La mesa de servicios tecnológicos se contacta telefónicamente con el usuario

para realizar el cierre del ticket reportado.

- ✓ Mesa de servicios tecnológicos intentará contactar al usuario un día para confirmar el cierre de solicitud o incidente, luego de éste lapso se considerará el ticket cerrado a menos que el usuario reporte lo contrario.

- ✓ En caso que la mesa de servicios tecnológicos no pueda contactar al usuario en un día, se procederá al cierre del ticket dando por aceptado la satisfacción del mismo.

- ✓ La mesa de servicios tecnológicos es responsable de brindar un servicio de calidad para ello realiza la gestión de incidentes, problemas y niveles de servicio.

- ✓ El analista de mesa de servicios reporta a la Dirección Nacional de Informática y al cliente el desempeño del servicio según los niveles de servicio pactados.

- ✓ La mesa de servicios tecnológicos mediante la gestión de incidentes y problemas, propone la mejora del servicio con el fin de mejorar el nivel de servicio acordado con el cliente.

- ✓ La mesa de servicios tecnológicos medirá periódicamente la satisfacción del usuario a través de encuestas periódicas.

5. RESTRICCIONES Y PROHIBICIONES

- ✓ No se receptarán, ni se resolverán solicitudes e incidentes que no se ajusten a la presente política.

- ✓ Ninguna solicitud o incidente será resuelta sino está registrada en el Sistema.

6. ANEXOS

ANEXO 1: CATÁLOGO DE SERVICIOS TI.

Catálogo de Servicios de TI
La Unidad de Gestión de las tecnologías de la Información ofrece el soporte a incidentes y problemas, administración, mantenimiento e innovación de los siguientes servicios:
o Redes e Internet
o Equipos Computacionales
o Software de Oficina
o Antivirus
o Licenciamiento de Software
o Sistema Académico Actual
o Sistema Financiero
o Correo Electronico EMI

ANEXO 2: Medios de comunicación Mesa de Servicios Tecnológicos

Medios de comunicación Mesa de Servicios Tecnologicos
Los medios por los que un usuario puede reportar sus solicitudes o incidentes referentes al catálogo de servicios tecnológicos son:
o Vía correo electrónico: mst@utpl.edu.ec
o Vía telefónica: 1800 8875 8875 ext. 3333

7. GLOSARIO DE TÉRMINOS

- ✓ **DNI:** Dirección Nacional de Informática.
- ✓ **Cliente:** Es la empresa o persona responsable de las decisiones y términos que se lleguen a pactar en el acuerdo de nivel de servicio o contrato del servicio de tecnología.
- ✓ **Usuario:** Es la persona que utiliza el servicio de tecnología contratado.
- ✓ **Mesa de servicios tecnológicos:** Es el punto único de contacto para que la comunidad de la Escuela Militar de Ingeniería reporte las solicitudes o incidentes

referentes a los servicios del catálogo de servicios de TI.

- ✓ **ITIL:** La Biblioteca de Infraestructura de Tecnologías de Información, es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general.

- ✓ **Solicitud de servicio:** Son consultas estándares de los usuarios o cambios menores que un usuario requiere sobre los servicios ofertados en el catálogo.

- ✓ **Incidente:** Una interrupción no planificada de un Servicio de TI o una reducción de la Calidad de un Servicio de TI.

- ✓ **Problema:** Causa subyacente, aún no identificada, de una serie de incidentes o un incidente aislado de importancia significativa.

- ✓ **Gestión de Incidentes:** Tiene el deber de detectar cualquier alteración en los servicios de TI ofertados en el catálogo, registrar y clasificar las alteraciones y asignar al personal adecuado para restaurar el servicio, lo más rápido, según los niveles de servicio acordado con el cliente.

- ✓ **Gestión de Problemas:** Está a su cargo investigar las subyacentes a toda alteración, real o potencial, del servicio TI, determinar posibles soluciones, proponer las peticiones de cambio para restablecer la calidad del servicio y realizar las revisiones post implementación para asegurar que los cambios se han realizado eficazmente.

- ✓ **Gestión de Niveles de Servicio:** Es responsable de buscar un compromiso realista entre las necesidades y expectativas del cliente y los costes de los servicios asociados, de forma que estos sean asumibles tanto por el cliente como por la organización TI.

- ✓ **Catálogo de servicios de TI:** Contiene todos los servicios de Direccion Nacional de Informática soportados por la Mesa de Servicios Tecnológicos; así como los que están por incluirse en un corto plazo.

- ✓ **Acuerdo de nivel de servicio:** Es un contrato o acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

- ✓ **Analista de mesa de servicios:** La persona encargada que la mesa de servicios cumpla con los niveles de servicio acordados con el cliente. Monitorea, da seguimiento y coordina el cumplimento de la gestión de incidentes, problemas y niveles de servicio con el fin asegurar un servicio de calidad.

- ✓ **Ticket:** Un número generado automáticamente por el servidor de registro de solicitudes o incidentes y que es enviado por al mail del usuario para el seguimiento de su requerimiento.

- ✓ **Checklist:** o lista de verificación, es un documento que detalla uno por uno distintos aspectos que se deben analizar, comprobar y verificar acerca la solicitud o incidente reportado y que son necesarios para la documentación y/o solución del caso.