PROPÓSITO
Garantizar que la información, las áreas de procesamiento de información, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información que se encuentran dentro del Centro de Datos de la Unidad Nacional de Protección estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.
ALCANCE
Inicia con la solicitud de acceso al área segura; sigue con la autorización y validación de ingreso; y culmina con la cancelación de los permisos de acceso a el área segura de la Unidad Nacional de Protección.

RESPONSABILIDADES

RESPONSABLES	RESPONSABILIDADES
CIO y/o líder de proceso de Gestión tecnológica	Liderar, aprobar, realizar seguimiento y verificación de la correcta adopción del procedimiento.
Líder de Infraestructura.	Persona responsable por la implementación y seguimiento sobre la ejecución de las actividades del procedimiento de trabajo en áreas seguras.
Analistas de Infraestructura.	Responsable de ejecutar y llevar a cabo las labores y actividades dentro del Centro de Datos y/o ares seguras de acuerdo con el presente procedimiento.
CISO y/o Oficial de seguridad de la Información.	Verificar y realizar siguiente sobre la correcta ejecución del procedimiento.

DEFINICIONES

TÉRMINO	DEFINICIÓN
Acceso	En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas de la Entidad. (ISO 27000)
Acceso físico	Significa ingresar a las áreas de misión crítica o instalaciones en general del Centro de Datos. (Norma ISO 27000)
Personal	Conjunto de las personas que trabajan en un mismo organismo, dependencia, fábrica, taller. (Real Academia Española - RAE)

DEFINICIONES	
TÉRMINO	**DEFINICIÓN**
Confidencialidad	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (Norma ISO 27000)
Disponibilidad	Propiedad de la infraestructura de estar accesible y utilizable cuando lo requiera una entidad autorizada. (Norma ISO 27000)
CIO	Chief Information Officer – Oficial de Tecnologías de la Información (Modelo de Seguridad y Privacidad de la Información – MSPI de MINTIC)
CISO	Chief Information Security Officer – Oficial de Seguridad de la Información (Modelo de Seguridad y Privacidad de la Información – MSPI de MINTIC)

MARCO LEGAL

- Decreto 2573 de 2014 Lineamientos Generales de Gobierno en línea
- Ley 1581 de 2012 Ley de Protección de Datos Personales
- Decreto 1078 de 2015, Reglamento Único de las TIC
- ISO/IEC 27001: 2013 Sistema de Gestión de Seguridad.
- Decreto 2609 de 2012 se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado
- Modelo de seguridad y privacidad de la información de MINTIC

DOCUMENTOS RELACIONADOS

- GTE-MA-01 Manual de Mantenimiento Preventivo y Correctivo.
- GTE-MA-02- Manual de Políticas Específicas de Seguridad y Privacidad de la Información.
- GTE-FT-37 Formato Bitácora de Ingreso al Centro de Datos
- GIN-MA-01 Manual Gestión Estratégica Integrada.

CONSIDERACIONES GENERALES

1. Directrices de seguridad para todo el personal

Para dar cumplimiento al acceso físico y lógico a la información e infraestructura tecnológica del Centro de Datos (Área Segura), todos los involucrados en el alcance de este procedimiento deberán acatar lo siguiente:

- Se deberá asignar un nombre de usuario para conceder el acceso a los sistemas de información de la UNP.
- Para generar acceso tanto físico como lógico a proveedores como contratistas, el supervisor del contrato debe realizar la solicitud al área de infraestructura tecnológica con las respectivas justificaciones para otorgar el acceso.
- Una vez que el contrato del contratista o proveedor haya finalizado, el supervisor del contrato tiene la responsabilidad de solicitar la cancelación de los derechos de acceso a el(los) usuario(s) vinculado(s) con ese contrato.
- Se deberá deshabilitar los usuarios y nombres de usuario correspondientes al personal que ya no tenga relación con la UNP.
- Se deberán realizar revisiones periódicas en los diferentes sistemas de la UNP para garantizar que se remuevan los usuarios deshabilitados o redundantes, mínimo una vez al mes.
- El personal autorizado para trabajo en áreas seguras no deberá compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes.

