Módulo Teórico-Práctico

Actividad en contexto

Módulo
Teoría de Seguridad de la Información
Nombre de la entrega
Invertir en seguridad: una oportunidad para crecer empresarialmente
Nivel académico
Especialización
Tipo de entrega
Análisis de un caso práctico

Nota

Tenga en cuenta que el tutor le indicará qué herramienta requiere y qué estrategia deberá desarrollar para evidenciar su participación individual en un trabajo colaborativo.

DESCRIPCIÓN DE LA ACTIVIDAD

En esta actividad se presenta un caso práctico para que el estudiante analice la situación y proponga soluciones frente a la problemática planteada.

CASO O PROBLEMA

Asesorías Integrales y Procesos Administrativos AIPAD SAS es una empresa colombiana de tipo familiar dedicada a la tercerización de servicios administrativos.

La principal línea de negocio es Gestasalud, cuyo objetivo es integrar servicios administrativos en salud, que a través de su gestión permite una ágil y adecuada ejecución de los parámetros indicados por el Sistema General de Seguridad Social en Salud, aplicando para ello procesos que permiten presentar la información de acuerdo a los estándares políticos, económicos, medioambientales y tecnológicos establecidos por la normatividad, contribuyendo con el sostenimiento financiero de nuestros clientes.

Los servicios prestados para cumplir con dicho objetivo son:

- Minimizar a los clientes, los tiempos de ejecución de los trámites que están establecidos por el Sistema General de Seguridad Social en Salud.
- Integrar soluciones tecnológicas y procesos administrativos eficientes que permitan el mejoramiento continuo de las actividades de manejo y procesamiento de la información en el sector salud.

- Monitorear el movimiento del marco legal que rige el sector salud con el fin de garantizar una respuesta oportuna frente a los cambios y la correcta aplicación de la normatividad.
- Diseñar e implementar un Sistema de Gestión de Calidad que permita la medición y el mejoramiento continuo de cada uno de los procesos de la empresa.
- Diseñar e implementar un Sistema de Gestión de Seguridad de la información, que genere mayor confiabilidad a los clientes para el manejo de la información.

» Servicios

AIPAD S. A. S. ha caracterizado los servicios de cada una de sus líneas de negocio. Se ha concentrado principalmente en el servicio **ECAT**, por ser el servicio de mayor demanda en el mercado, cuyos costos operativos son relativamente bajos y que genera utilidades por proyecto del 15 al 20%.

El servicio se describe a continuación:

FICHA TÉCNICA						
GESTION DE SERVICIOS ADMINISTRATIVOS EN SALUD	GESTIÓN DE SERVICIOS ADMINISTRATIVOS DE SALUD SERVICIO RECLAMACIONES POR EVENTOS CATASTRÓFICOS Y/O ACCIDENTES DE TRÁNSITO ECAT					AIPAD SAS
VERSIÓN :	3	CÓDIGO:	ECAT 001	FECHA DE ACTUALIZACIÓN:	03/03/2017	PAGINA 1 DE 1
1. DEFINICIÓN :	Trámite de la documentación generada por las IPS al prestar servicios catalogados como eventos catastróficos o accidentes de tránsito ante e FOSYGA, con el fin de recaudar eficazmente los dineros provenientes de dichos servicios a nuestros clientes.					
2. OBJETIVO:	Garantizar a nuestros clientes la efectividad en la presentación de los documentos ante el FOSYGA para obtener el máximo valor de recaudo por los servicios prestados (ECAT) en el menor tiempo posible					
3. ALCANCE:	De acuerdo a la normatividad vigente para el recaudo (organización , análisis y verificación de la información brindada por el cliente, digitación de la misma, creación de estructuras para los formatos exigidos por el FOSYGA y presentación de medios					
	3 TRAZABILIDAD PARA EL ALCANCE DEL SERVICIO :					
	ACTIVIDAD					RESPONSABLE
3.1	Recepción y registro de la documentación en el sistema					Gestión Documental
3.2	Revisión de la documentación y/o ejecución de los procedimientos propios de la verificación					Coordinador Ecat - Direccion Operativa
3.3	Digitación de la información depurada en el paso anterior					Digitador
3.4	Auditoria de Calidad de las cuentas digitadas					Gestión de Calidad
3.5	Creación de estructura para formatos solicitados					Coordinadr de Proyecto
3.6	Validación de Estructura Malla validadora					Coordinadr de Proyecto
3.7	Generación del Medio Magnético para presentación ante el FOSYGA					Auxiliar de Soporte
3.8	Presentación ante el FOSYGA					Auxiliar de Soporte
4. NECESIDADES Y EXPECTATIVAS DEL CLIENTE:	Garantizar la prestación del servicio con un alto grado de efectividad a un precio justo y en el menor tiempo posible					
5. CARACTERÍSTICAS DEL SERVICIO:	Accesibilidad, oportunidad, continuidad, idoneidad , seguridad , pertinencia, suficiencia, integridad, eficacia, eficiencia, efectividad, confiabilidad, satisfacción del cliente , productividad, tecnologia					
6. REGISTROS PARA EL CONTROL:	Registro de competencia del personal, registro documentación que ingresa, registro de documentación depurada, registro documentación digitada, registro control de temperatura y humedad en oficina de registro, registro de auditorías de calidad, registro documentación presentada ante el FOSYGA, registro recaudo efectivo					
FECHA DE EMISIÓN:	Junio de 2013					
ELABORÓ:	Alexandra Peña Daza	REVISÓ:	Guillermo Gonzalo Peña	APROBÓ:	Liliana Peña Daza	
CARGO:	Director de TI y Planeación	CARGO:	Director Comercial	CARGO:	Director Operaciones	

» Tecnología

Para la prestación de los servicios en AIPAD, se ha tenido en cuenta la tecnología como factor diferenciador para el cumplimiento de su propuesta de valor:

Por tal motivo se cuenta con los siguientes recursos, los cuales se espera ampliar para mejorar tiempos de respuesta, oportunidad en el servicio, fidelización de clientes y obtención de clientes nuevos.

