

UNIVERSIDAD FRANCISCO GAVIDIA

TECNOLOGÍA, INNOVACIÓN Y CALIDAD

DIRECCIÓN DE TECNOLOGÍA Y COMUNICACIONES



POLÍTICA DE SEGURIDAD

**“DISPOSICIONES PARA LA ADMINISTRACIÓN, OPERACIÓN Y USO DE
RECURSOS INFORMÁTICOS”**

SAN SALVADOR, MARZO DE 2013

ÍNDICE

Contenido	Página
INTRODUCCIÓN	1
OBJETIVOS	2
Objetivo General	2
Objetivos Específicos	2
CAPÍTULO I	2
1.0 GENERALIDADES	2
1.1. Ámbito de Aplicación	3
1.2. Normas de Actualización	3
1.3. Aprobación y Vigencia del Instructivo	3
1.4 Responsabilidades	3
1.5. Definiciones	4
1.5.1 Políticas de Seguridad	4
1.5.2 Política	4
1.5.3 Estándar	4
1.5.4 Guía	4
1.5.5 Procedimiento	5
1.5.6 Seguridad Informática	5
1.5.7 Usuarios de los Centros de Cómputo	5
1.5.7.1 Usuarios de Educación Continua	5
1.5.7.2 Usuarios Externos	5
CAPÍTULO II	5
2.0 ÁMBITO DEL EQUIPO	5
2.1. Instalación del Equipo Informático	5
2.2 Mantenimiento del Equipo Informático	6
2.3. Actualización del Equipo Informático	7
2.4 Reubicación del Equipo Informático	7
2.5 Reemplazo del Equipo Informático	8
2.6 Donación del Equipo Informático	9

CAPÍTULO III	10
3.0 ÁMBITO DEL SOFTWARE	10
3.1 Adquisición e Instalación del Software	10
3.2 Actualización del Software	11
3.3 Auditoría del Software Instalado	12
3.4 Software Propiedad de la Institución	12
3.5 Donación del Software Propiedad de la Institución	13
CAPÍTULO IV	14
4.0 CONTROL DE ACCESOS	14
4.1. Acceso a Áreas Críticas	14
4.2. Control de Acceso al Equipo Informático	14
4.3. Control de Acceso a Centros de Cómputo	15
4.4 Control de Acceso Remoto	16
4.5 Acceso a los Sistemas Administrativos	16
4.6 Restricciones a Usuarios	17
4.7 Ámbito de Internet	18
CAPÍTULO V	19
5.0 UTILIZACIÓN DE LOS RECURSOS DE LA RED	19
5.1 Utilización de los Recursos	19
5.2 Control de la Información	21
5.3 Sanciones	22
CAPÍTULO VI	23
6.0 IMPLEMENTACIÓN	23
CAPÍTULO VII	24
7.0 GLOSARIO	24

INTRODUCCIÓN

Conforme las tecnologías se han esparcido se han transformado en un continuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar ataques y transgresiones.

La seguridad de las instituciones en muchos de los países se ha convertido en cuestión de seguridad nacional, por ello contar con un documento de políticas de seguridad es imprescindible, y debe plasmar mecanismos confiables que con base en la política institucional proteja los activos de la UFG.

La seguridad informática consiste en asegurar que los recursos del Sistema de Información como material informático, hardware y software sean usados adecuadamente. La Universidad consciente del valor de estos recursos, ha desarrollado a través de la Dirección de Tecnología y Comunicaciones sus propias políticas para normar el uso de los recursos informáticos o tecnológicos.

El objetivo principal de la Dirección de Tecnología y Comunicaciones es brindar a los usuarios los recursos informáticos con la cantidad y calidad que demandan, esto es, que tengamos continuidad en el servicio por lo menos en un 95% anual. Así, la cantidad de recursos de cómputo y de comunicaciones con que cuenta la UFG son de consideración y se requiere que se protejan para garantizar su buen funcionamiento.

De esta manera, las políticas de seguridad informática de la UFG, emergen como el instrumento para sensibilizar y orientar a los usuarios, sobre la importancia de la información y servicios ofertados a toda la comunidad.

