

“SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN”

Oswaldo Macías Muñoz
Superintendente de Pensiones

II Seminario Iberoamericano sobre la aplicación de las tecnologías en la mejora de la gobernanza y gestión de las instituciones de seguridad social



Santiago, 27 de julio de 2023

Seguridad y Protección de la Información

- En la Superintendencia de Pensiones.
- En el Sistema de Pensiones y Seguro de Cesantía.



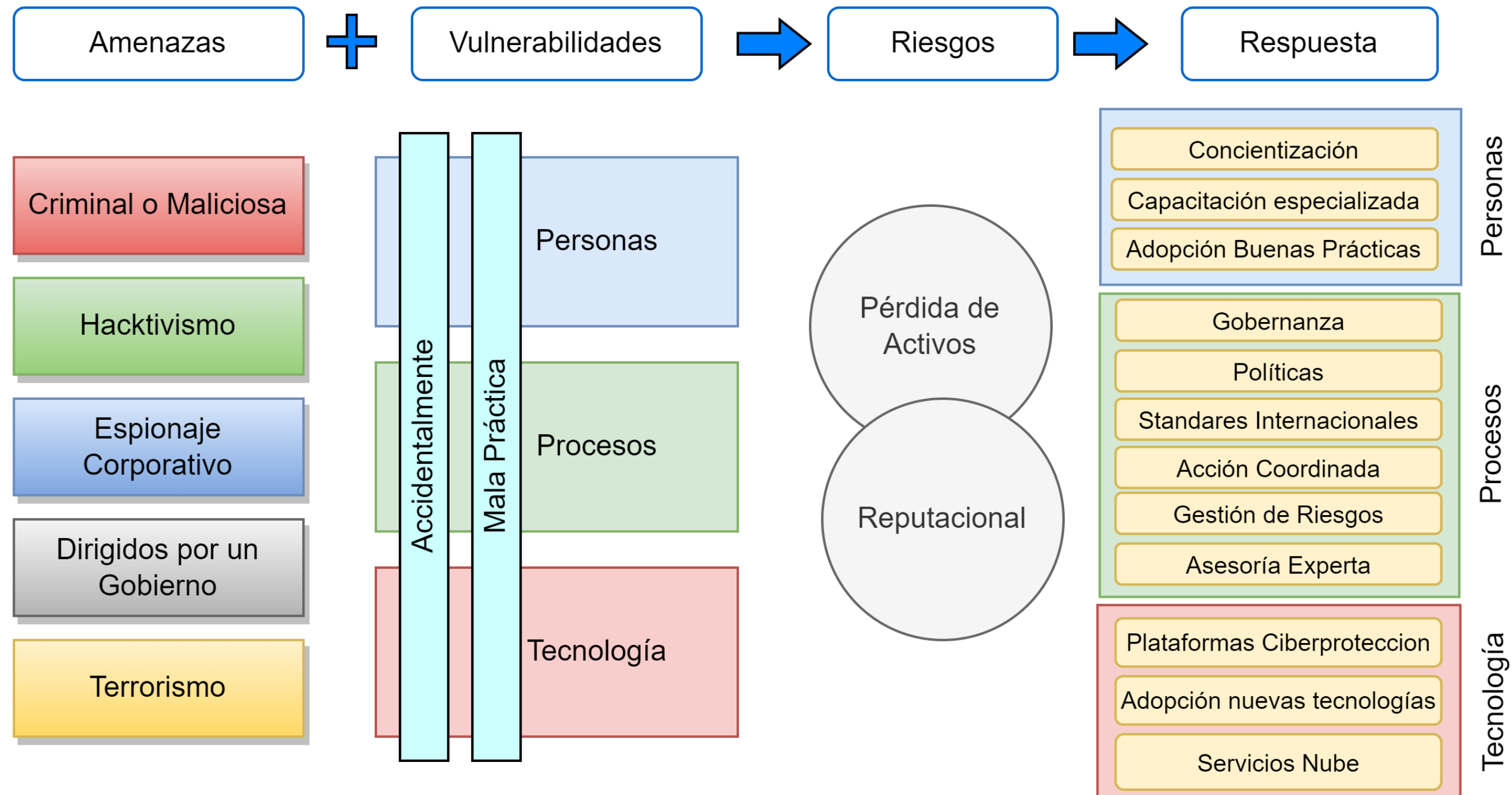
Agenda

➤ **En la Superintendencia
de Pensiones**



Rol de la SP

Estrategia de Ciberseguridad en la SP



Respuestas Estratégicas en Seguridad de la Información y Ciberseguridad

❖ Personas

- Encargado de **Seguridad de la Información** y encargado de **Ciberseguridad** que asesora al equipo directivo de la institución.
- **Comité de Seguridad de la Información** que define políticas internas.
- **Equipo de Seguridad Local** que gestiona las plataformas y servicios de ciberseguridad.
- Campañas de **evaluación** del comportamiento ante amenazas (Phishing – Ransomware).
- Plataforma para **concientización** para envío de recomendaciones y noticias.
- **Capacitación** al equipo especialista en metodologías y herramientas de ciberseguridad.
- Adopción de buenas prácticas entregadas por el **CSIRT** (Equipo de Respuestas ante Incidentes de Seguridad Informática del Estado).

Respuestas Estratégicas en Seguridad de la Información y Ciberseguridad

❖ Procesos

- Sistema de Gestión de Seguridad de la Información (**SGSI**) basada en la Norma ISO 27001-27002-27032.
- Actualización de **políticas y controles** de manera permanente.
- **Colaborar** activamente con el CSIRT de Gobierno y grupo de encargados de ciberseguridad del Estado.
- **Gestión de Riesgos** interna todos los ámbitos de la seguridad de la información y ciberseguridad para su seguimiento y fortalecimiento.
