PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

HOSPITAL SAN JUAN DE DIOS
E.S.E.
PAMPLONA

2024

E.S.E. Hospital San Juan de Dios de Pamplona

Tabla de contenido

INTRODUCCIÓN

La ESE Hospital San Juan de Dios de Pamplona, es consciente que la informaciónes un activo de alto valor, máxime en estas épocas de Pandemia, donde debidoa la obligación del teletrabajoo trabajoen casa, gran parte de la informaciónse encuentra almacenada fuera de la institución, por lo cual se hace necesario definir un sistema de gestión de seguridad de la información que permita garantizar la integridad, confidencialidad y disponibilidadde la información, con el fin de prevenir cualquier tipode ataques o usos fraudulentosde la misma.

Para generar este Plan, es necesario realizar un diagnósticodel estado actual en materia de seguridad de la información, así mimo, identificarlas necesidades de la ESE en este ámbito. Una vez realizado este diagnóstico, se identificanlas debilidades, fortalezas y oportunidadesde mejora, generando una política de seguridad.

El presente documento, expone los lineamientos planteados para implementar las mejoras prácticas de seguridad informática en la ESE, con el fin de optimizar la disponibilidad, la integridad, la confidencialidad, privacidad, entre otros principios relevantes, teniendoen cuenta la infraestructura y limitaciones actuales.

1. OBJETIVO

1.1. OBJETIVO GENERAL

Desarrollar el Plan de Seguridad y Privacidad de la Informaciónpara la ESE Hospital San Juan de Dios de Pamplona.

1.2. OBJETIVOS ESPECIFICOS

- Establecer los lineamientos generales del manejo de la informaciónpara la ESE Hospital San Juan de Dios de Pamplona.
- Generar el Modelode Seguridad y Privacidad de la Información.
- Implementarel Plan de Acción.

2. MARCO LEGAL

El presente documentose realizó basado en la norma ISO – IEC 27001:2013 Sistema de Gestión de la Seguridad de la Información, apoyados en el Plan de Seguridad y Privacidad de la informaciónde la ESE Hospital San Juan de Dios de Pamplona.

3. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es definida por la norma ISO/IEC 27001 como: "La Preservación de la confidencialidad, la integridady la disponibilidadde la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad", este es un concepto que no debe confundirse con la seguridad informática, la cual únicamente se encarga de la seguridad en medios informáticos, teniendoen cuenta que la información puede estar contenidade otras maneras.

Más específicamente, la ISO define integridad, disponibilidad y confidencialidad de la
siguiente manera:

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006].

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006].

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. [NTC 5411- 1:2006].

4. LINEAMIENTOS GENERALES DEL MANEJO DE LA INFORMACIÓN

A continuación, se presenta un diagnóstico del estado actual del manejo de la información en la ESE Hospital San Juan de Dios de Pamplona.

4.1. Gestión de Activos

Con el fin de garantizar la administración y el control sobre los activos de la ESE, cada dependencia debe mantener el inventario actualizado, identificando al propietario de cada elemento, quien debe asegurar la información y los activos asociados con su proceso. Este inventario debe actualizarse siempre que se realice algún desplazamiento de cualquier activo, el funcionario responsable deberá mediante un oficio, informar a almacén y a la oficina de informática y estadística del movimiento que se va a realizar, incluyendo detalladamente los equipos y sus respectivos seriales.

Cuando se presente alguna falla o daño en cualquiera de los activos de información, se debe reportar inmediatamente a la oficina de informática y estadística, quien es el único responsable de hacer el diagnóstico, la reparación o reemplazo del elemento afectado.

Todos los activos de información son propiedad exclusiva de la ESE Hospital San Juan de Dios de Pamplona, de igual manera, es el dueño de la propiedad intelectual desarrollada por los funcionarios y contratistas derivadas del objeto y cumplimiento de funciones y/o de las tareas asignadas. Los administradores de estos activos de

informaciónson funcionarios, contratistas o colaboradores directos y autorizados de la ESE.

Todo cambio, creación, eliminación o modificaciónde programas, aplicativos, formatosy reportes que afecte los recursos informáticos, deben ser solicitados formalmentepor los usuarios a las respectivas Subdirecciones con el fin de que los administradores de los sistemas ejecuten dichas solicitudes.

4.2. Acceso a la información

Cada dependencia de la ESE, debe establecer políticas de acceso a los sistemas de informacióncon el fin de evitar los riesgos asociados al acceso no debidode los mismos.

