GUÍA PARA USO DE DISPOSITIVOS PERSONALES BYOD

INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR

Tabla de Contenido

1. OBJETIVO

Establecer los lineamientos y directrices para que los colaboradores del ICBF puedan ejercer actividades en el marco de sus funciones u obligaciones contractuales 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 institucional 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, CAIVAS, CESPAS, CAVIF, SRPA, Casas de Justicia y Unidades Locales.

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.

AMENAZA: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

DATOS PERSONALES: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

INFORMACIÓN: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea USO DE DISPOSITIVOS MÓVILES PERSONALES - BYOD Código: GS01-I27 Versión: 1 Página 3 de 9 magnético, en papel, en pantallas de computadoras, audiovisual u otro.

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.

.

MALWARE: tipo de programa informático o código malicioso, cuyo objetivo es infiltrarse en un dispositivo sin la autorización del usuario, para dañar el sistema o causar un mal funcionamiento.

SISTEMA OPERATIVO: conjunto de órdenes y programas que controlan los procesos básicos de un computador y permiten el funcionamiento de otros programas.

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.

CIBERSEGRUIDAD: es la práctica de proteger sistemas, redes y datos de ataques digitales. Su objetivo es garantizar la **confidencialidad, integridad y disponibilidad** de la información, protegiendo contra amenazas como el malware, el phishing, el ransomware y otros tipos de ciberataques

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.

[1] Norma ISO 31000:2018

4. DESARROLLO

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 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, podría conllevar a la materialización de riesgos inherentes de seguridad y privacidad, ciberseguridad y continuidad de la operación. El uso de dispositivos personales sin verificación y revisión puede ocasionar incidentes de seguridad de la información, como pérdida o robo de información, robo de dispositivos, robo de credenciales y 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, Regionales, Centros Zonales, 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.

Toda la información de carácter institucional 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

4.1.2 Para la conexión del Dispositivo **BYOD** a la red institucional, éste debe cumplir con los siguientes requisitos: Sistema operativo con parches, antivirus actualizado y herramienta ofimática licenciada (la proporcionada por la entidad); así como también es de carácter obligatorio que estos equipos deben estar físicamente protegidos a través de usuario y contraseña de ingreso.

4.1.3 Es responsabilidad de los 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 la red institucional. Se deberá utilizar conexiones seguras y aplicar los lineamientos de la Política de Seguridad y Privacidad de la Información Ciberseguridad y Continuidad de la Operación.

4.1.4 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 de la Entidad.

4.1.5 El colaborador propietario del **BYOD** deberá velar por la instalación periódica de las actualizaciones de seguridad tanto para el sistema operativo, así como, para el antivirus instalado en el **BYOD**, , lo cual será validado por el soporte en sitio y/o ingeniero regional.

4.1.6 En caso de pérdida o robo de un dispositivo BYOD, el incidente o evento de seguridad de la información deberá ser reportado a la entidad a través de los canales de la Mesa Informática de Soluciones (MIS). Esto permitirá que se tomen las medidas necesarias para mitigar los riesgos asociados, como la desactivación remota del dispositivo, la revocación de credenciales y el monitoreo de posibles accesos no autorizados.

4.1.7 Todos los **BYOD** deben ser revisados previa solicitud del jefe inmediato o supervisor del contrato a través de una solicitud o requerimiento a la mesa de servicio (MIS), a través del F1.P2.GTI formato de solicitud de Servicios de Tecnología, para que el personal de mesa de servicios o ingeniero regional valide que estos dispositivos cumplan con las requisitos, condiciones técnicas y reglas de seguridad establecidas en este documento.

4.1.8 Al conectar un dispositivo **BYOD** a la red institucional, el propietario acepta los controles establecidos en la resolución que adopta la la Política de Seguridad y Privacidad de la Información Ciberseguridad y Continuidad de la Operación, así como, los anexos y procedimientos asociados los cuales están publicados en el portal web o intranet de la entidad.

4.1.9 Para el ingreso o salida de dispositivos **BYOD** a las instalaciones del ICBF, se deben registrar en la bitácora de ingreso y/o salida de equipos en la recepción.

4.1.10 Los dispositivos BYOD (equipo personal), que cumplan con los requisitos de seguridad para conectarse a la red ICBF, deberá tener en cuenta las buenas prácticas de seguridad de la información incluyendo: contar con contraseña o pin para el inicio de sesión en el equipo y cerrar sesión en aplicaciones y en el equipo cada vez que finalice su sesión o que se deba ausentar de su área o puesto de trabajo.

