PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Tabla de Contenido

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

## EXPOSICION DE MOTIVOS

Ante el esquema de globalización que las tecnologías de la información han originado, principalmente por el uso masivo y universal de la Internet y sus tecnologías, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear y robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crakers, etc., es decir en transgresores.

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

El objetivo principal de la oficina de sistemas es brindar a los usuarios los recursos informáticos con la calidad y la cantidad que demanden, es decir, prestando servicios con continuidad los 365 días del año de manera confiable. Ya que la cantidad de recursos de cómputo y de telecomunicaciones con que cuenta el hospital son de consideración y se requiere que se protejan para garantizar su buen funcionamiento.

Así pues, ante este panorama surgen las políticas rectoras que hacen que la oficina de sistemas pueda disponer de los ejes de proyección que en materia de seguridad la Institución requiere.

## OBJETIVOS

El objetivo de estas políticas es describir el uso adecuado de los servicios, aplicativos, equipos de computación y las redes dentro del Hospital. Estas reglas buscan proteger la información, las personas y el hospital.

El uso inapropiado de los recursos tecnológicos exponen al Hospital a riesgos innecesarios, como ataques de virus, compromisos de las redes y sistemas y problemas de índole jurídico.

## ALCANCE

Estas políticas están dirigidas a los empleados administrativos, asistenciales, estudiantes, alfabetizadotes, contratistas, consultores, y demás miembros del

Hospital, incluyendo al personal vinculado con empresas que prestan servicios al Hospital que utilizan tecnologías de información.

## INTRODUCCIÓN

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado un gran auge, y más aún con el carácter globalizado como son la de Internet y en particular la relacionada con la Web, la visión de nuevos horizontes explorando más allá de las fronteras naturales, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

Lo anterior ha llevado a que muchas organizaciones gubernamentales y no gubernamentales internacionales desarrollen políticas que normen el uso adecuado de estas destrezas tecnológicas y brinden recomendaciones para aprovechar estas ventajas, y evitar su uso indebido, ocasionando problemas en los bienes y servicios de las entidades.

De esta manera, las políticas de seguridad en informática de la institución emergen como el instrumento para hacer consciencia entre los miembros de la organización a cerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten al área de sistemas cumplir con su misión.

La política de seguridad en informática requiere un alto compromiso con la institución, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea.

## 1. Políticas de seguridad

La persona encargada de sistemas en el Hospital San Juan de Dios de Segovia, se encarga de brindar servicio directo al usuario, desde la adquisición, instalación, configuración, puesta en marcha, traslado y asesoría en el manejo de hardware, software y telecomunicaciones. Capacitación y entrenamiento en el uso de las herramientas informáticas, custodia y resguardo de las bases de datos e información de las diferentes dependencias de la empresa. Así pues este documento contiene una clasificación de estas políticas, las cuales son:

## *1.1. Del HARDWARE*

1.1.2. De la adquisición de equipos

La compra de equipos se realiza, dando cumplimiento al estatuto e contratación de la ESE. Los equipos de cómputo, que se adquieren con garantía, una vez instalados los equipos de computo, se inicia un periodo de inducción y capacitación del personal del área de sistemas.

1.1.3. De la instalación de equipo de cómputo.

- Todo el equipo de cómputo (computadoras, estaciones de trabajo, servidores y equipos periféricos), que esté o sean conectado en la institución o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe cumplir con los siguientes requisitos:
- Visto bueno por el área de sistemas
- Estar cubierto por el seguro contra corriente débil
- Estar plaqueteado y relacionado en el inventario del área a la cual se ha asignado.
- Contar con una adecuada instalación eléctrica
- Verificar que el área de trabajo sea segura y cuente con el inmobiliario mínimo para su uso.
- Los equipos informáticos no deben instalarse cerca de ventanales en los cuales entra directamente la luz del sol, ya que el calor puede dañar los circuitos electrónicos.
- La oficina de sistemas tiene un registro de todos los equipos propiedad del hospital.
- El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, sera ubicado en un área que cumpla con los requerimientos de: Seguridad física, las condiciones ambientales, la alimentación eléctrica.
- La protección física de los equipos corresponde a quienes en un principio se le asigna, y corresponde notificar los movimientos en caso de que existan, a la persona encargada de sistemas de la ESE.
- Todo equipo que se conecte a la red de datos de la empresa debe tener instalado programa de antivirus debidamente licenciado y actualizado.
- La instalación de equipos de cómputo del hospital debe ser autorizado y realizado por personal de sistemas.
- La capacitación al usuario debe ser realizado por el líder de la aplicación o por el funcionario que éste delegue.
- La inducción sobre el manejo específico de los recursos informáticos que el Hospital entregue al usuario final está a cargo del personal de sistemas.