En caso de que personas o Entidades externas requieran acceder a información específica y confidencial, se debe cumplircon los protocoloslegales establecidos para la transmisión de la informaciónque tiene establecida la ESE.

4.3. Uso de Usuario y contraseñas

La oficina de informática y estadística es la encargada de administrar y generar las contraseñas para el acceso al sistema de informaciónKubapp y gestión documental, a las redes de WI- FI distribuidas en las instalaciones de la ESE, así como la gestión de las contraseñas de los usuarios de los equipos de comunicaciones y las claves iniciales de las cuentas de los correos institucionales.

Cada funcionarioo contratistadeberá tener una clave personal e intransferiblede acceso que le permitiráingresar de formaexclusiva al equipode cómputo asignado para su labor, así como a las bases de datos y a los aplicativos a los que está autorizado. Cabe resaltar que cada funcionario o contratista es responsable del uso de su clave de acceso debiéndola mantener en secreto, ya que cualquier modificación no autorizada de la información, daño o acceso irregular que ocurra y se detecte, es responsabilidad directa del funcionario, pudiendohacerse acreedor a las sanciones de tipolegal y disciplinarioque esto conlleve.

En caso de que el personal requiera algún permiso especial o algún cambio en la configuración de su perfil de Kubapp, estos cambios deben ser autorizados por las Subdirecciones y solicitados por escrito o vía correo electrónico, una vez autorizado, serán ejecutados directamentepor la oficina de Informáticay Estadística.

4.4. Uso de Internet/Intranet de la ESE

El acceso al servicio de Internet/Intranet es utilizado por funcionarios, contratistas o practicantes, cabe resaltar que no hay ningún tipode bloqueode páginas por parte de la Oficina de Informática y Estadística, comprometiendo a los funcionarios a utilizar este activo con responsabilidad y ética laboral.

Todos los funcionarios, contratistas y practicantes con autorización al uso y acceso a estos servicios deben:

- Utilizar este servicio exclusivamente para fines laborales.
- Conservar normas de respeto, confidencialidady criterioético

Descargar documentoso archivo tomando las medidas de precaución es responsabilidad de cada usuario con el fin de evitar el acceso de virus en las redes y equipos informáticos, en caso de necesitar asesoría en este proceso, se debe hacer el requerimiento a la oficina de Informáticay estadística quien debe prestar apoyo.

Está Prohibidoél envió, descarga y/o visualización de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autory/oque atentencontra la buena imagen de la ESEo su Personal.

4.5. Uso de dispositivos de almacenamiento externo

La ESEno restringe el uso de dispositivos de almacenamiento externo a sus funcionarios, teniendo en cuenta su utilidad para transportar y resguardar información, incluso ha facilitado la adquisición de estos dispositivos para su utilización institucional. Sin embargo, es responsabilidad de cada funcionariola correcta utilización de estos medios.

4.6. Seguridad de la Información

Los trabajadores de planta y contratistas son responsables de la información que manejan y deben garantizar su custodia, integridad, confidencialidad, disponibilidad y confiabilidad, evitando pérdidas, accesos no autorizados, exposición, modificación y/outilizaciónindebida de la misma, especialmente si dicha información está protegidaporreserva legal o ha sido clasificada como confidencialy/ocrítica.

El software adquirido y desarrollado por funcionarios o colaboradores de la ESE, es exclusivo para las operaciones de la Institución, estado prohibidasu utilización, copia o venta para fines ajenos a la ESE.

4.7. Uso de Impresoras y Escáneres

La utilización de las impresoras debe estar basada en la política de Hospital Verde adoptada por la institución, primandola impresión a doble cara, la utilización de papel reciclable y los correos electrónicos con el fin de reducir la cantidad de papel gastado. Cabe resaltar que la utilización de las mismas es exclusiva para asuntos laborales, estando prohibido la impresión de documentos personales con los equipos de la ESE.

Cualquier fallo que se presente, debe ser informado a la oficina de informática y estadística, la cual realizará las reparaciones correspondientes y, en caso de presentarse malas utilizaciones por parte del personal responsable, se aplicarán las sanciones correspondientes.

4.8. Seguridad Física y en el Entorno

Las áreas designadas para el almacenamiento de los activos de información(Servidores, Routers, Switches, UPS y cableado estructurado), son áreas restringidas cuyo acceso está controladoporel personal de la Oficina de Informáticay Estadística de la ESE.