- Servicio de asesoría experta en Ciberseguridad Externa para el Monitoreo y Gestión de Incidentes (**SOC: Security Operation Center**).
- **Actualización** de las plataformas tecnológicas para disminuir los riesgos de vulnerabilidades.
- **Alineamiento** a la normativa legal vigente.

❖ Tecnología

- **Herramientas automáticas** para el monitoreo, alerta y análisis de vulnerabilidades de las plataformas tecnológicas.
- **Nuevas tecnologías** en la generación de plataformas tecnológicas con mejores características de seguridad.
- Plataformas y servicios en la **Nube Pública** para aumentar la alta disponibilidad, productividad y resiliencia de los servicios de la Superintendencia.

➤ **En el Sistema de Pensiones y Seguro de Cesantía**

Seguridad de la información

Ciberseguridad: Marco de referencia

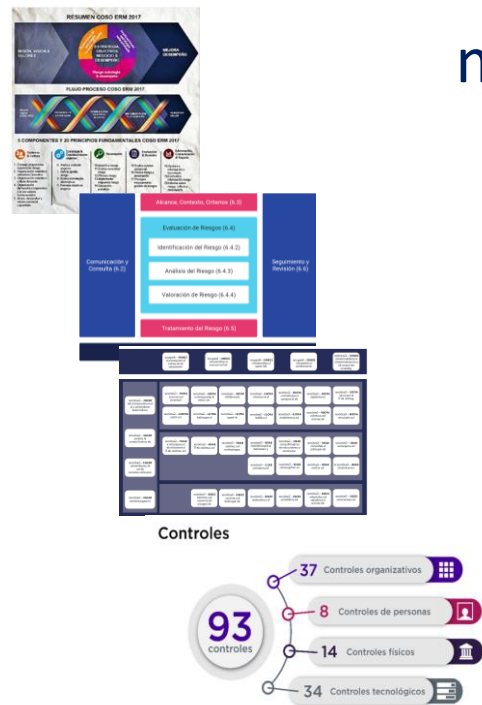
- ❖ Algunos principios relevantes que se integran en la actitud de supervisión y las normas de la SP para cumplimiento de las administradoras:
 - El **Sistema de Gestión de Seguridad de la Información** está integrado a los procesos de la organización y en su **estructura de gestión**, por tanto, está considerado en el diseño de los procesos, sistemas de información y controles.
 - La seguridad de la información forma parte de los **procesos de gestión** para conservar la confidencialidad, integridad y disponibilidad de la información, entregando confianza a las partes interesadas.
 - El directorio y la alta dirección deben demostrar **liderazgo y compromiso** con respecto del sistema de gestión de la seguridad de la información.
 - **La Seguridad de la Información es más que un problema tecnológico.** La administradora debe implementar controles para tratar el riesgo sobre los activos de información. Esto incluye proteger la información, personas y la plataforma que la soporta, resguardándola de la materialización de amenazas internas y externas.