1.1.4. Del mantenimiento de equipo de cómputo.

- Al personal de sistemas, le corresponde la realización del mantenimiento preventivo y correctivo de los equipos, y debe garantizar su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin se desarrolla un plan de mantenimiento preventivo y correctivo.
- El personal de sistemas tiene el listado de los equipos con los respectivos usuarios de estos, así mismo como la lista de los aplicativos que puede utilizar con las respectivas licencias y la fecha de actualización si es el caso.

1.1.5. De la reubicación del equipo de cómputo.

La reubicación del equipo de cómputo se realiza diligenciando la solicitud de traslado de inventario físico de la empresa.

## *1.2. Del control de accesos*

1.2.1. Del acceso a áreas críticas

El acceso al área de Informática está restringido:

• Sólo ingresa al área el personal que trabaja en la misma.
• Siempre ésta área debe permanecer cerrada, limpia y organizada.
• Esta área debe recibir aseo y mantenimiento por lo menos una vez al día

1.2.2. Del control de acceso al equipo de cómputo.

Cualquier Terminal que pueda ser utilizada como acceso a los datos de un Sistema controlado, es encerrada en un área segura o guardada, de tal manera que no sean usadas, excepto por aquellos que tengan autorización para ello.

Restricciones que se aplican:

• Determinación de los períodos de tiempo para los usuarios a las terminales.
• Tiempo de validez de las contraseñas.

Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, el personal de sistemas tiene la facultad de acceder a cualquier equipo de cómputo del Hospital.

Los equipos cuentan con mecanismos de seguridad según su uso o tipo.

En los lugares donde se tienen instalados los equipos informáticos esta prohibido consumir alimentos.

1.2.3. Del control de acceso local a la red.

Los programas de control de acceso identifican los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas:

a) Nivel de consulta de la información: El privilegio de lectura está disponible para cualquier usuario y sólo se requiere un conocimiento de la estructura de los datos, o del sistema de otro usuario para lograr el acceso. (Existen limitaciones para información confidencial o por su importancia estratégica para la empresa, así como de control).

b) Nivel de mantenimiento de la información: El concepto de mantenimiento de la información consiste en:

- Ingreso: Permite insertar datos nuevos pero no se modifica los ya existentes.
- Actualización: Permite modificar la información pero no la eliminación de datos.
- Borrado: Permite la eliminación de datos.

El personal de sistemas es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
Dado el carácter unipersonal del acceso a la red, el personal de sistemas verifica el uso responsable de las tecnologías de la información.
El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, etc.) conectado a la red es administrado por el personal de sistemas.
Todo el equipo de cómputo que esté o sea conectado a la Red o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe sujetarse a los procedimientos de acceso que emite el personal de sistemas.

1.2.4. De acceso a los sistemas administrativos.

La instalación y uso de los sistemas de información se rigen por las políticas del personal de sistemas:
A los servidores de bases de datos administrativos, se prohíbe el acceso de cualquier usuario, excepto para el personal de Informática.

1.2.5. De acceso a la información.

Todas las personas que laboran en el Hospital o terceros autorizados para acceder a la red corporativa deben identificarse mediante la utilización de códigos de usuario, claves de acceso. Los códigos de usuarios son asignados por personal de sistemas, previa autorización escrita del líder del proceso, informando en que módulos va a trabajar y cuales son las funciones asignadas.