4.2 LINEAMIENTOS ESPECIALES

4.2.1 Una vez se autorice la conexión de un dispositivo **BYOD** a la red de dominio 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 Sistema de Gestión de Seguridad de la Información (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 Con el fin de prevenir riesgos asociados a la pérdida o fuga de información aplicados a los equipos **BYOD** autorizados, no se podrá almacenar información institucional de manera local en estos equipos 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 esta 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 o perdida o daño de los dispositivos personales BYOD.

4.2.4 Al usar en equipo BYOD el colaborador, proveedor o tercero se compromete a hacer uso productivo y seguro de la red de dominio ICBF.

4.2.5 Para acceder a la plataforma tecnológica y sistemas de información de la Entidad, el colaborador debe evitar hacer uso de redes de datos inalámbricas públicas; así como también dejar configurado su contraseña por defecto

4.3 INCIDENTES DE SEGURIDAD DE LA INFORMACION

4.3.1 Todos los incidentes o y/o eventos de seguridad relacionados con dispositivos **BYOD**, deben ser reportados inmediatamente a través de los canales disponibles de la Mesa Informatica de Soluciones (MIS), 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 y privacidad de la información, ciberseguridad y continuidad de la operación.

4.3.2 Las vulnerabilidades detectadas que aún no se hayan convertido en incidentes y/o eventos deben ser reportadas por medio de los canales establecidos por la Mesa Informática de Soluciones (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 y privacidad de la información, ciberseguridad y continuidad de la operación, 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 27001 y la ISO 27002: correspondiente a la aplicación de los controles que minimicen el riesgo de indisponibilidad, perdida de confidencialidad e integridad de la información del ICBF.

5.2 Conexión de Equipos con infección de virus (malware, troyanos, códigos maliciosos, ransomware). La conexión de un equipo infectado coloca en riesgo la confidencialidad, integridad y disponibilidad de la Información y adicionalmente generará un incidente de seguridad, impactando la operación de los procesos institucionales.

6. APROPIACION Y CONCIENTIZACIÓN

6.1 Los referentes y equipo 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 Manual de políticas de seguridad de la información

8. DOCUMENTOS DE REFERENCIA

P25.GTI Procedimiento Gestión de Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad

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
03/07/2024	Versión 3	Se realizan ajustes de forma en todo el documento y la Política de Seguridad y Privacidad de la Información Ciberseguridad y Continuidad de la Operación Se elimina: 4.3.4 Para acceso a la red institucional, al colaborador le será instalado el agente NAC, el cual permitirá el acceso a la red corporativa, verificando previamente el estado de la seguridad del equipo. 4.3.5 Cuando se requiera utilizar la VPN para acceder a la red institucional en un equipo BYOD (equipo personal), necesitará instalar un software especializado para la conexión el cual validará la postura de seguridad del dispositivo BYOD, estos resultados deben ser satisfactorios para proceder a permitir el acceso, de lo contrario se denegará y se comunicará al usuario la falencia de seguridad del dispositivo para su remediación la cual estará bajo responsabilidad del colaborador u operador propietario del equipo BYOD.
15/11/2022	Versión 2	Se realizan ajustes de forma en todo el documento y se actualiza la resolución de la Política de Seguridad y Privacidad de la Información. En el ítem 2. Alcance se elimina el contenido de titulado “Excepción” En el ítem definiciones se incluyeron los siguientes términos: Amenaza, Información, Datos Personales, Nac, Malware, Sistema Operativo. En el ítem 4.2 Lineamientos especiales se agrega: 4.2.4 “El colaborador se compromete a hacer uso productivo y seguro de la red de dominio ICBF”. 4.2.5 “Para acceder a la plataforma tecnológica y sistemas de información de la Entidad, el colaborador debe evitar hacer uso de redes de datos inalámbricas públicas”. 4.2.6 “Para acceso a la red institucional, al colaborador le será instalado el agente NAC, el cual permitirá el acceso a la red corporativa, verificando previamente el estado de la seguridad del equipo”. 4.2.7 “Cuando se requiera utilizar la VPN para acceder a la red institucional en un equipo BYOD (equipo personal), necesitará instalar un software especializado para la conexión el cual validará la postura de seguridad del dispositivo BYOD, estos resultados deben ser satisfactorios para proceder a permitir el acceso, de lo contrario se denegará y se comunicará al usuario la falencia de seguridad del dispositivo para su remediación la cual estará bajo responsabilidad del colaborador u operador propietario del equipo BYOD”.
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.