EMPRESA SOCIAL DEL ESTADO
HOSPITAL DE LA VEGA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2022

CONTENIDO

EXPOSICION DE MOTIVOS....4
INTRODUCCIÓN....4
ALCANCE....5
OBJETIVOS....5
OBJETIVO GENERAL....5
OBJETIVOS ESPECIFICOS....5
DEFINICIONES....5
NORMATIVIDAD....7
DESCRIPCIÓN DEL PLAN....7
LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN....7
GESTIÓN DE ACTIVOS DE INFORMACIÓN....7
COMPONENTES Y HERRAMIENTAS TECNOLÓGICAS DE LA ENTIDAD....8
COMPROMISOS DE CONFIDENCIALIDAD....11
SEGURIDAD DE LA INFORMACIÓN....11
ROLES Y RESPONSABILIDADES....12
SOCIALIZACIÓN Y EDUCACIÓN SOBRE LA SEGURIDAD DE LA INFORMACIÓN.....12
CONTROL DE INGRESO Y SALIDA DE PERSONAL....13
ENTREGA DE ACTIVOS ASIGNADOS....13
SEGURIDAD FÍSICA....13
PROTECCIÓN DE LOS EQUIPOS....14
CONTROL DE CAMBIOS....15
GESTIÓN DE LA CAPACIDAD DE ALMACENAMIENTO Y PROCESAMIENTO....15
IMPLEMENTACIÓN Y ACTUALIZACIÓN DE SOFTWARE....15
PROTECCIÓN DE INFORMACIÓN ANTE POSIBLE SOFTWARE MALICIOSO....16
COPIAS DE SEGURIDAD....16
OBSERVACIONES....17
SEGUIMIENTO, CONTROL Y MEJORA....17

BIBLIOGRAFIA 17

CONTROL DE CAMBIOS 18

EXPOSICION DE MOTIVOS

De acuerdo a los lineamientos y estrategias proporcionadas por la ISO 27001 y ante una cultura organizacional enfocada al uso las tecnologías de la información, se ha originado principalmente 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.

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.

El Plan de Seguridad y Privacidad de la Información de la ESE Hospital de la Vega se enmarca en los lineamientos de la política de seguridad digital establecida en el Modelo Integrado de Planeación y Gestión MIPG, y se encuentra alineado a la estructura organizacional vigente del Hospital, así como con sus objetivo, metas y proyectos.

ALCANCE

Estas políticas están dirigidas a los empleados administrativos, asistenciales, estudiantes, alfabetizadores, contratistas, consultores, y demás miembros del hospital, incluyendo al personal vinculado con empresas que prestan servicios al hospital que utilizan tecnologías de información. Estas políticas incluyen a los equipos propios o arrendados que tiene el hospital y a los equipos propiedad de personas que sean conectados a las redes del hospital.

OBJETIVOS

OBJETIVO GENERAL

Establecer estrategias que permitan a la E.S.E Hospital de La Vega gestionar la seguridad de la información para la protección de los activos de información.

OBJETIVOS ESPECIFICOS

- Promover lineamientos que permitan al cliente interno el correcto manejo de la información.
- Fortalecer en la entidad la cultura de la seguridad y privacidad de la información.
- Garantizar la seguridad y privacidad de la información en la entidad.

DEFINICIONES

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.

NORMATIVIDAD

Para la elaboración del plan se tiene como base la norma ISO 27001, la cual está enfocada a los procesos y lineamientos de los sistemas de gestión de seguridad de la información para las organizaciones. Adicionalmente las guías de seguridad y privacidad de la información del MINTIC.

DESCRIPCIÓN DEL PLAN

LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La oficina de sistemas de la E.S.E Hospital de La Vega, se encarga de brindar servicio directo al cliente interno, 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.

El objetivo de los lineamientos es garantizar la protección de los activos de información de la entidad, teniendo en cuenta los clientes internos y externos de la entidad.

GESTIÓN DE ACTIVOS DE INFORMACIÓN

Con el propósito de garantizar la administración y el control de los activos de información, las diferentes áreas de la E.S.E Hospital de La Vega deberán realizar un inventario de activos que permita obtener un control total de la información producida y procesada.

El inventario permite identificar el propietario del activo, quien deberá asegurar y resguardar la información y los activos asociados al proceso que están llevando. El área será responsable del manejo y el control para el acceso a la información.

