Clínica Especializada

EMMSA®

MANUAL SEGURIDAD DE LA INFORMACIÓN

Bello, Antioquia- Colombia.

Tabla de Contenido

1 OBJETIVOS

1.1. OBJETIVO GENERAL

Establecer y difundir las Políticas y Estándares de Seguridad Informática a todo el personal de la Clínica Especializada Emmsa, para que sea de su conocimiento y cumplimiento, de manera que los servicios tecnológicos, de infraestructura y de seguridad informática se ofrezcan con calidad, confiabilidad, integridad, disponibilidad y funcionalidad.

1.2. OBJETIVOS ESPECÍFICOS

- Crear y definir las políticas generales que faciliten la ejecución de las actividades relacionadas con los componentes informáticos y de infraestructura de la Clínica Especializada Emmsa.
- Definir normas para los procesos de tecnología e infraestructura con la finalidad de aplicar buenas prácticas de seguridad de información.

2. ALCANCE

El ámbito de aplicación de las manual, es la infraestructura tecnológica y el entorno informático de la red.

3. DEFINICIÓN DE TÉRMINOS

- **Activo de información**: Es cualquier elemento que tenga valor para la organización y, en consecuencia, debe ser protegido.
- **Amenaza:** Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación.
- **Incidente de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Qué son las normas de Seguridad:** Las normas son un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar

respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red institucional**.**

- **Qué son las políticas de Seguridad:** Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas, a su vez, establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de los mismos.

4. POLÍTICAS

4.1 SEGURIDAD ORGANIZATIVA

4.1.1 RESPONSABILIDADES DEL ÁREA DE SISTEMAS

- Velar por la seguridad de los activos informáticos.
- Gestión y procesamiento de la información.
- Velar por el cumplimiento de las políticas de seguridad informática.
- Reporte de novedades al área de gestión humana para aplicación de llamados de atención y/o correctivos según el caso.
- Capacitación a los usuarios en temas de seguridad de la información.
- Apoyar y coordinar esfuerzos para consolidar un plan de contingencia que dé sustento o solución a la infraestructura física de la empresa.
- Prestar especial atención a los usuarios de la red institucional sobre sugerencias o quejas con respecto al funcionamiento de los activos de la organización.
- Mantener en buen estado los servidores

4.1.2 RESPONSABILIDAD POR LOS ACTIVOS

- Cada empleado, será responsable por los activos que estén a su cargo.
- Cada empleado, como responsable de los activos a su cargo, velará por el cuidado de los activos físicos (hardware y medios magnéticos), activos de información (Bases de datos, archivos, documentación de sistemas de

información, procedimientos operativos, configuraciones), activos de software (aplicaciones, software de sistemas, herramientas), que se encuentren en su equipo asignado.

4.1.3 SEGURIDAD LIGADA AL PERSONAL

- La información procesada, manipulada o almacenada por cualquier empleado de Clínica Especializada Emmsa, y haciendo uso de los activos fijos de la compañía, es de propiedad exclusiva de Clínica Especializada Emmsa.
- Clínica Especializada Emmsa no se hace responsable por daños causados provenientes de sus empleados a la información o activos de procesamiento, propiedad de la empresa, daños efectuados desde sus instalaciones de red a equipos informáticos externos.
- Los contratos laborales cuentan con cláusula de confidencialidad la cual se describe: Texto incluido en contrato de trabajo

"SEXTA: Además tiene como deberes especiales los siguientes: No comunicar a terceros, salvo autorización expresa, las informaciones que sean de naturaleza reservada y cuya divulgación pueda ocasionar perjuicios a la empresa, lo que no obsta para denunciar delitos comunes o violaciones del contrato o de las normas legales del trabajo ante las autoridades competentes.