Seguridad de la información

Ciberseguridad: Marco de referencia

- ❖ La normativa de la Superintendencia tiene una **mirada preventiva** y en los procesos de supervisión se aplica el modelo de Supervisión Basado en Riesgos de la SP, el cual considera estándares de buenas prácticas aplicables.
- ❖ En forma específica, se han considerado los estándares de buenas prácticas contenidos en los siguientes marcos de referencia:

- Gestión de Riesgo: COSO ERM - 2017: Gestión del riesgo empresarial, integrando Estrategia y Desempeño, ISO 31000. Gestión de Riesgo – Directrices.
- Seguridad de la Información y Ciberseguridad: familia ISO 27.000.
- NIST: Cybersecurity Framework.
- Gestión de Tecnologías, Cobit 5.0, 2019: marco de trabajo para el gobierno y la gestión de las tecnologías de la información empresariales.
- Gestión de Servicios, ITIL.



Seguridad de la información

Ciberseguridad: Normativa vigente

❖ *SP NCG N° 216, 2017 Gestión de Riesgos: establece el objetivo de la Seguridad de la Información.*

“(...) debe existir una adecuada gestión de las tecnologías de información definida por el Directorio, que entregue los lineamientos para que la entidad administre las tecnologías de información, la seguridad y la continuidad operacional, con el objetivo de minimizar los riesgos relacionados con la confidencialidad, disponibilidad e integridad de la información”.

❖ *SP NCG N° 278 AFP y N° 72 AFC, 2021: Seguridad de la Información y Ciberseguridad*

La gestión de la seguridad y ciberseguridad **es una tarea que comprende a toda la organización** y, por lo tanto, para establecer un Sistema de Gestión de la Seguridad y Ciberseguridad, que mitigue los riesgos de disponibilidad, confidencialidad e integridad se debe establecer una **estructura de procesos**, considerando los objetivos, roles, infraestructura y tecnología de los niveles estratégico, táctico y operacional, de la administradora.

Seguridad de la información

Ciberseguridad: Normas vigentes

❖ *Gestión de Incidentes: NCG N° 298/2022, para las AFP y N° 80/2022 para la AFC.*

- Complementa las normas de seguridad y ciberseguridad e incorpora directrices para la creación y gestión de un **registro de incidentes**.
- Establece la obligación de las administradoras de disponer de sistemas, procedimientos y mecanismos de gestión para: identificar, registrar, evaluar, controlar, mitigar y monitorear incidentes.
- Se crea una **Base de Datos de Incidentes** que contiene los incidentes materializados que afecten o pongan en riesgo la **continuidad de operaciones, los objetivos de los fondos de pensiones y de cesantía, la entrega eficiente y oportuna de los servicios, beneficios y prestaciones en favor de las personas**.
- Comunicación a la Superintendencia: las administradoras deben informar en 30 minutos la **materialización de un incidente**; en 72 horas su **evaluación y análisis**, y una vez cerrado el incidente, su **resolución, reparación y cierre**. Para prevenir su propagación **también deben comunicar, en paralelo**, a las partes interesadas y a las entidades que conforman el sistema previsional o de cesantía.

