MEDICIÓN
DESEMPEÑO INSTITUCIONAL

Recomendaciones de Mejora Política Seguridad Digital

Fecha de generación: 2020-07-30 19:15:14

Entidad: **MINISTERIO DE DEFENSA NACIONAL**

#	Política	Recomendaciones
1	Seguridad Digital	Incorporar el análisis del contexto interno y externo de la entidad dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno.
2	Seguridad Digital	Contemplar por parte del Jefe de Control Interno que sus informes de seguimientos y auditoría emitidos por las oficinas de control interno, contribuyan a la formulación de acciones enfocadas a la gestión del riesgo.
3	Seguridad Digital	Realizar un diagnóstico de seguridad y privacidad de la información para la vigencia, mediante la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI).
4	Seguridad Digital	Elaborar el plan operacional de seguridad y privacidad de la información de la entidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.
5	Seguridad Digital	Desarrollar jornadas de capacitación y/o divulgación a sus servidores y contratistas sobre seguridad digital.
6	Seguridad Digital	Analizar la información recopilada por la entidad para identificar y caracterizar (en lo social, geográfico, económico o lo que la entidad considere de acuerdo con su misión) sus grupos de valor.
7	Seguridad Digital	Definir los planes, proyectos y programas de la entidad con base en el análisis de la información recopilada para identificar y caracterizar (en lo social, geográfico, económico o lo que la entidad considere de acuerdo con su misión) sus grupos de valor.
8	Seguridad Digital	Definir las estrategias de servicio al ciudadano, rendición de cuentas y trámites con base en el análisis de la información recopilada para identificar y caracterizar (en lo social, geográfico, económico o lo que la entidad considere de acuerdo con su misión) sus grupos de valor.
9	Seguridad Digital	Definir el direccionamiento estratégico de la entidad teniendo en cuenta los lineamientos para la gestión del riesgo (Política de Riesgo).
10	Seguridad Digital	Tener en cuenta los resultados de las auditorías internas y externas, para la toma de las decisiones en el ejercicio de la planeación institucional. Desde el sistema de control interno efectuar su verificación.

11	Seguridad Digital	Tener en cuenta los resultados de la evaluación de la gestión de riesgos, para la toma de las decisiones en el ejercicio de la planeación institucional. Desde el sistema de control interno efectuar su verificación.
12	Seguridad Digital	Tener en cuenta la medición del desempeño en periodos anteriores, para la toma de las decisiones en el ejercicio de la planeación institucional. Desde el sistema de control interno efectuar su verificación.
13	Seguridad Digital	Fortalecer las capacidades en seguridad digital de la entidad a través de su participación en las jornadas de socialización y promoción del uso del modelo de gestión de riesgos de seguridad digital convocadas por el Ministerio de Tecnologías de la Información y las Comunicaciones.
14	Seguridad Digital	Fortalecer las capacidades en seguridad digital de la entidad a través de su participación en las jornadas de sensibilización y capacitaciones del uso seguro de entorno digital convocadas por el Ministerio de Tecnologías de la Información y las Comunicaciones.
15	Seguridad Digital	Fortalecer las capacidades en seguridad digital de la entidad a través de su participación en los ejercicios de simulación nacional o internacional para desarrollar habilidades y destrezas en materia de seguridad digital.
16	Seguridad Digital	Fortalecer las capacidades en seguridad digital de la entidad a través de convenios o acuerdos de intercambio de información para fomentar la investigación, la innovación y el desarrollo de temas relacionados con la defensa y seguridad nacional en el entorno digital.
17	Seguridad Digital	Reconocer y adoptar en la entidad las herramientas o instrumentos en seguridad digital definidas por el Gobierno Nacional tales como la Guía para la Guía para la identificación de infraestructura critica cibernética.
18	Seguridad Digital	Reconocer y adoptar en la entidad las herramientas o instrumentos en seguridad digital definidas por el Gobierno Nacional tales como el Plan Nacional de protección de la infraestructura crítica cibernética.
19	Seguridad Digital	Reconocer y adoptar en la entidad las herramientas o instrumentos en seguridad digital definidas por el Gobierno Nacional tales como los Estudios relacionados con Seguridad Digital (por ejemplo Estudio sobre el Impacto Económico de los Incidentes, Amenazas y Ataques Cibernéticos (Encuesta OEA).
20	Seguridad Digital	Reconocer y adoptar en la entidad las herramientas o instrumentos en seguridad digital definidas por el Gobierno Nacional tales como el Modelo seguridad y privacidad de la Información (MSPI).
21	Seguridad Digital	Fortalecer las capacidades en Seguridad digital del talento humano de la entidad, a través de su participación en las convocatorias de capacitación en Gobierno Electrónico realizadas por el Gobierno Nacional.

22	Seguridad Digital	Fortalecer las capacidades en Seguridad digital del talento humano de la entidad, a través de su participación en las convocatorias de Posgrado en gestión TI y seguridad de la información realizadas por el Gobierno Nacional.
23	Seguridad Digital	Fortalecer las capacidades en Seguridad digital del talento humano de la entidad, a través de su participación en las convocatorias de capacitación en gestión TI y seguridad de la información realizadas por el Gobierno Nacional.
24	Seguridad Digital	Fortalecer las capacidades en Seguridad digital del talento humano de la entidad, a través de su participación en las convocatorias de competencias gerenciales realizadas por el Gobierno Nacional.
25	Seguridad Digital	Fortalecer las capacidades en Seguridad digital del talento humano de la entidad, a través de su participación en las convocatorias de Encuentros de Gestores de Incidentes Cibernéticos convocados por el CSIRT Gobierno.
26	Seguridad Digital	Fortalecer las capacidades en Seguridad digital del talento humano de la entidad, a través de su participación en las convocatorias de Desarrollo del Talento Digital convocadas por el Gobierno Nacional.
27	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como registrarse en el CSIRT Gobierno y/o ColCERT.
28	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la guía para la identificación de infraestructura crítica cibernética.
29	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como realizar la identificación anual de la infraestructura crítica cibernética e informar al CCOC.
30	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en la contrucción de los planes sectoriales de protección de la infraestructura crítica cibernética.
31	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en las mesas de construcción y sensibilización del Modelo Nacional de Gestión de Riesgos de Seguridad Digital.
32	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en entidades públicas.
33	Seguridad Digital	Destinar recursos económicos y humanos que satisfagan las necesidades de seguridad de la información de la entidad.
34	Seguridad Digital	Hacer campañas de concientización en temas de seguridad de la información de manera frecuente, específicas para cada uno de los distintos roles dentro de la entidad.