"Como en el desarrollo de sus funciones EL TRABAJADOR tiene acceso a la información, secretos industriales, inventos, software y en general propiedad intelectual y confidencial de la compañía, ambas partes han acordado que constituye justa causa de la terminación de su contrato de trabajo la violación a un leve de las siguientes obligaciones y prohibiciones:

El trabajador se obliga a no divulgar, durante la vigencia y aun después de la terminación de su contrato de trabajo la información confidencial y científica a la que llegue a tener conocimiento en desarrollo de su contrato de trabajo, se entiende por "información confidencial y científica" a la que llegue a tener conocimiento en desarrollo de su contrato de trabajo, se entiende por "información confidencial y científica "lo siguiente: Cualquier información técnica, financiera, comercial, de negocios, de mercado estratégica y cualquier otra relacionada con los negocios de la empresa. La información confidencial puede ser escrita, oral o visual, o estar contenida en cualquier medio magnético o en cualquier forma o medio y puede haber sido identificada como confidencial o no.

PARAGRAFO: la divulgación de esta información podría hacer incurrir al TRABAJADOR en un tipo penal, consagrado en Código Penal Colombiano art. 308, cuyo texto expresa: “El que emplee, revele o divulgue descubrimiento, invención científica, proceso o aplicación industrial o comercial, llegados a su conocimiento por razón de su cargo, oficio o profesión y que deben permanecer en reserva, incurrirá en presión de dos (2) a cinco (5) años y multa de veinte (20) a dos mil (2.000) salarios mínimos legales mensuales vigentes.

En la misma pena incurrirá el que indebidamente conozca, copie u obtenga secreto relacionado con descubrimiento, invención científica, proceso o aplicación industrial o comercial…”

A. El trabajador se obliga a no utilizar los equipos de computación y sistemas, al igual que el software de la compañía para los fines diferentes a los de su contrato de trabajo. Por lo tanto está prohibido hacerlo para algo diferente.

B. la violación de las anteriores obligaciones o prohibiciones en el evento de incurrir en ellas, ambas partes han convenido que constituye justa causa de terminación del contrato de trabajo y adicional a ello, El TRABAJADOR le pudiese ocasionar a la EMPRESA, perjuicios que las partes, tasan anticipadamente en la suma de TRES SALARIOS MENSUALES que el TRABAJADOR recibe, sin que esto signifique, que no se puedan cobrar los mayores que se logren acreditar en un proceso judicial. Lo anterior sin perjuicio de las sanciones penales en que pudiese incurrir EL TRABAJADOR

4.1.4 PROHIBICIONES

- Está prohibido el consumo de alimentos cerca de los equipos de cómputo.
- Se prohíbe a los usuarios utilizar equipos informáticos, herramientas o servicios propios de Clínica Especializada Emmsa para un objetivo distinto del que están destinadas o para beneficiar a personas ajenas a la compañía.
- No se deben alterar documentos, expedientes o registros, mediante el tratamiento electrónico, proporcionando datos falsos, que pueden perjudicar la correcta operatividad de Clínica Especializa Emmsa.
- Acceder físicamente o manipular los servidores, switches, routers, antenas, puntos de red o telefónicos y elementos activos y las bases de datos que almacenan información privilegiada y transacciones propias de la clínica.

Estas acciones serán realizadas única y exclusivamente por el personal de sistemas.

- A ingresar físicamente a los cuartos de comunicaciones ubicados en cada piso de la clínica, al centro de cómputo principal salvo autorización expresa del coordinador de sistema de la clínica.
- Hacer uso del correo electrónico corporativo o personal (desde el internet brindado por la clínica) para transmitir información con contenido que pueda ser discriminatorio, ofensivo, obsceno, amenazante, intimidante o destructivo para cualquier individuo u organización.

