ANEXO N°20
INFORME DE AUTOEVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Para informar acerca de la autoevaluación de Gestión de la Seguridad de la Información, establecida en el Capítulo I, Título V del Libro VII, del Compendio de Normas del Seguro de la Ley N°16.744, se ha definido la tabla "Autoevaluación de la Seguridad de la Información" que a continuación se especifica.

El organismo administrador podrá anexar información que considere pertinente para dar mayor nivel de detalle a lo informado.

Los campos específicos a reportar son los siguientes:

a) Resultado de autoevaluación: deberá indicar para cada pregunta, el estado en el que se encuentra el cumplimiento de acuerdo a las siguientes opciones:
   i) Cumple: El organismo administrador cumple con la implementación de las accionesdefinidas para el tema especificado.

   ii) Cumple parcialmente: El organismo administrado cumple parcialmente con la implementación y ejecución del tema especificado.

   iii) No cumple: El organismo administrador no ha implementado ni ejecutado el tema especificado.

b) Descripción del fundamento de la Autoevaluación: incluir el fundamento que explique y justifique la evaluación establecida por el organismo administrador.

Tabla: Autoevaluación de la Seguridad de la Información			
	Pregunta	Resultado de autoevaluación	Descripción del fundamento de la autoevaluación
1	El organismo administrador ha implementado medidas técnicas y de organización para gestionar los riesgos de seguridad de la información y ciberseguridad de las redes, equipos y sistemas que utilizan para el otorgamiento de las prestaciones. Detallar las medidas		
2	El organismo administrador ha determinado las medidas de gestión que garanticen la disponibilidad, integridad y confidencialidad de la información. Detallar las medidas.		

3	El organismo administrador cuenta con una política de seguridad de la información y ciberseguridad, establecida por el Directorio o la Dirección.		
4	El organismo administrador ha realizado un levantamiento de los activos de Información críticos. Adjuntar documento con el levantamiento de los activos de información.		
5	El organismo administrador ha identificado los riesgos críticos de las tecnologías de la información, individualizando aquellos que afecten la seguridad de la información y ciberseguridad. Adjuntarlos riesgos identificados.		
6	El organismo administrador ha establecido formalmente el nivel de riesgos aceptado en materia de tecnologías de Información, considerando además los niveles de disponibilidad mínimos para asegurar la continuidad operacional. Aportar documento de respaldo.		
7	El organismo administrador ha designado a un responsable del diseño, mantención y seguimiento de los riesgos de seguridad de la información y ciberseguridad. Señalar al designado responsable (nombre y cargo).		
8	El organismo administrador ha creado un registro formalmente documentado de los sistemas de información existentes al interior de la organización, señalando que proceso de negocio gestiona, el área usuaria, identificación de la base de datos y sistema operativo que soporta el aplicativo. Aportar documento de respaldo.		
9	Los criterios de tratamiento del riesgo se encuentran especificados y formalmente documentados. Adjuntar documento correspondiente.		
10	El organismo administrador ha implementado medidas asociadas a la seguridad de acceso físico tanto a los		

	servidores como a la inmediación o a cualquier centro sobre el que se encuentre información sensible. Detallar medidas.		
11	El organismo administrador ha implementado reglas de accesos (identificación y autenticación) a los sistemas de información mediante usuarios individualizados y contraseñas encriptadas.		
12	Las cuentas de usuarios con privilegios de Administrador se encuentran formalmente definidas e identificadas, tanto en la base de datos, sistema operativo que soporta el aplicativo y el aplicativo en sí. Aportar detalle.		
13	Existe un procedimiento formalmente documentado que considere las autorizaciones necesarias y perfiles de accesos para los sistemas de información. Aportar documento.		
14	Se ha implementado un monitoreo de accesos periódicos sobre los sistemas con el objeto de identificar accesos no autorizados o sospechosos a los sistemas de información. Aportar informe de resultados.		
15	Se han implementado ambientes de desarrollo y prueba separados del ambiente productivo para los sistemas de información que soportan procesos críticos del organismo administrador.		
16	Se encuentran formalizados y documentados los hitos de conformidad y autorización frente a un cambio en los sistemas, tanto del área dueña del proceso así como también la contraparte técnica.		

17	Se considera como parte del proceso de cambios a los sistemas, la documentación de las pruebas de usuario y la respectiva conformidad. Aportar documento de ejemplo.		
18	Existe un procedimiento formalmente documentado de control y gestión de cambio a los sistemas y datos. Aportar documento.		
19	Existe un procedimiento formalmente documentado de procedimiento de respaldo y restauración de los sistemas críticos. Aportar documento.		
20	Existe un plan formalmente documentado de administración de ciberincidentes. Aportar documento.		
21	El organismo administrador ha considerado en el plan anual de auditoría interna la revisión sobre la consistencia de los datos reportados a los sistemas de información de administración de esta Superintendencia. Aportar informe de resultados.		
22	El organismo administrador ha definido la ejecución de un hacking ético periódicamente. Aportar si aplica.		