Las solicitudes de códigos de usuarios son realizadas al personal de sistemas, certificando su capacitación, indicando el perfil.

Cuando un usuario se retira del Hospital o es trasladado a otro servicio es deber del líder del proceso, solicitar oportunamente el retiro o cambio de permisos al personal de sistemas.

## *1.3. De la Web*

- El personal de sistemas emite las normas para el uso de los servidores Web, el manejo de las bases de datos, el uso de la Intranet, así como las especificaciones para que el acceso a estos sea seguro.
- Los accesos a las páginas Web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan por el personal de sistemas.
- El personal de sistemas es la responsable de la verificación de respaldo y protección adecuada.
- El material que aparezca en la página de Internet del Hospital debe ser aprobado por la Gerencia y personal de sistemas, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).
- El personal de sistemas tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información, y conservar información del tráfico.

## *1.4. De utilización de los recursos de la red*

Los recursos disponibles a través de la red del Hospital serán de uso exclusivo para asuntos relacionados con las actividades del Hospital.

Le corresponde al personal de sistemas administrar, mantener y actualizar la infraestructura de la red del Hospital.

Dado el carácter confidencial que involucra el correo electrónico el personal de sistemas deberá emitir la reglamentación, acorde a políticas.

Los equipos de la tecnología de la información no se utilizan para realizar trabajos personales.

1.4.1. Del manejo de las contraseñas

- Evite utilizar contraseñas que tengan palabras que se pueden encontrar en el diccionario, ya que son más fáciles de violar mediante el uso de software especializado.
- Evite el uso de información que lo defina y que sea fácil de encontrar, como los números de su teléfono o los nombres de personas allegadas etc.
- Evite utilizar la misma contraseña.
- Cambie sus contraseñas con frecuencia.
- Utilice claves que son mezclas aleatorias de números y letras. Si es posible, también mezcle caracteres en mayúsculas y minúsculas.
- No revele su contraseña. De nada sirve crear una palabra clave que no se pueda violar, si la deja apuntada en un papel pegado a su computador.
- La contraseña debe contener como mínimo 8 caracteres.

## *1.5. Del Software*

1.5.1. De la adquisición de software.

Los productos de software que se adquieren cumplen con los requisitos y requerimientos específicos de la institución, en cuanto a la plataforma de software y de hardware. Tienen una alta calidad en cuanto al grado que satisface los requerimientos de la institución: precisión requerida, cantidad de recursos utilizados, control del acceso, facilidad de uso, facilidad de mantenimiento y prueba, portabilidad del software y facilidad de ínter operación.

Todo el software de la empresa está licenciado respetando los derechos de autor y se mantiene actualizado permanentemente con los parches y mejoras que le realizan al software.

Las licencias que se adquieren son las últimas que existen en el mercado y están probadas, por ningún motivo se debe adquirir software en fase de desarrollo o beta.

Se vela por las actualizaciones periódicas de los programas antivirus, sistemas operativos, software de oficina, manejador de bases de datos, utilitario etc.

En cuanto a la paquetería sin costo se respeta la propiedad intelectual intrínseca del autor.

La oficina de sistemas promueve y propicia que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

1.5.2. De la instalación de software.

El personal de sistemas brinda la asesoría, y supervisa la instalación del software básico para cualquier tipo de equipo.
En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permite la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.
Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen).
La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento al personal de sistemas.
Si se instala software en el servidor principal se saca una copia de seguridad completa de éste, y se guarda en el servidor de reserva, el cual está preparado para la instalación definitiva de un sistema operativo virtual.

1.5.3. De la actualización del software.

El personal de sistemas autoriza cualquier adquisición y actualización del software.

1.5.4. De la auditoria de software instalado.

La oficina de sistemas y de control interno son las responsable de realizar revisiones periódicas para asegurar que sólo programas con licencia estén instalados en las computadoras de la institución.
Se cuenta con un inventario detallado del software instalado en cada maquina.