A continuación, se listan recomendaciones para un uso aceptable de los activos de información:

- La información, archivos físicos, los sistemas, los servicios y los equipos (estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones y teléfonos, son activos de la Institución y se proporcionan a los funcionarios, contratistas y terceros autorizados, para cumplir con las actividades contratadas.

- La E.S.E Hospital de La Vega podrá monitorear, supervisar y utilizar la información producida por la entidad dependiendo el proceso administrativo o legar que la entidad requiera.

- El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los clientes internos de la entidad.

- El contratista deberá comprometerse a dar a dar buen uso de la información producida, en caso de hacer mal uso de la información el contratista estará expuesto a procesos legales.

COMPONENTES Y HERRAMIENTAS TECNOLÓGICAS DE LA ENTIDAD

La E.S.E Hospital de La Vega cuenta con herramientas tecnológicas que son parte fundamental para el desarrollo de las actividades de cada una de las áreas que componen la entidad, se debe tener presente que estas herramientas son de uso exclusivo para la E.S.E Hospital de La Vega, a continuación, se listan las herramientas tecnológicas y las recomendaciones para el buen uso de las mismas.

CONEXIÓN A INTERNET

Los clientes internos de la E.S.E Hospital de La Vega, deberán tener en cuenta las siguientes recomendaciones.

- El usuario deberá evitar el acceso a páginas con contenido pornográfico, sitios web que promuevan la venta y el consumo de sustancias sicoactivas, evitar sitios web que puedan causar ataques informativos y/o cualquier otra página que vaya en contra de la ética moral y las leyes vigentes.

- El acceso y el uso indebido de los servicios de cambio o transferencia de información puede causar ataques informáticos sobre la entidad.

- Evitar el intercambio no autorizado de información a clientes externos a la entidad.

- La descarga, intercambio o instalación de software de sospechosa procedencia, son un riesgo latente para la seguridad y privacidad de la información. Se debe tener presente que esto puede atentar contra la propiedad intelectual de sus autores.

El área de sistemas con el fin de preservar la seguridad de la información deberá realizar el monitoreo permanente de la navegación a internet de los funcionarios, contratitas y/ terceros. Así mismo. Podrá inspeccionar, registrar y evaluar las actividades realizadas durante la navegación web, de acuerdo a la legislación nacional vigente.

El usuario es responsable de dar un uso adecuado a este recurso y en ningún momento puede usar el servicio de internet para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros.

Por último, el uso del internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la E.S.E Hospital de La Vega.

SERVICIO DE CORREO ELECTRÓNICO

Los clientes internos de la E.S.E Hospital de La Vega, deberán tener en cuenta las siguientes recomendaciones para un uso adecuado del correo electrónico.

- El correo electrónico corporativo es una herramienta de comunicación o intercambio de información oficial entre personal o instituciones, no es una herramienta de difusión indiscriminada de información.

- La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro del Hospital.

- Los mensajes y la información contenida en los buzones de correo son propiedad de la E.S.E Hospital de La Vega y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- La asignación del correo electrónico se realiza de acuerdo con la necesidad del proceso, el tamaño de almacenamiento y la creación del correo electrónico lo realiza el área de sistemas.

- El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo corporativa proporcionada. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal dentro de la institución.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la entidad y deben conservar en todos los casos el mensaje legar corporativo de confidencialidad.

- El correo electrónico corporativo es la única vía de remisión o envío de documentos de carácter administrativo interno en el hospital.

- El usuario no tiene permitido utilizar la dirección de correo electrónico de la E.S.E Hospital de La Vega como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, Instagram, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

- El usuario debe evitar el envió de cadenas de información ya que no se conoce el origen de la información, esto podrá causar posibles filtraciones de información o ataques informativos.

- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva y las áreas de Sistemas y Comunicaciones de la institución.

RECURSOS TECNOLOGICOS

Los clientes internos de la E.S.E Hospital de La Vega, deberán tener en cuenta las siguientes recomendaciones para un uso adecuado de los recursos tecnológicos.

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la E.S.E Hospital de La Vega es responsabilidad del área de Sistemas, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por el E.S.E Hospital de La Vega a través de esta área.

- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios son realizados únicamente por el área de Sistemas.

- El área de Sistemas definirá y actualizará, de manera periódica, la lista de software y aplicaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones instaladas y administradas por el Hospital.