2. Directrices de seguridad para el Control de acceso físico

- Se deberá identificar al personal que requiere acceso a las áreas seguras y conceder los privilegios necesarios para el acceso físico.
- Se deberá contar con mecanismos de control de acceso para las áreas seguras (Centro de Datos); tales como cámaras, puertas de seguridad, sistema de ingreso por control de tarjeta de proximidad, llaves, entre otras, que la Unidad Nacional de Protección considere pertinentes.

CONSIDERACIONES GENERALES

- Las puertas de acceso al centro de datos que alberga información crítica deberán permanecer siempre cerradas y aseguradas. De igual manera, los gabinetes y puertas de los equipos que se encuentran en las áreas mencionadas deberán permanecer cerrados.
- Se deberá aprobar de manera previa las solicitudes de acceso de terceros al Centro de Cómputo (área segura), además se deberá acompañar permanentemente a los visitantes durante su estancia en el área determinada.
- Se deberá registrar el ingreso de los visitantes al centro de datos en el Formato GTE-FT-37 Formato Bitácora de Ingreso al Centro de Datos ubicado en la entrada de estos lugares de forma visible.
- Se deberá monitorear los ingresos al centro de datos permanentemente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.
- Se deberá bloquear de manera inmediata los privilegios de acceso físico al Centro de Datos tan pronto el personal termine su vinculación.

3. En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

- Fumar dentro del Centro de Datos.
- Introducir alimentos o bebidas al Centro de Datos
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.

CONSIDERACIONES GENERALES

- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

4. **El centro de datos debe estar provisto de:**

- Pisos elaborados con materiales no combustibles.
- Sistema de refrigeración por aire acondicionado de precisión.
- Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
- Alarmas de detección de humo y sistemas de extinción de fuego.
- Los detectores deberán ser probados de acuerdo con las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
- Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.
- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un Servidor Público y/o contratista autorizado por el Líder del Proceso de Gestión Tecnológica o Líder de Infraestructura de la UNP.
- Las puertas del centro de datos deben permanecer cerradas; Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el Servidor Público o contratista responsable de la actividad se ubicará dentro del centro de datos.

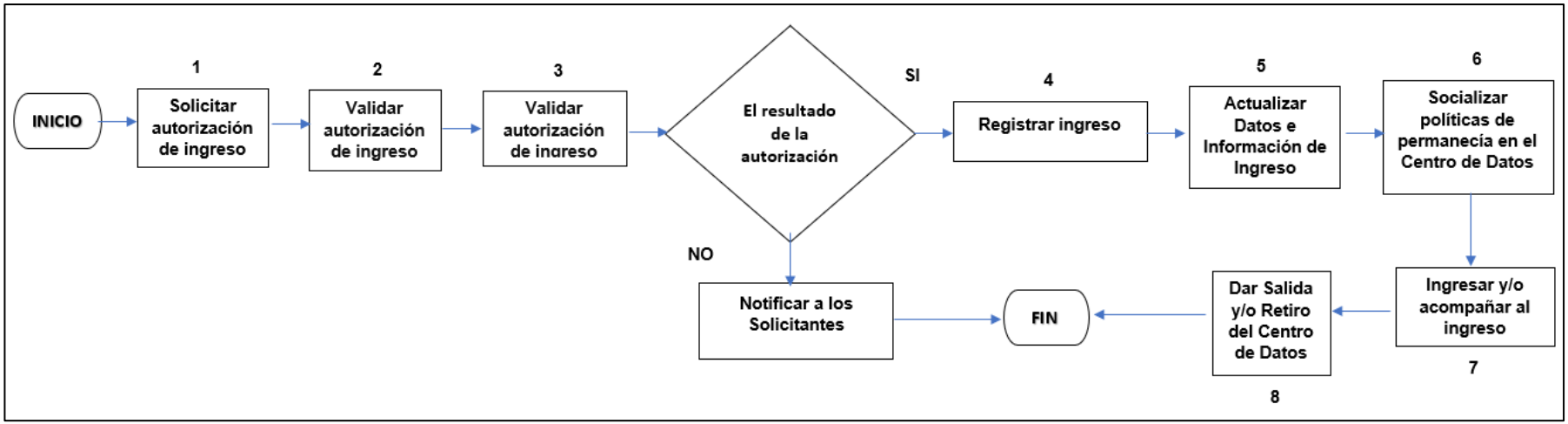
CONSIDERACIONES GENERALES
• Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad. • Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas. • Los equipos del centro de datos que lo requieran deben estar monitoreados para poder detectar las fallas que se puedan presentar.