El proponer esta política requiere un compromiso institucional, agudeza técnica para determinar fallas y deficiencias, constancia para su renovación en función del ambiente dinámico que nos rodea.

La Dirección de Tecnología y Comunicaciones, presenta el documento “Disposiciones para la Administración, Operación y Uso de Recursos Informáticos” a fin de que la Universidad Francisco Gavidia pueda disponer de los ejes de proyección que en materia de seguridad informática la Institución requiere.

OBJETIVOS

Objetivo General

- Regular el suministro, distribución, conservación y uso de los recursos informáticos de la Universidad Francisco Gavidia.

Objetivos Específicos

- Establecer un conjunto de normas y disposiciones que reglamenten las obligaciones, responsabilidades y derechos en relación a los recursos informáticos de la Universidad Francisco Gavidia.
- Servir de guía para orientar sobre la administración, uso y operación de los recursos informáticos de la Universidad Francisco Gavidia.

CAPÍTULO I

1.0 GENERALIDADES.

Podemos entender como seguridad, un estado de un sistema, el cual indica que este se encuentra libre de peligro, daño o riesgo. Dependiendo de las fuentes de amenazas, la seguridad puede dividirse en seguridad lógica y seguridad física. Se puede definir entonces que un sistema es seguro cuando cumple con las características de: Integridad, confidencialidad, disponibilidad.

Es así, que las políticas de seguridad en materia de informática, han sido elaboradas para normar a la institución en este rubro.

La propuesta ha sido analizada y revisada a fin de no contravenir con los derechos básicos de los usuarios, no pretende ser una camisa de fuerza, se orienta más a una forma de operar el sistema con seguridad.

1.1. Ámbito de Aplicación.

La presente es aplicable a la Red Informática de la UFG, la cual esta formada por: Red Administrativa, Centros de Cómputo, Laboratorios Especializados, Registro Académico, Sistema Bibliotecario y Centros de Cómputo del Centro Regional de Occidente; es decir, en todas las áreas en las que se tenga equipo informático o tecnológico propiedad de la UFG.

1.2. Normas de Actualización.

Por su naturaleza, el presente instructivo deberá ser actualizado por la Dirección de Tecnología y Comunicaciones, de acuerdo a las necesidades o cambios que se generen en la institución.

1.3. Aprobación y Vigencia del Instructivo.

El presente instructivo será aprobado por el Consejo Directivo de la UFG y entrará en vigencia a partir de su aprobación y se actualizará en función de las necesidades que se presenten.

1.4 Responsabilidades.

1.4.1 Es responsabilidad de la Dirección de Tecnología y Comunicaciones y sus dependencias:

Garantizar el cumplimiento de las políticas de seguridad “Disposiciones para la Administración, Operación y Uso de Recursos Informáticos” y sus actualizaciones a fin de preservar el activo que en materia involucra.

1.4.2 Es responsabilidad de los usuarios: Acatar y cumplir la normativa establecida en el presente documento.

1.5. Definiciones.

1.5.1 Políticas de Seguridad: La Dirección de Tecnología y Comunicaciones, conciente de la estructura de la Red Informática de la UFG, divide las políticas de seguridad según su naturaleza.

- a) Ámbito del Hardware.
- b) Ámbito del Software.
- c) Control de Accesos.
- d) Utilización de los Recursos de la Red.
- e) Supervisión y Evaluación de Servicios.

1.5.2 Política: Declaración general de principios, que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas deben ser pocas (es decir, un número pequeño), deben ser apoyadas y aprobadas por la alta dirección, así mismo deben ofrecer direccionamientos a toda la organización o a un conjunto importante de dependencias.

1.5.3 Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Sirven como especificaciones para la implementación de las políticas.

1.5.4 Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son, esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas, a menos que existan argumentos documentados y aprobados para no hacerlo.

1.5.5 Procedimiento: Presentación por escrito, en forma narrativa y secuencial, de cada una de las operaciones utilizadas para delinear los pasos que deben ser seguidos por una dependencia, para implementar la seguridad o actividad relacionada a dicho proceso o sistema.

