Seguridad de Información y Continuidad
de Negocio
Gerencia General

RESUMEN EJECUTIVO

PLAN DIRECTOR DE SEGURIDAD DE INFORMACIÓN
2019 – 2025

Resumen

Presenta resultado del estudio de Brechas de Seguridad de Información, el análisis de resultados y propone una serie de Planes de Acción basados en el catálogo del Plan de Seguridad que el área de Seguridad que se generó el 2019, con el objetivo de dar respuesta a las necesidades internas de Seguridad de la Información.

Uso Interno Solamente **Comité Seguridad**

Versión: 1.0	PDSI
	Autor: Joel Serey
Fecha de edición: 01.03.2019	**Fecha de impresión:**

INDICE

1 INTRODUCCIÓN 3

2 ASPECTOS RELEVANTES 4

3 POSICIONAMIENTO FRENTE AL ESTÁNDAR ISO 27001 ..... ERROR! BOOKMARK NOT DEFINED.

4 PROPUESTA DE PROYECTOS (BREVE DESCRIPCIÓN) 6

1 Introducción

Como resultado de la aplicación del Plan Director de Seguridad y la necesidad de evaluar el grado de avance en la materia de Protección de la Información, PGA ha realizado un estudio de Brechas respecto de la Norma ISO 27001 / ISO 17799, a fin de establecer un **Plan Director de Seguridad de Información** (PDSI) cuyo desarrollo se enmarca en el ejercicio de los próximos 5 años.

Los planes propuestos en el Marco del Plan Director de Seguridad de Información asumen las siguientes limitaciones:

- El tiempo disponible para dedicar al desarrollo de este estudio de brechas de seguridad no permitió obtener una aproximación fina al plan de acción.

- El estudio de brechas de seguridad se ha basado principalmente en la realización de entrevistas y en el análisis de la documentación recogida, a partir de lo cual se han obtenido las apreciaciones y conclusiones que fundamentan los planes de acción. El grado de adhesión a la norma queda, por lo tanto, sujeto a la veracidad y completitud de la información proporcionada en su oportunidad.

Esta es la primera versión del documento y podrá sufrir variaciones conforme requiera ser refinado por todos los departamentos afectados en la Organización.

En función de estos refinamientos, se irán produciendo versiones parciales. La primera versión estable consensuada por todos los departamentos implicados.

2 Aspectos Relevantes

La premisa fundamental que gatilla la implementación anterior de un Plan Director de Seguridad, eminentemente tecnológico, era la existencia de nuevos riesgos que aumentaban del grado de inestabilidad y de incertidumbre de los procesos de negocio.

Una vez cerrado el PDS, se hace necesario evaluar el grado de avance, lo que gatilla la realización de este estudio y con él, la creación de un plan de acción mucho más transversal a la organización y basado en la nueva versión de la Norma ISO 17799.

El gráfico muestra el resultado de la evaluación, cuyo detalle se encuentra en el documento ***Informe Evaluacion ISO 27001,*** enviado a los Gerentes noviembre de 2018.

Este nuevo plan ha sido denominado **Plan Director de Seguridad de Información**, para mantener una coherencia con su predecesor.

Se destacan como aspectos relevantes a tomar en cuenta:

- A partir de los antecedentes recopilados, el cumplimiento promedio de los dominios revisados de la Norma ISO 27001 corresponde a un 46%, lo que representa un **nivel medio** de adhesión a la norma.

- Los resultados obtenidos se explican principalmente por los dominios de control relacionados con Tecnologías de la Información, que representan un nivel de cumplimiento significativamente mayor al promedio general verificado.

- La cobertura de las políticas existentes, es cercana al 30% de los dominios contenidos en la norma, los mecanismos de difusión son deficientes, y los procesos de inducción no consideran aspectos

1 Resultado Evaluación Brechas ISO 17799, PGA

de seguridad de información.

- La ausencia de una definición formal de propiedad y responsabilidad sobre los activos de información.

- Los planes de continuidad son aplicados a las unidades negocios, llegando en la actualidad a una cobertura de sólo el 50%, y no contempla la existencia de un plan de continuidad central que gestione la crisis. El reconocimiento de los procesos críticos no se encuentra formalizado y no corresponde a criterios basados en la seguridad de la información.

- El proceso definido para la selección de personal, requiere un fortalecimiento en la definición de perfiles de los candidatos, en la inclusión de condiciones relativa al manejo de información sensible, y en la rigurosidad de la validación de los antecedentes presentados por los candidatos.

- La presencia de software no licenciado en las estaciones de trabajo de los usuarios, expone a la organización a multas de parte de las entidades controladoras.

