PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

ESE HOSPITAL SAN JOSE MARSELLA

VIGENCIA 2020

Carrera 14 N° 16-20 –Telefax: 3685023 - 3685024 – Barrio La Pista - Código Postal: 661040
E-mail: contacto@hospitalsanjosemarsella.gov.co Pag Web: www.hospitalsanjosemarsella.gov.co

INTRODUCCIÓN

El Sistema de Redes de Computadoras e información contenida en el servidor, ordenadores, periféricos y accesorios, utilizados por los funcionarios de cada dependencia de la **ESE Hospital San José Marsella,** están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos factores de riesgos humanos y físicos.

OBJETIVO

El Plan de Seguridad y Privacidad de la Información de la **ESE Hospital San José Marsella**, tiene los siguientes objetivos:

General

Garantizar la seguridad y el respaldo del sistema de información (Bases de datos, información contable, documentos de Excel y Word, etc.) de la **ESE Hospital San José Marsella,** mediante la aplicación del plan de contingencia informático institucional.

Específicos

- Enseñar a los funcionarios a utilizar las herramientas tecnológicas para minimizar el riesgo de pérdida de información.
- Implementar políticas de buen manejo y seguridad de la información.

ALCANCE

La Política de Seguridad de la Información aplica para todos los usuarios internos en todos los niveles jerárquicos, usuarios externos, proveedores y terceros; que produzcan, administren, custodien o que tengan acceso a la información de la Administración Central.

La Red de la **ESE Hospital San José Marsella,** cuenta con Tecnologías de la información (TI) en lo referente a: Sistemas de comunicación, sistemas de información y servicios Informáticos que se brinda de forma interna a las diferentes Oficinas y Dependencias.

- Servidor de programa institucional: ZEUS.

- Servidor de Internet.
- Extensor de señal WiFi.
- Sistema de vigilancia a través de video-cámaras.

SEGURIDAD DE LA INFORMACION Y PROTECCIÓN DE DATOS

En la Seguridad Informática se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos. Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección.

Sin embargo, hay que destacar que, aunque se diferencia entre la Seguridad de la Información y la Protección de Datos como motivo u obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas.

En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación no autorizada.

La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo, existen más requisitos como por ejemplo la autenticidad entre otros.

El motivo o el motor para implementar medidas de protección, que responden a la Seguridad de la Información, es el propio interés de la institución o persona que maneja los datos, porque la pérdida o modificación de los datos, le puede causar un daño (Material o inmaterial). Entonces en referencia al ejercicio con el banco, la pérdida o la modificación errónea, sea causado intencionalmente o simplemente por negligencia humana, de algún récord de una cuenta bancaria, puede resultar en pérdidas económicas u otras consecuencias negativas para la **ESE Hospital San José Marsella**.

PROTECCIÓN DE DATOS

En el caso de la Protección de Datos, el objetivo de la protección no son los datos en sí mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta.

Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la **ESE Hospital San José Marsella** o persona que maneja los datos, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información.

En muchos Estados existen normas jurídicas que regulan el tratamiento de los datos personales, como por ejemplo en España, donde existe la "Ley Orgánica de Protección de Datos de Carácter Personal" que tiene por objetivo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor, intimidad y privacidad personal y familiar

Sin embargo, el gran problema aparece cuando no existen leyes y normas jurídicas que evitan el abuso o mal uso de los datos personales o si no están aplicadas adecuada o arbitrariamente.

Pero una buena Gestión de Riesgos no es una tarea única sino un proceso dinámico y permanente que tiene que estar integrado en los procesos (cotidianos) de la estructura institucional, que debe incluir a todas y todos los funcionarios -¡¡la falla el eslabón más débil de la cadena!!- y que requiere el reconocimiento y apoyo de las directivas. Sin estas características esenciales no están garantizadas, las medidas de protección implementadas no funcionarán y son una pérdida de recursos.

AMENAZAS Y VULNERABILIDADES

AMENAZAS

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información.

Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

Desde el punto de vista de la entidad que maneja los datos, existen amenazas de origen externo como por ejemplo las agresiones técnicas, naturales o humanos, sino también amenazas de origen interno, como la negligencia del propio personal o las condiciones técnicas, procesos operativos internos.

Generalmente se distingue y divide tres grupos

- **Criminalidad:** Son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.

- **Sucesos de origen físico:** Son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.

- **Negligencia y decisiones institucionales:** Son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

Existen amenazas que difícilmente se dejan eliminar (virus de computadora) y por eso es la tarea de la gestión de riesgo de preverlas, implementar medidas de protección para evitar o minimizar los daños en caso de que se realice una amenaza.

VULNERABILIDADES

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades en grupos característicos: Ambiental, Física, Económica, Social, Educativo, Institucional y Política.

