INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR
GUÍA PARA USO DE DISPOSITIVOS PERSONALES BYOD

Tabla de Contenido

1. OBJETIVO

Establecer los lineamientos y directrices para que los colaboradores del ICBF puedan ejercer actividades en el marco de funciones u obligaciones a través del uso de dispositivos personales o que no sean propiedad de la entidad con el fin de controlar y proteger la información mientras se accede a la red institucional.

2. ALCANCE

Los lineamientos aquí contenidos aplican a los dispositivos personales que tienen la capacidad de almacenar, transferir y/o procesar cualquier tipo de información, y son utilizados por servidores públicos, pasantes, practicantes, proveedores, judicantes, contratistas y operadores de prestación de servicios profesionales y de apoyo a la gestión para el ejercicio de sus funciones u obligaciones en el ICBF ya sea en la Sede de la Dirección General, Regionales y Centros Zonales y si aplica a (CAIVAS, CESPAS, CAVIF, SRPA Casas de Justicia y Unidades Locales.

Excepción:

Para las dependencias adscritas a los procesos de Promoción y Prevención y Protección, está expresamente restringido el uso y manejo de equipos personales, lo anterior, teniendo en cuenta que en estos procesos manejan información sensible de niños, niñas, adolescentes y jóvenes razón por la cual su uso debe estar restringido.

3. DEFINICIONES

BYOD: Del inglés Bring Your Own Device (Trae Tu Propio Dispositivo). Son los lineamientos mediante los cuales el ICBF permite el acceso a su información y plataforma tecnológica a través de dispositivos personales.

CONEXIÓN SEGURA: Se entiende por conexión segura toda aquella que se establece en un punto de red que requiera algún tipo de autenticación.

DISPOSITIVOS PERSONALES: Se entiende como dispositivo personal cualquier artefacto que tenga la capacidad de almacenar, transferir y/o procesar cualquier tipo de información. Entre estos dispositivos se incluye los equipos computo (portátiles o de escritorio), teléfonos inteligentes, tabletas, entre otros.

DISPOSITIVOS BYOD: Dispositivos personales cobijados por los lineamientos establecidos en el presente documento.

INCIDENTE DE SEGURIDAD DE LA INFORMACION: Uno o más eventos de seguridad de la información que comprometen las diferentes operaciones y la seguridad de la información.

TRAE TU PROPIO DISPOSITIVO: Es una guía que consiste en que los colaboradores y proveedores de la entidad traigan sus propios dispositivos a su lugar de trabajo para tener acceso a recursos del ICBF y poder ejecutar sus funciones o actividades

MIS: Mesa Informática de Soluciones

RIESGO: Según la ISO 31000 es el efecto que genera la incertidumbre en los objetivos. Los objetos pueden tener un efecto si no los desviamos de lo esperado. Puede ser positivo, negativo o ambos y puede abordar, crear o dar lugar a oportunidades y amenazas. Los objetivos pueden tener distintos aspectos y categorías, y se pueden aplicar a distintos niveles. El riesgo se suele expresar en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y su probabilidad.[1]

SGSI: Sistema de Gestión de Seguridad de la Información.

VPN: Del inglés Virtual Private Network (Red Privada Virtual) supone una tecnología de red que, por razones de costo y comodidad, brinda la posibilidad de conectarse a una red pública generando una extensión a nivel de área local

4. DESARROLLO

4.1 DESCRIPCION

La aplicación de lo establecido en la Ley 1221 de 2008 y su Decreto Reglamentario 884 de 2012 Por la cual se establecen normas para promover y regular el Teletrabajo y la ley 2088 de 2021 **POR LA CUAL SE REGULA EL TRABAJO EN CASA** ha impactado de manera significativa la forma de operar del ICBF lo cual ha permitido a los colaboradores la incorporación de sus dispositivos móviles personales (portátiles, smartphones, tabletas) o que no sean de propiedad del ICBF a las redes corporativas

[1] Norma ISO 31000:2018

desde su casa, la propia oficina o cualquier otro lugar, aceptando su uso compartido, tanto para las tareas profesionales de uso corporativo como para las personales de los colaboradores.