4.2 POLÍTICAS DE SEGURIDAD

4.2.1 SOBRE LA INTEGRIDAD Y DISPONIBILIDAD DE LOS RECURSOS

- No alterar o eliminar ordenadores (hardware o configuración del Sistema Operativo), software o periféricos que estén asignados a otros usuarios, sin la debida autorización del Responsable Administrativo o Coordinador de Sistemas según el caso.
- No entorpecer o absorber recursos compartidos de forma tal que impidan a otros realizar sus tareas de una forma eficiente. Esto incluye, al menos, lo siguiente:
- Uso de programas que puedan saturar los servidores o las redes de la Clínica, cuando haya alternativas más eficientes o no tengan una prioridad alta. En cualquier caso, se deberá solicitar con la suficiente antelación al coordinador.
- Modificación no autorizada de privilegios o permisos.
- Intentos de desactivar servidores o cortar el funcionamiento de las redes.
- Intento de realizar cualquier tipo de daño (físico o lógico) a las herramientas informáticas de la clínica (equipos, aplicaciones, documentos, etc.).
- No desarrollar o usar programas cuyo objetivo sea dañar otras máquinas o acceder a recursos restringidos (malware: virus, troyanos, puertas traseras, etc.). Más aún, deberán controlar que no se les infecte su equipo con este tipo de software, para lo cual el Coordinador de Sistemas, deberá proporcionar las herramientas y utilidades adecuadas. El uso de este tipo de programas, contra un agente externo o contra la propia Clínica.

- No utilizar los enlaces de red para otros usos que no sean los permitidos o los propios necesarios para el desempeño de su actividad.

4.2.2 SOBRE ACCESOS NO AUTORIZADOS Y SUPLANTACIÓN DE IDENTIDAD

- No conseguir accesos a sistemas o recursos a los que no estén autorizados y ni tampoco permitir o facilitar que otros lo hagan.
- Respetar los derechos del resto de usuarios; la mayoría de los sistemas de uso compartido proporcionan mecanismos para proteger los datos e información privada de posibles consultas por parte de otros. Los intentos de saltarse estos mecanismos para conseguir accesos no autorizados, a información calificada como personal, supondrán una violación de esta política.
- El personal del Departamento de Sistemas podrá acceder, exclusivamente, por motivos de mantenimiento y/o de seguridad, a aquellos ficheros de usuario que permitan detectar, analizar y seguir las trazas de una determinada sesión o conexión.
- En cualquier caso, el personal del Departamento de Sistemas tiene el deber de guardar secreto sobre el contenido de los ficheros de los usuarios, no estando autorizado a permitir que terceros puedan acceder a los mismos.
- En el supuesto de que una política interna expresamente lo autorice, el personal del Departamento de Sistemas podrá permitir el acceso a terceros (responsables de proyectos, directores, gerentes,...) a determinados ficheros de otros usuario, debiendo contar en todo caso, tanto con la autorización del Responsable Administrativo como del propietario de los archivos.
- No acceder a ordenadores, aplicaciones, datos o información o redes para las que no estén debidamente autorizados. Tampoco deberán permitir de forma intencionada que otros lo hagan, independientemente de que el recurso (equipo, aplicación, red, datos, etc.) pertenezca o no a la Clínica.
- No está permitido realizar de forma intencionada acciones cuyo fin sea la obtención de contraseñas de otros usuarios sin el consentimiento de estos.
- Todo aquel usuario que haya sido autorizado a usar una cuenta mediante un sistema de usuario/contraseña será responsable de mantenerla en secreto y no darla a conocer a nadie más, esto aplica tanto para personal médico, como personal administrativo. Será siempre el responsable de lo que se

ejecute en el sistema desde esa cuenta. Ninguna persona podrá utilizar el usuario y clave de otro usuario, inclusive con consentimiento del primero, ambos serán responsable de la utilización de este. Los usuarios y las claves son personales e intransferibles.

- Evitar tener compartidos los recursos (ficheros, directorios, etc.) sin el mecanismo de seguridad necesario y disponible en cada sistema operativo y/o aplicaciones que garanticen la seguridad de su equipo y la red.