1.5.5. Del software propiedad de la institución.

Toda la programática adquirida por la institución sea por compra, donación o cesión es propiedad de la institución y mantiene los derechos que la ley de propiedad intelectual le confiere.
Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfases) desarrollados con o a través de los recursos del HOSPITAL se mantienen como propiedad de la institución respetando la propiedad intelectual del mismo.

Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.
Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución están resguardados.

1.5.6. De la propiedad intelectual.

La oficina de sistemas procura que todo el software instalado en el Hospital esté de acuerdo a la ley de propiedad intelectual a que dé lugar.

1.5.7. De supervisión y evaluación

Las auditorias de cada actividad donde se involucren aspectos de seguridad lógica y física se realizan periódicamente y deben sujetarse al calendario que establezca el personal de sistemas en conjunto con la oficina de control interno. Los sistemas considerados críticos, están bajo monitoreo permanente.

## *1.6. De las condiciones físicas*

El Hospital cuenta con un sistema de energía regulada que le permite minimizar las variaciones de voltaje, así mismo en los puntos críticos de la organización cuenta con sistemas de alimentación interrumpida UPS, y una planta de energía que le permite mantener corriente eléctrica en forma permanente en la institución.

1.6.1. Fusibles

- Si una parte de un computador funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo.
- A continuación debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible.
- Entre las causas menos problemáticas para que se fundan los fusibles o salten los diferenciales se encuentra la sobrecarga de un circuito eléctrico.

1.6.2. Caídas y Subidas de Tensión

Las caídas y subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen los computadores personales, los monitores, las impresoras y los demás periféricos. Si las oscilaciones se encuentran fuera de este margen, se recomienda pedir que un electricista revise el cableado e invertir en algún equipo de acondicionamiento de corriente (Estabilizadores de Voltaje).

### *1.7. De los discos magnéticos y discos duros*

- En general los discos magnéticos son medios de almacenamiento "delicados", pues si sufren un pequeño golpe puede ocasionar que la información se dañe o producir un CRASH al sistema.
- No está permitido mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.
- Está prohibido colocar el equipo en una zona donde se acumule calor, ya que el calor puede dilatar algunas piezas más que otras, o secar los lubricantes. Con ello se modifican la alineación entre el disco y los cabezales de lectura-escritura, pudiéndose destruir la información.
- Evitar en lo posible, la introducción de partículas de polvo que pueden originar serios problemas.

### *1.8. De las buenas prácticas en el uso de equipos Informáticos*

Reducción del consumo energético en los equipos informáticos.
Se debe apagar el equipo en los horarios prolongados de inactividad. Cuando no se ve a utilizar por media hora o mas y en el horario de alimentación.

Igualmente la impresora debe estar encendida solo si se necesita imprimir documentos.

### *1.9. Disposición final de lo equipos informáticos*

La decadencia, el deterioro y el agotamiento son componentes necesarios de la vida y del crecimiento; tenemos que aprender a valorarlos y gestionarlos. De todos los seres vivos, los humanos somos los supremos creadores de desechos, aunque sólo recientemente hemos empezado a pensar seriamente sobre las formas en que desechamos. Va quedando claro que nuestros desechos nos afectan profundamente; nuestras sensaciones, nuestra salud, nuestro confort cotidiano, y hasta nuestra supervivencia, están amenazados por ellos.

Para realizar la baja de los equipos, se requiere de concepto técnico del personal de sistemas o de terceros autorizados.

Los equipos que son dados de baja, están sin ningún tipo de información de la empresa, ya que han sido previamente formateados.

## 2. Convenios con terceros

Los terceros que se conecten a la red de datos del Hospital están obligados a seguir las políticas de seguridad existentes.

El hospital no asume ninguna responsabilidad por pérdida de equipos de cómputo propiedad de terceros, ni por la información almacenada en dichos equipos.

## 3. Papel o rol que desempeña cada área de la institución en la actividad informática.

### *3.1. Proceso de sistemas*

Es el proceso encargado de proporcionar en forma óptima la tecnología de sistemas que requiere la institución. Es responsable de que los equipos, herramientas informáticas, telecomunicación y sistemas de información, funcionen oportuna y adecuadamente.