1.5.6 Seguridad Informática: Es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos, encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

1.5.7 Usuarios de los Centros de Cómputo: Se consideran usuarios todos los estudiantes activos de la UFG de pre-grado, postgrado, docentes y personal administrativo.

1.5.7.1 Usuarios de Educación Continua: Son las personas particulares y/o estudiantes de la Universidad inscritos en cursos libres o diplomados, cuya naturaleza requieren uso de equipo informático para su formación académica.

1.5.7.2 Usuarios Externos: Son personas particulares que aun no recibiendo ningún tipo de servicio, requieren el uso de equipo informático los cuales deben de ser previamente autorizados por autoridades o funcionarios de la Universidad.

CAPÍTULO II

2.0 ÁMBITO DEL EQUIPO

CAPÍTULO III

3.0 ÁMBITO DEL SOFTWARE

CAPÍTULO IV

4.0 CONTROL DE ACCESOS.

4.1. Acceso a Áreas Críticas.

4.2. Control de Acceso al Equipo Informático.

4.3. Control de Acceso a Centros de Cómputo.

4.4 Control de Acceso Remoto.

4.5 Acceso a los Sistemas Administrativos.

4.5.1 Tendrá acceso a los sistemas administrativos solo el personal de UFG que es titular de una cuenta o bien tenga la autorización del responsable si se trata de personal de apoyo administrativo o técnico.

4.5.2. El manejo de información administrativa que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.

4.5.3. Tendrá acceso a los sistemas administrativos, el personal docente y administrativo de la UFG o usuarios que tengan la autorización del responsable del área en que aplique.

4.5.4 El acceso a los sistemas será categorizado de acuerdo a los privilegios de uso para cada grupo, entendiéndose las siguientes categorías de acceso:

- **Administradores de Sistema:** están facultados para la gestión de los sistemas informáticos, tienen la capacidad de desarrollar software para ser utilizados por otros usuarios, velar por el buen funcionamiento de estos y proveer soporte y mantenimiento a los servicios.
- **Usuarios Administrativos:** tienen acceso a los sistemas relacionados con los procesos administrativos de la institución como por ejemplo Sistema Contable, Sistema Financiero,

Sistema de Gestión de la Calidad, Correo Electrónico, entre otros. Son capaces de generar información relacionada a las actividades laborales que desempeñan.

- Docentes: cuentan con acceso a los sistemas relacionados con la actividad académica de la institución, esto incluye el ingreso a la Plataforma Virtual con la posibilidad de crear contenidos, actividades y evaluaciones. Además, poseen acceso a los sistemas de Registro Académico, correo electrónico, y algunos sistemas administrativos propios de la actividad académica.

- Estudiantes: cuentan con acceso a realizar consultas a los sistemas relacionados con el proceso aprendizaje lo que les permite visualizar sus notas, planes de estudio, etc. Tienen los permisos necesarios para interactuar con la Plataforma Virtual, esto les permite enviar tareas, presentar evaluaciones, participar en foros, entre otras actividades. Se les asigna un correo electrónico institucional y otras aplicaciones y beneficios para su proceso de aprendizaje.

4.5.5 La instalación y uso de los sistemas de información, se rigen por el reglamento de uso de la Red Informática y por las normas y procedimientos establecidos por el Departamento de UFGnet, en coordinación con la Dirección de Tecnología y Comunicaciones.

4.5.6 Los servidores de bases de datos administrativos son de acceso restringido, por lo que se prohíben los accesos de cualquier usuario que no posea la autorización de la Dirección de Tecnología y Comunicaciones.

4.5.7 El control de acceso a los sistemas de información de Registro Académico, será determinado por el funcionario Titular responsable de dirigir dicha Unidad.

4.6 Restricciones a Usuarios.

CAPÍTULO V

5.0 UTILIZACIÓN DE LOS RECURSOS DE LA RED.

CAPÍTULO VI

6.0 IMPLEMENTACIÓN.

CAPÍTULO VII

7.0 GLOSARIO

Activo: Recurso del sistema de información o relacionado con este, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenaza: Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Auditoría: Es un proceso orientado a inspeccionar el cumplimiento de las políticas, aplicadas a los sistemas, con el objetivo de asegurar la integridad de los mismos y recomendar cualquier cambio que se estime necesario.