DESCRIPCIÓN DEL PROCEDIMIENTO

N° ACTIVIDAD	RESPONSABLE	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	REGISTRO
1	Servidor Público o Contratista	Solicitar autorización de ingreso	Solicita la autorización o revocación de ingreso al jefe inmediato o supervisor del contrato determinando la necesidad de acceso, las actividades a desarrollar, los horarios requeridos e información relevante.	Correo Electrónico
2	Jefe inmediato o supervisor del contrato	Validar autorización de ingreso	Valida solicitud realizada por el Servidor Público o contratista	Correo Electrónico
3	Líder infraestructura	Validar autorización de ingreso	Valida la solicitud por parte del jefe inmediato sobre el ingreso del Servidor Público o contratista que requiere esta autorización para desempeñar sus funciones u obligaciones contractuales	Correo Electrónico
4	Líder Infraestructura	Registrar ingreso	Realiza el registro en el formato Bitácora de Ingreso a Áreas e informa a los encargados de las áreas involucradas, para proceder con el acceso; en caso contrario, responde a la persona que ha	GTE-FT-37 Formato Bitácora de Ingreso al Centro de Datos

DESCRIPCIÓN DEL PROCEDIMIENTO				
N° ACTIVIDAD	**RESPONSABLE**	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**REGISTRO**
			solicitado la autorización, notificando el porqué de la denegación.	
5	Analistas Infraestructura	Actualizar Datos e Información de Ingreso	Actualiza con los datos de la persona autorizada, los registros de autorización de acceso, conforme la solicitud.	GTE-FT-37 Formato Bitácora de Ingreso al Centro de Datos
6	Analistas Infraestructura	Socializar políticas de permanecía en el Centro de Datos	Indica las políticas de seguridad y permanencia en el centro de datos al Servidor Público o Contratista definidas en el apartado de consideraciones generales del presente documento	GTE-FT-37 Formato Bitácora de Ingreso al Centro de Datos
7	Analistas Infraestructura	Ingresar y/o acompañar el ingreso	Ingresa al área y documenta todas las actividades realizadas en la bitácora de ingreso. En caso de acceso temporal, la persona debe encontrarse acompañada por el Encargado del área segura durante su permanencia en ésta.	GTE-FT-37 Formato Bitácora de Ingreso al Centro de Datos
8	Analistas Infraestructura	Dar Salida y/o Retiro del Centro de Datos	Realiza las validaciones de la infraestructura tecnológica validando su correcto funcionamiento y operatividad e indicar el retiro del centro de datos del Servidor Público o contratista.	GTE-FT-37Formato Bitácora de Ingreso al Centro de Datos
	FIN			

FLUJOGRAMA



CONTROL DE CAMBIOS			
VERSIÓN INICIAL	**DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO**	**FECHA**	**VERSIÓN FINAL**
00	Creación del Procedimiento para el trabajo en el Centro de Datos de la Unidad Nacional de Protección – UNP, determinada como área segura teniendo en cuenta la criticidad de la información procesada y almacenada.	06/12/2022	**01**