- Los usuarios que requieren acceder a la infraestructura tecnológica de la entidad desde redes externas, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el área de Sistemas. Además, deberán informar previamente a la misma área para autorizar el acceso y brindar los permisos respectivos para la protección de la información, de acuerdo a lo definido por el área de sistemas.

- Las estaciones de trabajo y en general cualquier recurso de la organización no debe ser empleado para actividades recreativas.

- El personal de la E.S.E Hospital de La Vega no podrá copiar o replicar la información para uso personal.

COMPROMISOS DE CONFIDENCIALIDAD

Para la E.S.E Hospital de La Vega los clientes internos deberán aceptar los compromisos de confidencialidad definidos en la institución, estos compromisos deberán ser expuestos en su proceso de inducción o capacitación del personal. Los compromisos determinaran el buen uso de la información por parte del usuario. De igual manera los contratistas en su proceso de contratación deberán incluir los documentos para verificación de datos personales expedido por la Policía nacional de Colombia.

SEGURIDAD DE LA INFORMACIÓN

Con el fin de resguardar la información que pueda ser divulgada de forma no autorizada o manipulada erróneamente por parte de sus funcionarios, el área de sistemas en su proceso lleva a cabo un respaldo de información por medio de la NAS de la institución, La NAS cuenta con dos discos duros los cuales están destinados para el backups de información de los equipos de cómputo y para el backup de la base de datos del sistema de información.

El almacenamiento de las copias de seguridad del sistema de información se realiza cada 24 horas y los backup de los equipos de cómputo se realizan bajo cronograma de actividades de la oficina de sistemas de la E.S.E Hospital de La Vega.

De igual manera, cada una de las áreas de la entidad es responsable de resguardar la información que crean importante para el proceso que llevan a cabo.

En caso de identificarse un incidente de seguridad, este será registrado y notificado a la subgerencia administrativa y se hará la investigación respectiva para determinar las causas y responsables del suceso, posteriormente la entidad tomará las acciones pertinentes para el funcionario y/o tercero que esté vinculado con el incidente. De acuerdo con la naturaleza del evento y la gravedad, la E.S.E Hospital de La Vega en cabeza del gerente se tomará la acción disciplinaria.

ROLES Y RESPONSABILIDADES

El área de Talento Humana será la encargada de diseñar, documentar y actualizar el manual de funciones y competencias de La E.S.E Hospital de La Vega, el manual establece los roles, las responsabilidades y funciones a ser ejecutadas durante el desarrollo de las actividades en la Institución. Para los contratistas y terceros se describirán las responsabilidades en los contratos respectivos que intervienen con el Hospital.

SOCIALIZACIÓN Y EDUCACIÓN SOBRE LA SEGURIDAD DE LA INFORMACIÓN.

La E.S.E Hospital de La Vega por medio de las diferentes herramientas tecnológicas de aprendizaje deberá asegurar que todos los funcionarios conozcan y apliquen los lineamientos para un correcto uso de la información. Actualmente la E.S.E Hospital de La Vega cuenta con una plataforma de aprendizaje (MOODLE), el cual permite que el usuario sea capacitado y certificado sobre el manejo y la aplicación del plan de seguridad y privacidad de la entidad. Adicionalmente permite que el usuario interactúe con consejo básicos para un manejo óptimo de la información.

El proceso de capacitación está enfocado para que el personal asistencial y administrativo sea capacitado y conozca sobre los lineamientos básicos sobre la seguridad de la información.

CONTROL DE INGRESO Y SALIDA DE PERSONAL

Para la entidad el ingreso y la salida de personal debe ser controlado y registrado, por esta razón el personal que ingresa deberá realizar un proceso de inducción en donde cada área de la entidad hace una pequeña explicación del proceso que ejecuta, en el caso del área de sistemas, el personal de la oficina de sistemas deberá realizar la asignación de credenciales al sistema de información, ingresos biométricos, entre otros. Cada asignación de usuario debe ser notificado, la notificación la realiza el proceso administrativo o asistencial. De igual manera se deberá realizar la notificación a la oficina de sistemas para la desvinculación de usuarios que ya no pertenecen a la entidad.

ENTREGA DE ACTIVOS ASIGNADOS

Para la E.S.E Hospital de La Vega es importante velar por los activos de la entidad, por esta razón todo contratista al momento de su retiro o cambio de funciones en la institución debe hacer la entrega de equipo de cómputo asignado, con toda la información contenida en él. El área de sistemas será la encargada de almacenar la copia de seguridad del equipo, se debe tener en cuenta que la información en propiedad de la entidad.