Seguridad de la información

Ciberseguridad: Modelo de supervisión SP

❖ Instrumentos de supervisión de la NCG N° 278:

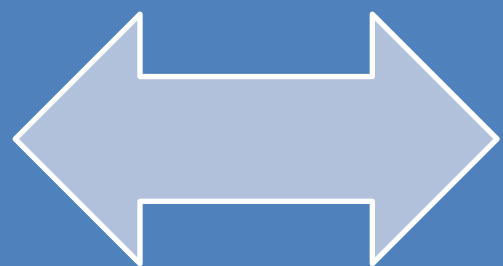
- La actitud de supervisión es preventiva e incorpora estándares de buenas prácticas en un modelo de supervisión que incluye actividades de control agrupadas en **12 procesos organizacionales involucrando procesos Estratégicos, Tácticos y Operacionales**.
- La supervisión también incluye un grupo de **10 controles técnicos**, los que refuerzan el Sistema de Gestión de Seguridad y Ciberseguridad.

Seguridad de la información

Ciberseguridad: Modelo de supervisión SP



Sistema de Gestión de Seguridad de la Información



12 PROCESOS ORGANIZACIONALES: NIVELES ESTRATÉGICOS, TÁCTICOS Y OPERATIVOS.

CATEGORÍAS	PROCESOS	
<p>ESTRATÉGICO</p> <p>TÁCTICO</p> <p>OPERATIVO</p>	DIR.01 Cumplimiento de requisitos de las partes interesadas	DIR.02 Gobernanza de la seguridad de la información y ciberseguridad
	TAC.01 Gestión de riesgos de seguridad de la información y ciberseguridad TAC.02 Gestión de incidentes de seguridad de la información y ciberseguridad	TAC.03 Auditoría
	OPE.01 Capacitación y toma de conciencia OPE.02 Medición	OPE.03 Implementación de respuestas de seguridad de la información y ciberseguridad OPE.04 Acciones correctivas y oportunidades de mejora

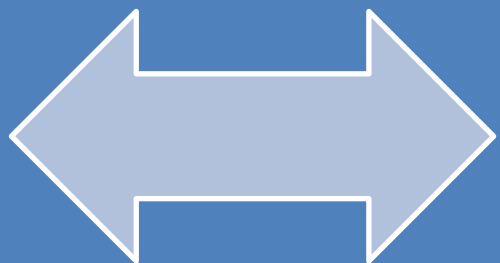
Seguridad de la información

Ciberseguridad: Modelo de supervisión SP

10 CONTROLES TÉCNICOS



Sistema de Gestión
de Seguridad de la
Información y
Ciberseguridad



1. Seguridad de
la arquitectura

3. Seguridad de
las áreas y
equipos

5. Seguridad de
los accesos

7. Seguridad del
Ciclo de
Desarrollo del
Software0

9. Seguridad de la
recuperación de
tecnologías de la
información y
comunicaciones

2. Seguridad del
personal

4. Seguridad de
los activos

6. Seguridad de
los servicios
tecnológicos

8. Seguridad de
los proveedores

10. Seguridad del
cumplimiento

Seguridad de la información

Ciberseguridad: Conclusiones

- La norma **fortalece las acciones de supervisión** de la Superintendencia, estableciendo un marco que permite evaluar el cumplimiento y el grado de madurez de los controles de Seguridad y Ciberseguridad en las administradoras.
- Sin embargo, la actitud de supervisión debe ser de **vigilancia constante**, aunque se verifiquen avances en el fortalecimiento de los controles de las administradoras.
- En este contexto de riesgo la normativa de Seguridad y Ciberseguridad mitiga, pero **no elimina la exposición a los riesgos**, al reforzar las acciones de vigilancia en la organización y promover la mejora continua.
- Los factores críticos de éxito del Sistema de Gestión de Seguridad y Ciberseguridad son la conciencia del **directorio y la administración, y la capacitación** constante de las personas.

“SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN”

Oswaldo Macías Muñoz
Superintendente de Pensiones

II Seminario Iberoamericano sobre la aplicación de las tecnologías en la mejora de la gobernanza y gestión de las instituciones de seguridad social



Santiago, 27 de julio de 2023