Lo anterior conlleva a la materialización de riesgos inherentes y asociados al uso de estos dispositivos personales que sin ninguna verificación y revisión podría ocasionar incidentes de seguridad de la información como: pérdida o robo de información, robo de dispositivos, robo de credenciales, utilización de sistemas de conexión no seguros, entre otros.

Bajo este contexto, se hace imperante la necesidad de establecer mecanismos, lineamientos y reglas de seguridad para el uso y control de dispositivos **BYOD** los cuales quedaran establecidos en el presente documento.

4.1 REGLAS DE SEGURIDAD PARA EL USO DE BYOD

A continuación, se describen las reglas para el uso de los dispositivos **BYOD**, de uso personal y que se utilicen para trabajar, dentro o fuera de las instalaciones de la Sede de la Dirección General SDG, regionales, CAIVAS, CESPAS, CAVIF, SRPA Casas de Justicia y Unidades Locales del Instituto Colombiano de Bienestar Familiar a nivel nacional.

4.1.1 El uso de Dispositivos **BYOD** deberá ser autorizado por el jefe inmediato o supervisor del contrato, en formato F1.P2.GTI Formato de solicitud de servicios de tecnología.

4.1.2 Toda la información contenida en los Dispositivos BYOD inherente a la ejecución de las funciones u obligaciones contractuales de los colaboradores debe estar almacenada en la cuenta de OneDrive o SharePoint asignada al colaborador.

4.1.3 Para la conexión del Dispositivo BYOD a la red institucional, éste debe cumplir con los siguientes requisitos: sistema operativo licenciado, antivirus licenciado y actualizado y herramienta ofimática licenciada (la proporcionada por la entidad) tal como lo indica la resolución 4286 del 2020 y 5515 del 2021 o aquella que la modifique o derogue.,

4.1.4 Es responsabilidad del colaboradores y operadores la protección de la información de la entidad que tenga bajo su manejo en estos dispositivos BYOD, la cual no debe ser compartida por ningún medio fuera de las redes institucionales, mediante conexiones seguras y aplicando los lineamientos y manual de la política de seguridad de la Información. Cuando se utilicen

dispositivos BYOD fuera de las instalaciones del ICBF, no deben ser dejados desatendidos (bloqueo de equipo) y deben estar físicamente resguardados.

4.1.5 Cuando se utilizan dispositivos BYOD en lugares públicos, el propietario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas, así como evitar la conexión a redes públicas, las cuales no cuentan con ningún tipo de monitoreo o seguridad y representan un riesgo para la seguridad de la información.

4.1.6 El colaborador propietario del BYOD deberá instalar periódicamente aplicar actualizaciones de seguridad para el sistema operativo, así como efectuar actualizaciones del antivirus instalado en el BYOD al menos cada 15 días, lo cual será validado por el soporte en sitio ingeniero regional periódicamente.

4.1.7 En caso de pérdida, robo del dispositivo BYOD, deberá ser reportado a la entidad como incidente de Seguridad a través de MIS.

4.1.8 Todos los BYOD deben ser revisados a través del F9.P2.GTI Formato Verificación de Equipos Personales por el soporte en sitio de cada regional y en la SDG, previa solicitud del jefe inmediato o supervisor del contrato a la mesa de servicio a través del F1.P2.GTI formato de solicitud de Servicios de Tecnología, para validar que cumplan con las condiciones técnicas y reglas de seguridad establecidas en este documento, antes de la configuración y autorización de ingreso a la red de la entidad a través de VPN.

4.1.9 Al conectar un dispositivo BYOD a la red institucional, el propietario acepta la política de seguridad de la información de la entidad adoptada mediante las Resoluciones 4286 del 27 de julio del 2020 y 5515 del 31 de agosto del 2021 o aquella que la modifique o derogue, así como los anexos y procedimientos asociados los cuales están publicados en el portal web de la entidad.

4.1.10 Para el ingreso de dispositivos BYOD a las instalaciones del ICBF se deben registrar en la bitácora de ingreso de equipos en la recepción.