Area Crítica: Es el área física donde se encuentra instalado el equipo informático y telecomunicación que requiere de cuidados especiales, cuya naturaleza los vuelve indispensables para el funcionamiento continuo de los sistemas de comunicación de la Red Informática.

CDSOFT: Centro de Desarrollo de Software de la UFG, es la entidad responsable de la creación y mantenimiento de soluciones de software, investigación de nuevas tecnologías y gestión del sitio Web de la Universidad.

Departamento de Redes/Telefonía: Es la entidad responsable de garantizar el buen funcionamiento y conectividad de la Red Informática de la UFG de la Sede Central y el Centro Regional de Occidente. Se atribuye a esta la prestación de servicios eficientes y de utilidad en la transmisión de datos, voz y video para apoyar efectivamente los requerimientos de los usuarios.

Departamento UFGnet: Es la entidad responsable de asegurar el buen funcionamiento de los Centros de Cómputo, laboratorios especializados, recursos informáticos y multimedia distribuidos en el campus de la Universidad de la Sede Central y el Centro Regional de Occidente.

Dirección de Tecnología y Comunicaciones: Es la responsable de garantizar el buen funcionamiento de los servicios informáticos de apoyo al proceso de enseñanza-aprendizaje, promover los avances en materia de tecnología y supervisar el eficiente funcionamiento de las dependencias que tiene bajo su responsabilidad: UFGnet, Redes/Telefonía, Soporte de Servicios Virtuales y Capacitaciones y Centro de Desarrollo de Software (CDSOFT).

Desastre o Contingencia: Interrupción de la capacidad de acceso a información y procesamiento de la misma, a través de computadoras necesarias para la operación normal de un negocio.

Equipo de Comunicación: Se refiere a todo dispositivo utilizado para dar conectividad de Internet en la red de la UFG.

Equipo Informático: Se refiere a computadoras, proyector multimedia, laptop, impresores, UPS, equipos de redes, telefonía y equipos especializados de comunicaciones.

Equipo de Laboratorio: Son todos aquellos instrumentos y equipos utilizados en las prácticas de los Laboratorios Especializados, tales como: unidad base, instrumento virtual, entrenador de antenas, osciloscopio, medidor de ROE, accesorios asociados.

Hardware: Se define como la parte tangible; en relación a una computadora, equipo de laboratorio o equipo de comunicación, son todos los dispositivos que utiliza para su funcionamiento.

Internet: Red mundial que permite acceder a información y la comunicación electrónica con personas ubicadas en lugares remotos. También conocido como un sistema avanzado para navegar a través de la red.

Intranet: Red interna de equipos informáticos instalados en la institución.

Mantenimiento Correctivo: Se conoce como toda actividad encaminada a corregir fallas o condiciones de error en un equipo informático o equipo de laboratorio.

Mantenimiento Preventivo: Se conoce como toda actividad encaminada a prevenir fallas o condiciones de error en un equipo informático o equipo de laboratorio.

Sitio Web: Conjunto de Páginas Web relacionadas, donde se accesa a información específica de un tema en particular, el cual es almacenado en un servidor http.

Centro de Cómputo: Término usado para identificar los centros de cómputo para uso de los estudiantes, red administrativa y Laboratorios Especializados.

Riesgo: Posibilidad de que se produzca un impacto determinado en un Activo, en un Dominio o en toda la Organización.

Software: Conocido como la parte intangible; en relación a las computadoras o equipo de laboratorio, se refiere a los programas que utiliza para interactuar con el usuario.

TI: Acrónimo de Tecnología de la Información.

Usuario: Personal docente a tiempo completo o administrativo de la UFG, que tiene asignado un equipo informático. También se consideran usuarios los estudiantes y personal externo debidamente autorizados.

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

Dado en el Salón de Sesiones del Consejo Directivo de la Universidad Francisco Gavidia, a los treinta días del mes de abril de dos mil trece.