agesic

Uruguay **Presidencia**

GUÍA DE AUDITORÍA

Marco de Referencia

SEGURIDAD DE LA INFORMACIÓN

Versión 4.1 - Noviembre 2019

Este documento ha sido elaborado por Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

El Marco de Ciberseguridad es un conjunto de requisitos (requisitos normativos y buenas prácticas) que se entienden necesarios para la mejora de la seguridad de la información y la ciberseguridad.

1 Introducción

1.1 Objetivo

Establecer las pautas para el uso de la Lista de Verificación, con la cual se evaluará el grado de adopción de los requisitos del Marco de Ciberseguridad y el nivel de madurez en el cual se encuentra la organización teniendo en cuenta el perfil asociado a la misma.

1.2 Alcance

Todas las auditorías y/o evaluaciones realizadas utilizando como marco de referencia el Marco de Ciberseguridad.

2 Evaluación de requisitos

2.1 Requisitos evaluados

Los requisitos evaluados en la auditoria son los señalados en Marco de Ciberseguridad.

2.2 Cumplimiento de requisitos

La organización deberá demostrar la adopción o implementación de los requisitos mediante los siguientes medios:

1. Presentando la documentación e información adicional solicitada por el auditor durante el proceso de auditoría, dentro de los plazos establecidos en cada solicitud.
2. Permitiendo el libre acceso a los auditores a los recursos pertinentes a la auditoría.
3. Entrevistas que se realicen con el auditor en el marco de las auditorias.

No obstante, la organización debe designar una contraparte para la auditoria; la misma debe participar activamente, por lo que deberá disponer del tiempo necesario para que la evaluación pueda ser hecha en los tiempos pautados.

Es importante considerar el modelo de madurez a la hora de realizar el relevamiento de requisitos, para evitar repreguntas.

2.3 Esquema de evaluación

La verificación de la implementación de los requisitos se realizará en conformidad a los siguientes elementos:

1. Comprender el contexto actual de la organización en relación al uso de tecnologías de la información y seguridad de la información.
2. Visitas a las instalaciones.
3. Evaluación de la información obtenida.
4. Elaboración de informe.

2.4 Escala de evaluación

Cada requisito será evaluado en conformidad a la siguiente escala:

1. Cumple: No se han observado desvíos considerables que hagan a la no implementación del requisito durante la ejecución de los procedimientos de la auditoría. Si falta documentación, pero se encuentra evidencia de cumplimiento y conocimiento del tema se deberá dar como “cumple” con las recomendaciones pertinentes.
2. No cumple: El organismo no ha implementado el requisito y se determina que no es subsanable, o afecta el funcionamiento del sistema o los fines previstos para el mismo.
3. No aplica: El requisito no está asociado a ninguna actividad del organismo.

3 Evaluación de madurez

Se realiza un relevamiento de todos los niveles de cada subcategoría propuesto en el modelo de madurez definido en el Marco de Ciberseguridad, indicando para cada subcategoría que nivel está cumpliendo.

Se debe recordar que los niveles superiores dan por cumplido los niveles inferiores. Por ejemplo, si en la subcategoría ID.GA-1 se indica el cumplimiento del nivel 3, implica que se cumple con el nivel 1 y 2.

Si no se verifica la adopción de las pautas establecidas en el nivel 1, corresponderá asignar el nivel 0 a la correspondiente subcategoría.

A la hora de presentar los resultados de madurez para una categoría, se deberá realizar el promedio simple las subcategorías respectivas. Teniendo por valor de cada subcategoría el nivel obtenido.