SEGURIDAD FÍSICA

La E.S.E Hospital de La Vega será la responsable de establecer el perímetro de la seguridad física de acuerdo con la clasificación de los activos de la información, controlando el acceso a la información a través de los siguientes controles:

- Acceso a áreas restringidas con chip para el personal asistencial y administrativo, la asignación de chip se realiza bajo solicitud.

- Entrega de chip con número de registro lo cual permite identificar y controlar el personar que ingresa por los accesos biométricos.

El control de acceso disminuye la posibilidad de riesgo de divulgación o perdida de información. El personal con asignación de chip en las áreas seguras y restringidas de la E.S.E Hospital de La Vega deben ser periódicamente revisados, actualizados y monitoreados.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran área de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser

auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

Por último, en caso de retiro o desvinculación laboral del funcionario, éste debe hacer devolución del respectivo chip asignado en desarrollo de sus funciones, previa firma y entrega del documento que certifique su paz y salvo con la entidad.

PROTECCIÓN DE LOS EQUIPOS

Los equipos que hacen parte de la Infraestructura tecnológica de LA E.S.E Hospital de La Vega tales como servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan o brinden servicios de soporte a la información crítica de las áreas, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Adicionalmente, los clientes internos que tengan acceso a los equipos que componen la infraestructura tecnológica de la entidad no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos, el vertimiento de estos puede causar daños a los equipos. De igual manera el traslado de equipos de cómputo se realizará bajo solicitud a el área de sistemas la cual verificará las condiciones técnicas y seguras de la instalación.

Una de las recomendaciones más importantes para la protección de los equipos de cómputo es que el personal que note algún problema de funcionamiento o ataque de virus en una estación de trabajo debe reportarlo de inmediato al personal de Sistemas mediante el uso de los canales de comunicación (Mesa de ayuda, correo electrónico) definidos para ello.

Por otra parte, la entidad debe proveer suministros y equipamiento de soporte como electricidad, aire acondicionado, planta eléctrica y un sistema de alimentación no interrumpida (UPS) que asegure el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información ante una falla en el suministro de cualquiera de estos elementos, evitando así la pérdida o corrupción de información. Estos suministros deben ser monitoreados, revisados

y medidos permanentemente para asegurar su funcionamiento y condiciones normales de operación y evitar futuros daños.

De igual manera, la E.S.E Hospital de La Vega debe establecer un programa de planeación y ejecución de mantenimientos preventivos anuales (como mínimo), a la infraestructura tecnológica.

NOTA

El personal de la E.S.E Hospital de La Vega, no está autorizado a sacar los equipos fuera de la entidad, los equipos son propiedad de la institución, en caso de que un funcionario tome la decisión de llevar un equipo fuera de las instalaciones, el usuario será investigado y podrá ser juzgado en un caso de robo o pérdida de información lo cual permite iniciar un proceso judicial.

CONTROL DE CAMBIOS

Todo cambio que se realice sobre la infraestructura tecnológica para el procesamiento de la información, comunicaciones y seguridad electrónica debe ser controlado, gestionado y autorizado adecuadamente, y debe ser sometido a una evaluación que permita identificar los riesgos asociados que pueden afectar la operación del negocio. El control de cambios se realiza en compañía del área de activos fijos y se realiza el respectivo formato para su nueva asignación.

GESTIÓN DE LA CAPACIDAD DE ALMACENAMIENTO Y PROCESAMIENTO

El área de sistemas en un proceso de mejora continua mantendrá en constante monitoreo el rendimiento y capacidad de la infraestructura tecnológica de procesamiento de información, con el fin de identificar y controlar el consumo de sus recursos y prever su crecimiento de forma planificada.

Periódicamente, se realizarán mediciones de las variables críticas de operación de la infraestructura tecnológica con el objetivo de verificar el estado y uso de los recursos. De esta forma, es posible definir proyecciones de crecimiento que aseguren la integridad de procesamiento y disponibilidad de la infraestructura.

