**Interpretaciones de las Encuestas Anexo 1**

##### 3.1.1.1 Resultados en la Tabulación de la Encuesta N°:1 (Dominio 5.- Políticas de Seguridad de la Información.).

En consecuencia de evaluar los resultados del primer instrumento (Encuesta 1) se concluyó que se debe elaborar prioritariamente una normativa de políticas de seguridad informática, que maneje un control de versiones y al culminando su creación y posteriores actualizaciones se debe oportunamente dar a conocer al talento humano de su existencia por resolución de la gerencia administrativa.

##### 3.1.1.2 Resultados en la Tabulación de la Encuesta N°:2 (Dominio 6.- Aspectos Organizativos de la Seguridad).

Analizando los conclusiones especificas en la Encuesta 2; se establece la siguiente resolución; Es conveniente la asignación del SGSI al Departamento de Sistemas y este necesita un asesoramiento de expertos en términos de Normativas de Seguridad, que permita garantizar los principios de seguridad y a la vez viabilizar el desarrollo de la investigación para la implementación del Plan de Seguridad Informática.

##### 3.1.1.3 Resultados de la Tabulación de la Encuesta N°:3 (Dominio 7.- Gestión de Activo).

Como conclusión de este apartado basado en los resultados de la encuesta N°:3 se infiere lo siguiente: se necesita implementar un control en el Sistema SYSCISEPRO para permitir restringir el acceso del talento humano al inventario de los activos incluidos en este dominio.

##### 3.1.1.4 Resultados de la Tabulación de la Encuesta N°:4 (Dominio 8.- Seguridad Ligada a los Recursos Humanos).

Basado en el análisis e interpretación de los datos estadísticos de la encuesta N°:4 se resuelve estipular procedimientos para mitigar el porcentaje de incidentes informáticos.

##### 3.1.1.5 Resultados de la Tabulación de la Encuesta N°:5 (Dominio 9.- Seguridad Física y del Entorno).

Después de valorar los resultados estadísticos de la encuesta N°:5 se concluyó que no existen vulnerabilidades física latentes; por lo que no aplica controles para este dominio dentro de las políticas de seguridad informática.

##### 3.1.1.6 Resultados de la Tabulación de la Encuesta N°:6 (Dominio 10.- Gestión de Comunicaciones y Operaciones).

Evaluando las interpretaciones estadísticas se detectó la vulnerabilidad en los accesos a la red local y medios de almacenamiento por lo que es conveniente establecer un control para estos apartados.

##### 3.1.1.7 Resultados de la Tabulación de la Encuesta N°:7 (Dominio 11.- Control de Acceso).

Analizando todo el apartado de este instrumento se llega a la conclusión que para el control de acceso no existen mayor vulnerabilidad; con la excepción de que se debe actualizar las políticas de control de acceso para amenorar el 33% que respondieron No en la Pregunta 2, para la aplicación de políticas eficientes en el control del acceso.

##### 3.1.1.8 Resultados de la Tabulación de la Encuesta N°:8 (Dominio 12.- Adquisición, Desarrollo y Mantenimiento de Sistemas).

Como resultado de analizar los datos estadísticos del apartado se concluye que para este dominio no se necesita estipular un control, sino establecer una política que permita verificar los existentes para auditarlos.

##### 3.1.1.9 Resultados de la Tabulación de la Encuesta N°:9 (Dominio 13.- Gestión de Incidentes en la Seguridad de la Información).

Cabe resaltar que el resultado del análisis de esta encuesta, concluye que aunque no existan controles formales para registrar e informar los incidentes informáticos y pese a no existir planes de respuesta y contingencia el universo cree conveniente recolectar las evidencias en cada hecho que se suscite, que permita instigar una solución (plan de respuesta y contingencia) con la necesidad de emplear una herramienta para registrar los sucesos informáticos.

##### 3.1.1.10 Resultados de la Tabulación de la Encuesta N°:10 (Dominio 14.- Gestión de la Continuidad del Negocio).

En consecuencia de la Pregunta 1 el 100% de los encuestados también respondió no en la Pregunta 2 referente a las pruebas de continuidad del negocio, mantenimiento y evaluación de los procesos informáticos; por lo que finalmente se acuerda conveniente la creación de una política o control para enmendar este Dominio.

##### 3.1.1.11 Resultados de la Tabulación de la Encuesta N°:11 (Dominio 15.- Cumplimiento).

Concluyendo el análisis de cada una de las preguntas se define que aunque en la empresa CISEPRO existan políticas la protección de la información; estas solamente abarcan el Sistema de Gestión de Integrado (SGI) y no son políticas acorde para aplique controles de seguridad informática; ni se basados en un estándar certificado para este proceso, por lo que las políticas que se desarrollen deben poder gestionar las auditorias informáticas que se realicen por el departamentos de sistemas y además manejar el inadecuado empleo de los recursos tecnológicos.