4.2.3 SOBRE EL USO DE LOS SERVICIOS DE COMUNICACIÓN Y DIFUSIÓN DE INFORMACIÓN.

- El correo electrónico, las listas de distribución, servicios de mensajería instantánea o foros de discusión son herramientas que facilitan la comunicación entre las personas, así, como la difusión de información a varios interlocutores de una sola vez. Por ello conviene tener en cuenta una serie de comportamientos a la hora de usar estos medios.
- No usar estas utilidades para el envío de mensajes con contenido fraudulento, ofensivo, obsceno o amenazante.
- Usar las listas de distribución de correo sólo para enviar mensajes relacionados con la finalidad de las mismas. Existirán también listas libres, que deberán cumplir con lo expuesto en el punto anterior.
- No usar los recursos de la Clínica para actividades personales que no tengan relación con las propias del desempeño laboral, salvo de forma esporádica y siempre dentro de las normas internas en cuanto a seguridad y con el permiso del jefe inmediato. En estos casos el personal de sistemas no está obligado a prestar soporte.
- No usar estos servicios con fines comerciales, salvo autorización expresa del Responsable Administrativo. En cualquier caso, el uso comercial que se haga debe estar relacionado con las actividades de la Clínica.

4.2.4 SOBRE USO DE LA INFRAESTRUCTURA DE COMUNICACIONES.

- Cualquier instalación de software en los servidores o equipos de la empresa deberá ser realizado únicamente por personal del área de sistemas o por un tercero quien deberá ser autorizado por el Coordinador de sistemas.
- No realizar la conexión, desconexión o reubicación de equipos o cambios de configuración de los mismos, sin la autorización expresa del responsable administrativo o del Coordinador de Sistemas.
- Estará prohibido la instalación de dispositivos y tarjetas de acceso remoto, módems, RDSI, ADSL, routers o cualquier otro dispositivo de comunicaciones en ordenadores o redes sin la autorización expresa del responsable administrativo o del Coordinador de Sistemas.
- Estará prohibido la conexión de equipos de comunicaciones para intercambio de información (routers, switches,...) entre equipos de las redes de la Clínica y otros ajenos a dichas redes.
- Estará prohibido el uso de la red y equipos de la Clínica para conseguir acceso no autorizado a cualquier equipo.
- Estará prohibido instalar o ejecutar en cualquier punto de la red informática (computadores o software de red) programas o ficheros que traten de descubrir información distinta de la del propio usuario, en cualquier elemento de la red. Esto incluye sniffer, escaneadores de puertos, etc.
- No se podrá facilitar a otra entidad acceso, a través de las redes de la Clínica, a la infraestructura de comunicaciones propias de este organismo; es decir, no se podrá proporcionar tránsito a otras instituciones, salvo obtención del consentimiento, previamente solicitado por el coordinador de sistemas con previa autorización de la gerencia.
- Evitar la circulación de información comercial (con excepción de respuestas a peticiones expresas sobre productos o servicios de interés para las actividades habituales).
- No se podrá proceder a la destrucción, manipulación o apropiación indebida de la información que circule por la red.
- Evitar el consumo excesivo de los recursos tecnológicos por parte de cualquier usuario.
- Respetar el derecho de privacidad de los diferentes usuarios de la red.

- No utilizar la infraestructura de red de la Clínica, bajo ningún concepto, para lo siguiente:
    - Transmisión de información o acto que viole las leyes Colombianas.
    - Fines privados o personales, con o sin ánimo de lucro.
    - Fines lúdicos
    - Fines no estrictamente relacionados con las actividades propias de la clínica.
    - Creación o transmisión de cualquier tipo de información que sea ofensiva, obscena o indecente.
    - Transmitir información difamatoria de cualquier tipo, ya sea contra entidades o personas.
    - No se podrá divulgar información que viole los derechos de propiedad intelectual.
    - No se podrá usar cualquier aplicación, de la cual se sepa que su uso pueda suponer una alteración de la red.

