CIRCULAR N° 000016

Bogotá D.C., 16 JUN 2021

DESTINATARIOS: Directores, Subdirectores, Jefes de Oficina, Coordinadores, Funcionarios y Contratistas

ASUNTO: Cumplimento lineamientos Sistema de Gestión de Seguridad de la Información

Considerando el rol de la Dirección General en cuanto al desarrollo del Sistema Integrado de Gestión Institucional (SIGI) y la responsabilidad de garantizar que la entidad cumpla con lo definido en la Política de Seguridad y Privacidad de la Información establecida mediante Resolución 0000683 de 17 de diciembre de 2020 que hace parte integral del Sistema de Gestión de Seguridad de la Información (SGSI), es importante solicitar que desde cada proceso, subproceso y grupo de trabajo, incluido los de carácter estratégico, misional, evaluación y control, en adelante Dependencias, así como a todos los funcionarios, contratistas, proveedores y todos los terceros que en ejercicio de sus funciones y las propias de la entidad que tengan acceso o gestionen la información institucional, den cumplimiento y seguimiento a todas las actividades establecidas por el SGSI y para los casos que corresponda, alimentar o retroalimentar la información y gestiones que se deriven de su competencia a la OTEC

Por lo anterior expuesto, es fundamental que se de cumplimiento oportunamente, entre otros, a los siguientes temas:

- **Documentación del SGSI a tener en cuenta para la adquisición, desarrollo, instalación o actualización de software**

  Toda dependencia debe reportar a la OTEC las necesidades de adquisición o desarrollo, instalación y/o actualización de software, con el fin de que se evalúe la viabilidad, correcta adopción del software en función de los términos y condiciones de uso, soporte, seguridad y demás particularidades que a ello compete. De acuerdo a lo anterior, se debe tener en cuenta la siguiente documentación:

  - **A3-PR-11 Ciclo de vida del software:** Establece las actividades relacionadas con la adquisición, desarrollo o mantenimiento de un programa (software) para la USPEC.
  - **A3-GU-02 Guía de Desarrollo Seguro:** Establece lineamientos de seguridad de información para el desarrollo de aplicaciones y sistemas de información que serán propiedad de la USPEC, ya sean In-house o tercerizados, a través de estándares de desarrollo de software seguro.
  - **A3-PR-09 Instalación de software operacional:** Establece los parámetros para la instalación temporal o definitiva de software operacional adicional al esquema instalado por la OTEC en la USPEC.
  - **A3-GU-01 Guía de Contraseñas Seguras:** Define los lineamientos asociados con la estructuración y el uso de contraseñas seguras.
  - **Resolución 1519 de 2020 Anexo 3 Seguridad Digital - MINTIC**: Se deberán aplicar las medidas de seguridad digital y de la información referidas en esta resolución.

❖ **Documentación del SGSI a tener en cuenta para la gestión de usuarios de aplicaciones y sistemas:**

Para las dependencias que tengan a cargo usuarios con el rol de administrador de sistemas de información, aplicativos o servicios internos o externos se deben tener en cuenta la siguiente documentación:

- **A3-PR-08 Gestión de Acceso a Usuarios**: Ayuda en la gestión de autorización y desautorización de los accesos, ya sean lógicos (es decir a sistemas y aplicaciones) que corresponde, manteniendo depurados y actualizados los controles de acceso a cada sistema y/o aplicación.
- **A3-PR-13 Control de cambios:** Es importante que todas las dependencias que tienen a cargo la administración de sistemas de información, trabajen en conjunto con las áreas involucradas en cuanto a la determinación de cambios a sistemas (actualizaciones y/o mantenimientos) de actividades que puedan repercutir en un impacto operacional en la entidad, esto debido a que las dependencias no contemplan los riesgos asociados a un cambio no controlado , generando en ocasiones la materialización de riesgos como indisponibilidad de servicios, indisponibilidad de información, pérdida de confidencialidad de información e incluso pérdida de integridad de activos de información.
- **A3-GU-01 Guía de Contraseñas Seguras:** Teniendo en cuenta la premisa de que el eslabón más débil en la cadena de seguridad de la información es el usuario (funcionarios, contratistas y partes interesadas), es importante que todos los funcionarios, contratistas y/o partes interesadas tengan en cuenta los lineamientos establecidos en esta Guía para el uso de contraseñas seguras en los Sistemas y aplicaciones de uso de la entidad.