4.9. Control de Virus Informáticos

La ESE Hospital San Juan de Dios de Pamplona cuenta con un Router Mikrotik, quien tiene configuradoun cortafuegos el cual previene ataques informáticos desde agentes externos a la intranet. En cuanto a los virus de computadoras, los funcionarios deben evitar al máximo la utilización de medios extraíbles de dudosa reputación que puedan infectar los equipos o la infraestructura de red, esto también aplica a los correos electrónicos y mensajes que se reciben de la internety que pueden contener software malicioso.

4.10. Almacenamiento y Respaldo de la Información

La ESE Hospital San Juan de Dios de Pamplona, cuenta con tres copias de seguridad en servidores diferentes del sistema de información Kubapp, el cual contiene las historias clínicas, información de facturación y financiera de la ESE.

Las copias de seguridad de la información local de cada funcionario, es responsabilidad de cada cual, solicitando el apoyo, si es necesario, de la oficina de informática y estadística.

4.11. Revisión equipos externos

La revisión de equipos de cómputo externos se realiza periódicamente por medio de plataformas de conexión remota. Garantizando el buen uso del mismo y vigilando que sea de uso institucional con las herramientas que se manejan en la institución.

5. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones- MINTIC, publica la cartilla del Modelo de Seguridad y Privacidad de la Información, este documento suministra requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información – MSPI,

4.9. Control de Virus Informáticos

con el fin de servir como guía para la implementación del Plan de Seguridad y Privacidad de la Información en las Entidades Públicas.

Esta implementación está directamente relacionada con las necesidades actuales, los requisitos de seguridad, procesos y tamaño de la infraestructura de la ESE, con el fin de promover y preservar la confidencialidad, integridad y disponibilidad de los activos de información.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, contribuir a mejorar los procesos de intercambio de información pública, dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades y Optimizar la gestión de la seguridad de la información al interior de las entidades, entre otras prácticas.

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que la ESE pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Estas fases, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible. En la siguiente figura, se presenta el macro modelo de la descripción del ciclo de operación planteado por el MinTic.

Figura 1. Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información

Componente	Actividades	Responsable	Meta / entregable	Fecha
Planeación	Determinar el estado actual de la gestión de seguridad y privacidad de la información	Oficina de Informática y Estadística	Diagnóstico del estado actual	2022
	Actualizar el inventario de activos de información de la	Oficina de Informática y Estadística	Cuadro de Inventario actualizado	OCT-22
	Actualizar las contraseñas de acceso al sistema Kubapp con el personal activo de ESE.	Oficina de Informática y Estadística	Contraseñas actualizadas	MAR-21
	Inhabilitar el acceso al sistema Kubapp a los usuarios que ya no pertenecen a la ESE	Oficina de Informática y Estadística	Nueva tabla de usuarios con acceso al sistema	Mensual
	Monitorear el consumo del ancho de banda de la red institucional por parte de los funcionarios	Oficina de Informática y Estadística	Control sistemático a través del Router Mikrotik	Quincenal
	Realizar mantenimiento periódico a las impresoras de la ESE	Oficina de Informática y Estadística	Correcto funcionamiento de las Impresoras	Mensual
	Realizar monitoreo permanente del estado de la sala cómputo con su respectivo mantenimiento.	Oficina de Informática y Estadística Personal de servicios generales	Correcto funcionamiento de los equipos de red	Semanal
	Implementar una herramienta informática para automatizar las copias de seguridad en un servidor nuevo	Oficina de Informática y Estadística	Copias de Seguridad realizadas	sep-22
Implementación	Implementación del Plan de Tratamiento de Riesgos	Oficina de Informática y Estadística	Documento con la descripción de los indicadores de gestión de seguridad y	Anual

			privacidad de la información.	
	Realizar la revisión y el seguimiento de ejecución del plan de Tratamiento de Riesgos	Oficina de Informática y Estadística	Informe de avances	Anual
	Evaluación semestral de oportunidades de mejoramiento	Oficina de Informática y Estadística	Informe de oportunidades de mejora	Semestral

Bibliografía

Modelo de seguridad y privacidad de la información, ministerio de tecnologías de la informacióny las comunicaciones- MinTic. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Norma técnica colombiana NTC- ISO/IEC 27001.