4.2.5 SOBRE EL USO DE INTERNET.

- Está totalmente prohibido el ingreso a páginas de contenido pornográfico, descarga de programas que permitan realizar conexiones automáticas o visores de sitios clasificados como pornográficos, la utilización de los recursos para distribución o reproducción, de este tipo de material ya sea vía Web o medios magnéticos.
- Está totalmente prohibido utilizar cualquier tipo de software o plataforma que permita o se utilice para bajar música y video.
- Está totalmente prohibido participar en juegos de entretenimiento en línea.
- Los usuarios utilizarán únicamente los servicios para los cuales están autorizados. No deberán usar la cuenta de internet de otra persona, ni intentar apoderarse de claves de acceso de otros, así como no deberán intentar acceder ni modificar archivos que no son de su propiedad, y mucho menos, los pertenecientes a la Clínica.
- Está prohibido el uso de sitios que salten la seguridad del proxy.
- Está prohibida la creación de correos electrónicos que no se encuentren en el dominio de la clínica, en caso de ser necesario es responsabilidad del coordinador de sistemas aprobar y controlar dicha autorización.

4.2.6 SOBRE LAS LICENCIAS DE SOFTWARE Y "COPYRIGHTS"

- Los usuarios y administradores deben respetar las condiciones de licencia y copyright del software que usen en sus equipos.
- Todo software adquirido para la Clínica deberá estar debidamente licenciado y la responsabilidad de esto recaerá en el Comité de compras.
- Todo software que se use en la Clínica debe estar debidamente licenciado, con las licencias que corresponda con el número de usuarios simultáneos. Por supuesto, podrá usarse en equipos de la Clínica software "libre" (Open source, freeware, etc.) con debida autorización del Coordinador de Sistemas.
- Todo software que se use que esté protegido por copyrights no puede ser copiado, salvo con autorización del propietario. No se podrán usar los medios que la Clínicapone a disposición de la clínica para copiar software protegido o romper las protecciones del mismo.
- Aparte del software, toda otra información que también posea derechos de autor, que esté en formato electrónico y que haya sido obtenida de otro equipo o red, se debe usar de acuerdo con la legislación vigente.
- Los usuarios responderán siempre personalmente del software que haya instalado en sus equipos, así como del uso que del mismo se efectúe y deberán cumplir con las obligaciones y requisitos que se deriven de su instalación y utilización.
- En ningún caso los usuarios podrán permitir que ninguna persona lleve a cabo la instalación de software en sus equipos que no esté debidamente licenciado.
- El incumplimiento de estas obligaciones por parte de los usuarios dará lugar a la aplicación de las medidas correctivas y disciplinarias.

4.3 POLÍTICAS PARA COPIAS DE SEGURIDAD

Con el fin de garantizar la continuidad del negocio y minimizar la pérdida de datos debido a fallos de hardware, fallos de software, errores voluntario o involuntarios por acción humana o desastres naturales además de garantizar uno de los principales activos que tiene la Clínica Especializada Emmsa, se determinan tres tipos de respaldos de la información:

- **Respaldo local:** Es la copia de información que se guarda en el mismo equipo pero en una ubicación diferente a la original. Generalmente se almacena en una partición lógica diferente a la partición del sistema operativo con el fin de prevenir pérdida por virus y software malintencionado.
- **Respaldo Remoto:** Es la copia de información que se guarda en un equipo diferente a donde originalmente se encuentra la información. Generalmente el equipo que almacena la copia de seguridad está dentro de la misma red de datos.
- **Respaldo Externo**: Es la copia de información de un equipo o que ya tiene respaldo remoto y después de un tiempo determinado es extraído a medio de almacenamiento externo como discos duros externos, memorias USB, Blue Ray entre otros para ser llevados a un sitio físicamente diferente de la empresa o también puede ser soportado en la nube.

5. CUADRO DE ELABORACIÓN, REVISIÓN, APROBACIÓN Y CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Elaboró	Revisó	Aprobó
1	07/10/2020	Se crea documento exclusivo de manual de seguridad de la información, este esta información estaba inmersa en el código de ética y buen gobierno institucional	Ricardo Hincapie Ruiz Coordinador de Sistemas	Carolina Gómez Gaviria Coordinadora de Calidad	Liliana Maria Villegas Romero Gerente