❖ **Documentación del SGSI a tener en cuenta a nivel transversal:**

- **A3-PR-04 Gestión de eventos e incidentes de seguridad de la información:** Cada líder de proceso (Director, subdirector y jefes de oficina) debe reforzar en sus áreas la cultura de seguridad de la información mediante la formulación de estrategias para el reporte continuo y respuesta oportuna antes eventos e incidentes de seguridad de la información,, ya que esto es fundamental para identificar la materialización de riesgos que pueden afectar la información institucional y/o la información de terceros que administra la entidad.
- **Seguridad de la información en la relación con los proveedores y contratistas:** Cada supervisor de contrato y supervisor de apoyo debe retroalimentar con los correspondientes proveedores de servicios y/o contratistas los aspectos de seguridad de la información definidos por USPEC.
- **A3-PR-07 Gestión de medios removibles:** Establece las actividades necesarias para el control de los medios de almacenamiento removibles con el objetivo de salvaguardar la disponibilidad, integridad y confidencialidad de la información de la USPEC.
- **Política de escritorio y pantalla limpios:** Establece los lineamientos para prevenir el acceso no autorizado, pérdida y/o daño de la información institucional, que se encuentra a cargo del personal que labora en la USPEC. Se debe bloquear el equipo de cómputo una vez el funcionario y/o contratista se retire de su lugar de trabajo al igual su puesto de trabajo debe permanecer sin documentación a la vista o accesible sin supervisión.
- **Política de transferencia de información:** La OTEC establece lineamientos para la transferencia de la información institucional catalogada como reservada o confidencial. Los responsables del proceso son los encargados de autorizar las transferencias de información sensible que tiene a su

cargo y el receptor de la información es el responsable de aplicar todos los controles pertinentes de seguridad de información con el fin de mantener la confidencialidad e integridad de la misma.

- **Plan de tratamiento de riesgos de seguridad de la información:** Cada dependencia es responsable de dar seguimiento y gestión a sus propios riesgos de seguridad de la información identificados en los proceso de auditoría o revisión interna del SGSI, por tal motivo, la OTEC tiene a cargo únicamente la consolidación de la información correspondiente a las gestiones que realice cada responsable.

El cumplimiento de lo establecido en la política de seguridad y privacidad de la información establecida a través de la Resolución 0000683 de 17 de diciembre de 2020, es obligación de todos los que intervienen o tienen cualquier tipo de gestión sobre los activos de información de la entidad, por lo tanto, se deben aplicar en todo momento y en toda gestión de la entidad las políticas específicas, los procedimientos, manuales y guías para prevenir los riesgos de seguridad de la información que puedan impactar la disponibilidad, integridad y confidencialidad de los activos de información.

El incumplimiento de lo mencionado en la presente circular y/o demás lineamientos del Sistema de Gestión de Seguridad de la Información se establecerá como un incidente de seguridad de la información y se notificará a su jefe inmediato y/o supervisor del contrato y en caso requerido se procederá a iniciar un proceso disciplinario teniendo en cuenta el procedimiento A2-PR-02 Procesos disciplinarios de la entidad.

Atentamente,

ALVARO AVILA

ÁLVARO ÁVILA CASTELLANOS
Director General (E)

Elaboró: Fernando Vargas Herrera- Técnico Operativo / Diana Paola Cárdenas Huertas- Profesional Universitario
Revisó: Ing. Imelda Muñoz Mancipe - Jefe Oficina de Tecnología / Camilo Alejandro Romero - Coordinador Grupo de Comunicaciones

Control de Legalidad: Jorge Mauricio Salinas Gutiérrez - Coordinador Grupo de Acciones Constitucionales,Conceptos y Control de Legalidad