4.2 LINEAMIENTOS ESPECIALES

4.2.1 Una vez se autorice la conexión de un dispositivo BYOD a los recursos tecnológicos del ICBF (VPN, office 365, Orfeo entre otros), la entidad tendrá acceso para visualizar y monitorear los datos del Instituto, que hayan sido almacenados, transferidos o procesados en el mismo. De igual manera, el Equipo del SGSI, Referentes Regionales del SGSI y soportes en sitio están autorizados a configurar cualquier dispositivo BYOD de conformidad con las reglas de uso consignadas en este documento, así como controlar el uso de los recursos asignados por la entidad a través de herramientas de seguridad en el dispositivo.

4.2.2 Un equipo BYOD no podrá almacenar información institucional de manera local, es por eso que para la protección de la información y datos que pertenecen al Instituto Colombiano de Bienestar Familiar, la entidad podrá realizar el borrado completo de todos los datos e información institucional que se encuentren en el dispositivo BYOD, si considera que es necesario, sin contar con el consentimiento del propietario del dispositivo, ante el incumplimiento de la política de operación consignada en la guía.

4.2.3 El Instituto Colombiano de Bienestar Familiar no pagará y/o reconocerá a los colaboradores, ningún valor o subsidio por el uso con fines laborales de los dispositivos BYOD.

4.3 INCIDENTES DE SEGURIDAD DE LA INFORMACION

4.3.1 Todos los incidentes de seguridad de la información relacionados con dispositivos BYOD, deben ser reportados inmediatamente a través de MIS Mesa Informatica de Soluciones y con copia al Líder de Gestión de Incidentes de Seguridad de la Información (verificar en micrositio del SGSI el especialista a cargo) conforme a lo estipulado en P5.GTI Procedimiento gestión de incidentes de seguridad de la información.

4.3.2 Las vulnerabilidades detectadas que aún no se hayan convertido en incidentes y/o eventos deben ser reportados por medio de los canales establecidos por MIS para el reporte de incidentes.

4.3.3 Los incidentes de seguridad reportados para BYOD serán gestionados acorde a lo estipulado: en P5.GTI Procedimiento gestión de incidentes de seguridad de la información, por ejemplo: robo o perdida de equipo

5. GESTIÓN DEL RIESGO

5.1 Diseñar e implementar las medidas de control necesarias, con el fin de evitar incidentes de Seguridad de la Información siguiendo los lineamientos de la Norma ISO 27001y la ISO 27002: correspondiente a la aplicación de los controles que minimicen el riesgo de indisponibilidad, perdida de confidencialidad e integridad de la información.

5.2 Conexión de Equipos con infección de virus (malware, troyanos, códigos maliciosos). La conexión de un equipo infectado pone en riesgo la disponibilidad e integridad de la información y adicionalmente generara un incidente de seguridad impactando la operación de los procesos

5.3 Los riesgos asociados al uso de BYOD, deberán ser identificados por cada proceso en su matriz de riesgos

6. APROPIACION Y CONCIENTIZACIÓN

6.1 Los especialistas del eje de seguridad de la información estarán a cargo de la sensibilización a los colaboradores de la entidad sobre el uso adecuado de los dispositivos BYOD, así como también de concientizar sobre las amenazas y riesgos más comunes a los que se expone la entidad al permitir el acceso a sus recursos tecnológicos a través de este tipo de dispositivos.

7. ANEXOS

A4.MS.DE Anexo 4 Manual de políticas de seguridad de la información

8. DOCUMENTOS DE REFERENCIA

P5.GTI Procedimiento gestión de incidentes de seguridad de la información.

9. RELACIÓN DE FORMATOS

CODIGO	NOMBRE DEL FORMATO
F1.P2.GTI	Formato de Solicitud de Servicios de Tecnología
F9.P2.GTI	Formato Verificación de Equipos Personales

10. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
03/08/2022	Versión 1	Se realizan ajustes de forma en todo el documento. En el ítem 2. Alcance: se incluye a proveedores, judicantes y operadores. En adición, se da alcance a los procesos de Promoción y Prevención y a Protección. En el ítem 5 se incluye Gestión de Riesgo