» *Software*

El *software* fue un desarrollo a la medida, diseñado y elaborado por un grupo de ingenieros calificados para tal fin, bajo el lenguaje de programación Cobol Versión gráfica. Este s*oftware* es altamente utilizado por entidades financieras gracias a su nivel de seguridad.

Actualmente se encuentra instalado en el equipo servidor de la empresa y el acceso al mismo por parte de los demás usuarios se realiza por medio de un recurso compartido por red.

Adicionalmente, el software permite la inclusión de información importante por medio de tablas que luego es utilizada en los registros presentados anteriormente. Esto facilita la labor de digitación y agiliza dicho proceso para elaborar mas cuentas en el menor tiempo y minimiza los errores que en digitación se pueden cometer.

» Red empresarial

La red es de tipo empresarial constituida por un *router* de proveedor de servicios de Internet, un *firewall* perimetral para seguridad en la navegación y un *switch* que suministra el acceso al aplicativo por parte de todos los equipos. Se cuenta con un direccionamiento público para uso de VPN por parte del personal que trabaja en *Outsourcing* y direccionamiento privado clase C. Cuenta con un servidor físico y dos máquinas virtuales, una para aplicaciones y otra para base de datos. El servidor tiene 2 discos duros configurados en RAID-1 y un tercer disco para cambio inmediato en caso de falla.

» Soluciones de seguridad

Actualmente, AIPAD SAS cuenta con esquema de seguridad, compuesto por un dispositivo de seguridad perimetral que permite control sobre la navegación y establecimiento de VPN hacia la red de AIPAD. Tiene un sistema de alarmas para ingreso a las oficinas operativas. Un antivirus para control de seguridad a nivel de EndPoint. Se cuenta con regulador de voltaje para evitar picos eléctricos que pueden afectar el acceso al recurso compartido.

» Gestion de *backup*

Se realiza un *backup* diferencial y un backup Incremental semanalmente, a través del *software Cobian Backup* 11. El *backup* es almacenado en tres fuentes diferentes, servidor físico, nube (Mega) y disco duro externo. Existe una política de *backup*.

» Políticas, procesos y procedimientos y formatos

AIPAD cuenta con una política de calidad, política de salud ocupacional, políticas de tratamiento de datos personales y política de gestión de *backup*.

Los procesos se encuentran definidos, de acuerdo al mapa de macroprocesos. Así mismo los servicios están plenamente caracterizados, según las líneas de negocio definidas.

Cada contrato en AIPAD es manejado como un proyecto, por lo cual cuenta con los siguientes formatos para el desarrollo de sus proyectos.

1. Acta de Inicio
2. Registro de Interesados
3. EDT
4. Cronograma
5. Plan General para la Gestión de Proyectos
6. Seguimiento y control de alcance, tiempo y costo
7. Lecciones aprendidas
8. Cierre de proyectos

Adicionalmente, para temas operativos, se cuenta con los siguientes documentos:

1. Descripción de roles
2. Manual de funciones
3. Lineamientos de contratación
4. Base de datos de clientes, proveedores y empleados
5. Campañas de *marketing* por línea de negocio
6. Plantilla de propuestas comerciales

7. Plantilla de Informes mensuales de operación
8. Monitores y control financiero
9. Evaluación de desempeño
10. Encuesta de satisfacción de clientes

» Cumplimiento norma ISO 27001

- AIPAD SAS cuenta con un procedimiento para la selección de personal, en el cual se revisan antecedentes penales. No hay un procedimiento claro para retiros.
- No se ha realizado un proceso claro para la identificación de activos.
- AIPAD cuenta con un sistema de alarmas con 3 personas autorizadas para el cierre de la oficina. No cuenta con cámaras o control de acceso físico. No se pueden ingresar a las oficinas sin la llave correspondiente. Solo 3 personas tienen dichas llaves. Cada PC tiene contraseña por usuario. El acceso a la carpeta compartida donde se encuentra el *software* de trabajo no cuenta con privilegios de seguridad.
- Los proveedores y aliados firman un acuerdo de confidencialidad.
- Los empleados firman acuerdo de confidencialidad.
- La empresa quiere implementar el sistema de Gestión de Seguridad de la información para la parte operativa de la línea de negocio GESTASALUD.
- La empresa se encuentra en desarrollo de *Help Desk* y manejo de personal.
- La empresa quiere implementar el sistema de gestión de calidad ISO 9001:2015.

PLANTEAMIENTO **DE LA ACTIVIDAD**

De acuerdo con el escenario indicado, responda los siguientes cuestionamientos:

1. Identifique por lo menos 3 activos de información importantes para la empresa
2. Confirme en qué medida la norma ISO 27001:2013 ayudaría a la empresa a tomar medidas con respecto a seguridad.
3. Si la empresa no realiza un ejercicio de implementar políticas de seguridad, ¿cómo se verían afectados cada uno de los principios? Mencione por lo menos 2 situaciones de afectación por cada principio.
4. De acuerdo con la afectación de los principios y los activos indicados, indique una vulnerabilidad, amenaza y riesgo por cada activo.
5. Mencione posibles ataques a los cuales estaría expuesta la empresa, si no se toman acciones para mejorar la gestión de la seguridad.