- La contratación de servicios externos, debe ser vista como una transferencia de funciones operativas a un tercero, y no como una transferencia de responsabilidades sobre los procesos, ya que éstas siempre deben permanecer en el interior de la organización, lo que exige la implementación de rigurosos controles de seguridad.

Se definió que el uno por ciento de los controles no es aplicable a la realidad de la empresa.

No fueron evaluados controles que representan el uno por ciento del total sugerido por la norma.

3 Propuesta de Planes de Acción

Consecuentemente con el resultado del estudio de Brechas 2018, se hace necesario concentrar los esfuerzos en aumentar el nivel de seguridad de los todos los temas evaluados, haciendo un esfuerzo adicional en los cuatro peor evaluados.

1. Completar la publicación de Políticas y Normas de Seguridad de Información, cubriendo todos los tópicos recomendados por el estándar.

2. Mejorar la difusión del sistema normativo y la educación en temas de seguridad al interior de la organización.

3. Establecer mecanismos de medición periódico de la efectividad de la aplicación de los controles de seguridad de información establecidos. Auditorias.

4. Fortalecer la organización de seguridad existente, involucrando a la alta gerencia en temas de decisión estratégica.

5. Establecer un mecanismo para inventariar activos de información indicando su grado de criticidad y exposición al riesgo. Definición formal de procesos críticos y su grado de exposición al riesgo.

6. Generar procedimientos para la gestión de información crítica o confidencial, considerando los diferentes medios de almacenamiento y las actividades de riesgo asociadas tales como:

    a. Copia
    b. Almacenamiento
    c. Transmisión
    d. Destrucción

7. Fortalecer los procesos de seguridad de información asociados a la selección, contratación y desvinculación de personal, incorporando responsabilidades formales respecto del tratamiento de los datos en el ejercicio de la labor cotidiana, gestión de accesos a sistemas e instalaciones y comunicación al resto de la organización de desvinculaciones recientes.

8. Relacionado con el anterior, es necesario formalizar el circuito de aprovisionamiento de usuarios en sistemas críticos de la compañía, que incluya procedimientos de revisión periódicos de los usuarios definidos en los sistemas.

9. Revisar y mejorar la formalización de segregación de funciones, en atención a los cambios de estructura que ha implementado la Gerencia General.

10. Gestión y administración de incidentes de seguridad, registro de fallas en sistemas críticos, base de conocimiento.

11. Implementación del uso de firma digital.

12. Mejorar y fortalecer la recolección, almacenamiento y protección de registros de sistema (log)

13. Definir y formalizar el uso de criptografía en los sistemas de información.

14. Fortalecer las políticas y normas orientadas a la seguridad de empresas externas que se relacionan con PGA para disminuir los riesgos a los que se expone la información que se intercambia con ellos.

15. Generación e implementación de un ISMS, incluyendo un sistema de seguimiento de la implementación de planes de acción en materia de riesgos latentes de seguridad de información.

16. Mejorar el proceso de control de acceso físico a los centros de procesamiento de datos.

4 Metas y Resultados esperados

Una vez establecidos los planes de acción, éstos deben ser sujeto de una decisión de prioridad por parte de la Gerencia General para conformar el Plan Director de Seguridad de Información definitivo. El área de Seguridad podrá entonces realizar un trabajo de ingeniería de detalles, que permitirá planificar en profundidad y valorizar cada proyecto.

Una vez realizada esta tarea se podrá proponer la solicitud de presupuestos necesaria en cada año según la prioridad asignada anteriormente.

La realización de este PDSI permitirá disminuir la brecha en cada tema abordado en el estándar y se espera que una vez realizado, se aumentará en un 25% el grado de cumplimiento con el ISO 17799, esto es, pasar desde un 46% a un 57% o 60%.

La planificación considera un período de 4 años para cumplir el objetivo planteado.

HOJA DE CONTROL DOCUMENTAL

Nombre del Archivo y ubicación original:	PDSI PGA y Filiales
Plantilla del documento:	Resumen Ejecutivo
Código Identificación:	
Clasificación de Seguridad: ***(Ver Normativa de Clasificación de información)***	Uso Interno Solamente
Ámbito de Distribución:	Comité Seguridad

Circuito de aprobación						
	Autor: GCL		**Revisado por:**		**Aprobado por:**	
	Fecha:	**Firma:**	**Fecha:**	**Firma:**	**Fecha:**	**Firma:**

Control de Versiones			
Vers.:	**Rev.:**	**Fecha:**	**Detalles:**
0	0		Versión de distribución inicial creada por Joel Serey (Asesor Externo).

Lista de distribución		
Nº	**Receptor:**	**Organización:**
1		
2		
3		
4		
5		
6		