### *3.2. Áreas usuarias*

Durante el desarrollo de los sistemas es responsable de la definición detallada de los requerimientos, del diseño detallado de los documentos, entradas y salidas de los sistemas, y de las pruebas y puesta en marcha de los sistemas desarrollados.

Con respecto a los sistemas de información implantados es responsable de usar el sistema eficientemente, velando por la oportunidad, consistencia y confiabilidad de los datos registrados e informes requeridos.

### *3.3. Control Interno*

Durante el desarrollo de los sistemas es responsable de establecer los requerimientos de control y seguridad del sistema y de establecer los procedimientos administrativos requeridos para que el sistema funcione en una forma segura y confiable.

Una vez implantados los sistemas es responsable de velar por el cumplimiento de las normas y controles establecidos y de verificar la validez y funcionalidad de los planes de contingencia de los equipos y de cada sistema de información.

## *Glosario*

Hacker: Persona que, gracias a sus grandes conocimientos informáticos, puede introducirse sin permiso en la información que tengan otros ordenadores o redes informáticas de particulares, empresas o instituciones si están conectados a Internet

Cracker: Persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los hackers, y pueden disponer de muchos medios para introducirse en un sistema

Intranet: Se llaman así a las redes tipo Internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizara protocolo TCP/IP y servicios similares como WWW.

Correo Electrónico: Sistema para enviar mensajes en Internet. El emisor de un correo electrónico manda los mensajes a un servidor y éste, a su vez, se encarga de enviárselos al servidor del receptor. Para acceder al correo electrónico es necesario que el receptor se conecte con su servidor

Internet: Internet es una Red informática de transmisión de datos para la comunicación global que permite el intercambio de todo tipo de información (en formato digital) entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas International Network (red internacional).

Hardware: Componentes físicos de un ordenador o de una red, en contraposición con los programas o elementos lógicos que los hacen funcionar.

Software: Programas o elementos lógicos que hacen funcionar un ordenador o una red, o que se ejecutan en ellos, en contraposición con los componentes físicos del ordenador o la red.

Malware: Cualquier programa cuyo objetivo sea causar daños a ordenadores, sistemas o redes y, por extensión, a sus usuarios.

Spyware: Programa que acompaña a otro y se instala automáticamente en un ordenador (generalmente sin permiso de su propietario y sin que éste sea consciente de ello) para recoger información personal (datos de acceso a Internet, acciones realizadas mientras navega, páginas visitadas, programas instalados en el ordenador, etc.).

Troyano: Programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema en el que se introduce de manera subrepticia (de ahí su nombre).

Bakdoor: Vulnerabilidad de un sistema operativo, página Web o aplicación que puede ser motivo de entrada para hackers, crackers, o gusanos. Uno de los más usados es la aplicación Back Orifice creado específicamente para entrar en sistemas operativos Windows usando troyanos. Puerta trasera.

Gusano: Programa informático que se auto duplica y auto propaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Los gusanos de redes fueron definidos por primera vez por Shoch & Hupp, de Xerox, en la revista ACM Communications (Marzo 1982).

Spam: Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico. Literalmente quiere decir loncha de mortadela

Firewall: Programa que sirve para filtrar lo que entra y sale de un sistema conectado a una red. Suele utilizarse en las grandes empresas para limitar el acceso de Internet a sus empleados así como para impedir el acceso de archivos con virus

Dispositivo que se coloca entre una red local e Internet y cuyo objetivo es asegurar que todas las comunicaciones entre los usuarios de dicha red e Internet se realicen conforme a las normas de seguridad de la organización que lo instala

Backup: Copia de ficheros o datos de forma que estén disponibles en caso de que un fallo produzca la perdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables, problemas si se realiza de forma habitual y periódica.

Phishing: Duplicación de una página Web con el objeto o con el efecto de hacer creer al visitante que se encuentra en la en la página original.

| CONTROL DE ACTUALIZACIONES | | |
|---|---|---|
| **VERSION** | **FECHA** | **CAMBIOS** |
| 01 | Enero de 2018 | No aplica |
| | | |
| | | |
| | | |
| | | |