ANALISIS DE RIESGO

El primer paso en la Gestión de Riesgo es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

CLASIFICACION Y FLUJO DE INFORMACION

La clasificación de datos tiene el propósito de garantizar la protección de datos (personales) y significa definir, dependiendo del tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso a los datos e informaciones. Considerando el contexto de nuestra misión institucional, tenemos que definir los niveles de clasificación como por ejemplo: confidencial, privado, sensitivo y público. Cada nivel define por lo menos el tipo de persona que tiene derecho de acceder a los datos, el grado y mecanismo de autenticación.

Una vez clasificada la información, tenemos que verificar los diferentes flujos existentes de información internos y externos, para saber quiénes tienen acceso a qué información y datos.

Clasificar los datos y analizar el flujo de la información a nivel interno y externo es importante, porque ambas cosas influyen directamente en el resultado del análisis de riesgo y las consecuentes medidas de protección. Porque solo si sabemos quiénes tienen acceso a qué datos y su respectiva clasificación, podemos determinar el riesgo de los datos, al sufrir un daño causado por un acceso no autorizado

ANALISIS DE RIESGO

Existen varios métodos de como valorar un riesgo y al final, todos tienen los mismos retos -las variables son difíciles de precisar y en su mayoría son estimaciones- y llegan casi a los mismos resultados y conclusiones.

En el ámbito de la Seguridad Informática, el método más usado es el Análisis de Riesgo.

La valoración del riesgo basada en la fórmula matemática Riesgo = Probabilidad de Amenaza x Magnitud de Daño.

Para la presentación del resultado (riesgo) se usa una gráfica de dos dimensiones, en la cual, el eje-x (horizontal, abscisa) representa la "Probabilidad de Amenaza" y el eje-y (vertical, ordenada) la "Magnitud de Daño". La Probabilidad de Amenaza y Magnitud de Daño pueden tomar condiciones entre Insignificante (1) y Alta (4). En la práctica no es necesario asociar valores aritméticos a las condiciones de las variables, sin embargo facilita el uso de herramientas técnicas como hojas de cálculo.

MAGNITUD DE DAÑO

Cuando hablamos de un impacto?	Como valorar la Magnitud de Daño?
• Se pierde la información/conocimiento. • Terceros tienen acceso a la información/conocimiento. • Información ha sido manipulada o está incompleta. • Información/conocimiento o persona no está disponible. • Cambio de legitimidad de la fuente de información.	• Consideración sobre las consecuencias de un impacto. - Quien sufrirá el daño? - Incumplimiento de confidencialidad (interna y externa) - Incumplimiento de obligación jurídica/contrato/convenio - Costo de recuperación (imagen, emocional, recursos, tiempo, económicos. • Valoración de magnitud del daño - Bajo: Daño aislado, no perjudica ningún componente de la organización - Mediano: Provoca la desarticulación de un componente de la organización. A largo plazo puede provocar desarticulación de la organización. - Alto: En corto plazo desmoviliza o desarticula la organización.

Se habla de un Impacto, cuando un ataque exitoso perjudicó la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones

Estimar la Magnitud de Daño generalmente es una tarea muy compleja. La manera más fácil es expresar el daño de manera cualitativa, lo que significa que aparte del

daño económico, también se considera otros valores como daños materiales, imagen, emocionales, entre otros. Expresarlo de manera cuantitativa, es decir calcular todos los componentes en un solo daño económico, resulta en un ejercicio aún más complejo y extenso.

Aunque conozcamos bien el impacto de un ataque exitoso, sus consecuencias pueden ser múltiples, a veces son imprevisibles y dependen mucho del contexto donde manejamos la información, sea en una ONG (derechos humanos, centro de información etc.), en una empresa privada (banco, clínica, producción etc.), en una institución Estatal o en el ámbito privado. Otro factor decisivo, respecto a las consecuencias, es también el entorno donde nos ubicamos, es decir cuáles son las leyes y prácticas comunes, culturales que se aplica para sancionar el incumplimiento de las normas.

OBTENCION Y ALMACENAMIENTO DE COPIAS DE SEGURIDAD (BACKUPS)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la **ESE Hospital San José Marsella**. Las copias de seguridad son las siguientes:

- Backup del servidor Z que incluye, programas y montaje del programa Xenco, que cuenta con los programas ejecutables de cada módulo los controladores para el correcto funcionamiento de este.
- Backup del servidor T: Se Guarda aquí por dependencias, que almacena la información en red de cada área administrativa y asistencial de la **ESE Hospital San José Marsella**.
- Backup del software Oracle: contiene la información financiera contable y clínica de la **ESE Hospital San José Marsella**.

Estas copias de seguridad deben ser realizadas por la persona encargada del área de sistemas en un disco externo y debe ser alojada en un lugar (a determinar por la Gerencia) externo a las instalaciones.