

Compendio de Normas que regulan a las Cajas de Compensación de Asignación Familiar

/ 6 LIBRO VI. GESTIÓN DE RIESGOS / 6.1 TÍTULO I. RIESGO OPERACIONAL / 6.1.12 CIBERSEGURIDAD / 6.1.12.1 Definiciones

6.1.12.1 Definiciones

6.1.12.1.1. Autenticación

Proceso utilizado en los mecanismos de control de acceso con el objetivo de verificar la identidad de un usuario, dispositivo o sistema mediante la comprobación de credenciales de acceso.

6.1.12.1.2. Autenticidad

Principio de seguridad que permite certificar la veracidad del origen de datos, elementos o sistemas.

6.1.12.1.3. Ciberataque

Cualquier incidente cibernético, provocado deliberadamente y que afecte a un sistema informático.

6.1.12.1.4. Ciberincidente

Todo evento que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y su infraestructura, que puedan afectar al normal funcionamiento de estos.

6.1.12.1.5. Ciberseguridad

Conjunto de acciones posibles para la prevención, mitigación, investigación y manejo de las amenazas e incidentes sobre los activos de información, datos y servicios, así como para la reducción de los efectos de los mismos y del daño causado antes, durante y después de su ocurrencia.

6.1.12.1.6. Confidencialidad

Principio de seguridad que requiere que los datos deben únicamente ser accedidos por el personal autorizado a tal efecto.

6.1.12.1.7. Disponibilidad

Capacidad de ser accesible y estar listo para su uso a demanda de una entidad o persona autorizada, incluida la Superintendencia.

6.1.12.1.8. Gestión de incidentes

Procedimiento para la detección, análisis, manejo, contención y resolución de un incidente de ciberseguridad y responder ante éste.

6.1.12.1.9. Incidente

Evento inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes, equipos y sistemas de información.

6.1.12.1.10. Infraestructura crítica

Se refiere a las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud o el bienestar de las personas.

6.1.12.1.11. Integridad

Principio de seguridad que certifica que los datos y elementos de configuración sólo son modificados por personal y actividades autorizadas. La Integridad considera todas las posibles causas de modificación, incluyendo fallos software y hardware, eventos medioambientales e intervención humana.

6.1.12.1.12. Riesgo

Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes, equipos y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen corporativa.

6.1.12.1.13. Seguridad de la información

Conjunto de medidas preventivas y reactivas de la C.C.A.F. y sus respectivos sistemas tecnológicos, que tienen por objeto resguardar y proteger la información, asegurando la confidencialidad, integridad, autenticidad y disponibilidad de los datos, continuidad de servicios y protección de activos de información.