IMPLEMENTACIÓN Y ACTUALIZACIÓN DE SOFTWARE

El área de Sistemas debe asegurar que los requerimientos y criterios, tanto funcionales como técnicos, para la aceptación de nuevos sistemas, actualizaciones y nuevas versiones de software estén claras y adecuadamente definidos, documentados y aprobados acordes a las necesidades

de la entidad. Estos nuevos requerimientos, actualizaciones y/o nuevas versiones de tecnología, sólo deben ser migrados al ambiente de producción después de haber sido formalmente aceptados de acuerdo a las necesidades técnicas y funcionales establecidas por el administrador del sistema de información.

Todo sistema que se implemente o instale, sea comprado o en comodato, debe tener la capacidad de integrarse al sistema corporativo y será evaluado por el área de Sistemas para verificar su buen funcionamiento y los procedimientos de mantenimiento y soporte de la solución.

PROTECCIÓN DE INFORMACIÓN ANTE POSIBLE SOFTWARE MALICIOSO

La E.S.E Hospital de La Vega anualmente proporciona presupuesto para la compra de herramientas para la protección de datos, por este motivo todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional.

De igual manera, La E.S.E Hospital de La Vega define que no están permitidas las siguientes acciones:

- El funcionario no tiene permitido la desinstalación y/o desactivación de software y herramientas de seguridad.

- El funcionario no tiene permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

- El funcionario no tiene permitido utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo. Si estos medios son requeridos por la organización, deben se provisto por ella con previa autorización del área de Sistemas.

COPIAS DE SEGURIDAD

Como anteriormente se mencionó en el ítem de seguridad de la información la entidad almacena sus copias de seguridad en la NAS de la entidad, el área de sistemas es responsable de salvaguardar dicha información, pero se debe tener en cuenta que dicha información se debe restaurar con el fin de hacer una verificación de la información guardada. La oficina de sistemas establece un plan de restauración y seguimiento de copias de seguridad del sistema de información, cuando se verifica el estado de la información el líder de sistemas dará el visto bueno

en el registro de copias de seguridad. Se debe tener presente que las restauraciones de dichas copias de seguridad se realizan cada 24 o 48 horas.

Por último, es responsabilidad de todo funcionario realizar periódicamente una copia de seguridad de la información almacenada en el disco duro del equipo que le fue asignado, para ello solicitará al área de Sistemas los medios necesarios, los cuales entregará para que sean resguardados de acuerdo con las medidas de protección y seguridad física apropiados.

OBSERVACIONES

- El uso de medios de almacenamiento removibles (ejemplo: CD, DVD, USB, memorias flash, discos duros externos) sobre la infraestructura para el procesamiento de la información de la entidad, estará autorizado para aquellos funcionarios cuyo perfil de cargo y funciones lo requiera.

- El área de Sistemas es responsable de implementar los controles necesarios para asegurar que en los sistemas de información de la E.S.E hospital de La Vega sólo los funcionarios autorizados pueden hacer uso de los medios de almacenamiento removibles. Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de la E.S.E hospital de La Vega.

- Todos los funcionarios de la E.S.E Hospital de La Vega deberán asumir un rol de responsabilidad para llevar a cabo un uso responsable de la información que procesa y produce la entidad.

- Todos los funcionarios deberán reportar cualquier actividad sospecha y que pueda afectar la privacidad y seguridad de la entidad. Los usuarios deberán reportar el evento a la oficina de sistemas.

SEGUIMIENTO, CONTROL Y MEJORA

Las acciones de seguimiento y control serán verificadas por el área de control interno y MIPG dando cumplimento al decreto 612 de 2018.

BIBLIOGRAFIA

Normas ISO. (s. f.). *ISO 27001 - Seguridad de la información: norma ISO IEC 27001/27002*. https://www.normas-iso.com/iso-27001/

CONTROL DE CAMBIOS

APROBACIÓN					
	NOMBRE	**CARGO**	**DEPENDENCIA**	**FECHA**	**FIRMA**
REALIZÓ	Sebastián García	TIC	Sistemas	26/01/2022	
REVISÓ	Jhonnatan Ortega Gómez	Líder Calidad	Calidad	26/01/2022	
APROBÓ	Viviana Clavijo	Gerente	Gerencia	26/01/2022	

CONTROL DE CAMBIOS				
VERSION	**FECHA DE APROBACIÓN**	**DESCRIPCIÓN DEL CAMBIO**	**SOLICITO**	**NOMBRE**
2	26/01/2022	Actualización del documento	TIC	Sebastián García