CONTENIDO

Nombre: John Edward Molano Hernández Cargo: Coordinador Grupo de Trabajo de Servicios Tecnológicos y Seguridad Digital.	Revisado y Aprobado por: Nombre: Oscar Javier Asprilla Cruz Cargo: Jefe Oficina de Tecnología e Informática.	Aprobación Metodológica por: Nombre: Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad. Fecha: 2018-08-24

1. OBJETIVO

Establecer las condiciones para permitir el uso de dispositivos móviles personales, en el ámbito de la Superintendencia de Industria y Comercio, para llevar a cabo actividades laborales.

2. DESTINATARIOS

Servidores públicos, contratistas y terceros de la SIC.

3. GLOSARIO

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

BYOD: Trae tu propio dispositivo, por sus siglas en ingles Bring Your Own Device.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

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

DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

DISPOSITIVO MÓVIL: Aparato electrónico con capacidades de procesamiento, con conexión a Internet, con memoria, diseñado específicamente para una función, que pueden llevar a cabo otras funciones más generales. Son dispositivos móviles: los teléfonos inteligentes, tabletas y equipos portátiles.

INCIDENTE DE SEGURIDAD: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

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

magnético, en papel, en pantallas de computadoras, audiovisual u otro.

INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos.

NAC: Control de acceso a la red de datos, por sus siglas en ingles Network Access Control, es una tecnología que permite controlar que dispositivos pueden acceder a la red de datos institucional.

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.

P2P: Acrónimo de peer to peer, que significa de igual a igual, es un método de intercambio de archivos, aplicaciones, programas, fotos, vídeos, entre dos o más usuarios.

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

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

SOFTWARE: Conjunto de programas y rutinas que permiten al computador realizar determinadas tareas.

USUARIO: Se refiere a todo servidor público o contratista.

VULNERABILIDAD: Es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

4. GENERALIDADES

El uso de dispositivos móviles personales (computadores portátiles, smartphones,

tablets, etc.), de propiedad del servidor público o contratista, en el ámbito corporativo o institucional es lo que se conoce como BYOD (Bring Your Own Device). Se trata de una práctica muy frecuente, por lo tanto, se debe prestar especial atención para que su uso no comprometa la seguridad de la información de la entidad.

Existen ciertos riesgos que se deben conocer antes de permitir el uso de dispositivos personales en el ámbito institucional:

- La exposición a redes de datos inseguras en el ámbito personal. Este tipo de conexión podría tener como consecuencia que la información institucional fuera accesible o pudiera ser interceptada por terceras personas no autorizadas.

- La instalación de aplicaciones que solicitan permisos para acceder a partes del dispositivo donde puede haberse almacenado información sensible, e incluso solicitar la activación de la geolocalización.

- La inexistencia de mecanismos de control de acceso a los dispositivos y la ausencia de medidas de seguridad en cuanto al almacenamiento de la información. Si alguien tuviera acceso al dispositivo no tendría ninguna dificultad a la hora de acceder o extraer información confidencial.

- La carencia de herramientas antivirus y de una normativa de actualizaciones adecuada. Actualizar las aplicaciones y disponer de un antivirus protegen al dispositivo de posibles ataques y accesos no autorizados.

- La opción (activada) de recordar y usar contraseñas de forma automatizada para acceder a redes de datos, aplicaciones, sitios web, etc. Si alguien tuviera acceso al dispositivo no necesitaría disponer de las credenciales de usuario para acceder a la información.[1]

La Superintendencia de Industria y Comercio, a través del presente documento, establece las directrices para la conexión a la red de datos de un dispositivo móvil personal, así como para el acceso a los servicios y recursos informáticos de la entidad.

[1] Instituto Nacional de Ciberseguridad – INCIBE.

En particular para los dispositivos móviles personales, la SIC presta los siguientes servicios:

- Correo electrónico institucional.
- Google Drive.
- Calendario.
- Formularios.

El presente documento tiene en cuenta las buenas prácticas de seguridad de la información en los dispositivos móviles para reducir los riesgos, de manera que no se vea comprometida la red de datos de la entidad, sus servicios y la confidencialidad de la información de la SIC.

5. DESCRIPCIÓN DE ACTIVIDADES Y RESPONSABILIDADES

5.1 Verificar el cumplimiento de las condiciones en teléfonos inteligentes y tabletas.

Antes de ingresar a la red de datos inalámbrica de la entidad o acceder desde cualquier otra red a los servicios de la SIC para dispositivos móviles, el usuario debe garantizar la implementación de los siguientes controles o requisitos en sus teléfonos inteligentes, tabletas personales, etc.:

Tipo de requisito	Descripción
Mecanismo de autenticación.	Debe tener un esquema de autenticación y desbloqueo, por contraseña, huella o patrón de movimiento.
Bloqueo programado.	Debe bloquearse automáticamente tras un periodo de inactividad.
Propiedad intelectual.	El software instalado debe ser de uso legal.
Protección contra malware.	Debe contar con antivirus actualizado para evitar el riesgo de infección por malware.
Borrado remoto de datos.	Contar con un mecanismo que permita borrar la información del dispositivo móvil personal de manera remota, impidiendo su utilización por un usuario no legítimo.

Si el usuario cumple con los anteriores requisitos y ha decidido ingresar a la red de datos inalámbrica de la entidad o acceder a los servicios de la SIC, debe cumplir con las siguientes condiciones de uso:

- El usuario se compromete a hacer uso productivo y seguro de la red de datos inalámbrica de la SIC.

- Para el acceso a los servicios tecnológicos de la SIC, el usuario debe evitar hacer uso de redes de datos inalámbricas públicas.

Es de anotar que, para acceder a los servicios tecnológicos de la SIC desde dispositivos móviles, se debe descargar e instalar la aplicación Google Apps Device Policy, lo cual implica compartir con la SIC las siguientes características del equipo móvil personal: modelo, serie, IMEI, sistema operativo, idioma, ID de dispositivo, operador, número de compilación, versión de kernel, versión de banda base, última sincronización, fabricante, parches de seguridad, versión de lanzamiento, marca, hardware y estado de la encriptación.

5.1.1. Tratamiento de Datos Personales

La configuración y uso de los servicios de la SIC en los dispositivos móviles personales, conlleva el siguiente tratamiento de datos personales:

- La SIC, a través de Oficina de Tecnología e Informática - OTI, podrá borrar todos los datos del dispositivo móvil de forma remota, siempre y cuando exista una solicitud escrita del propietario del dispositivo debidamente justificada (memorando o e-mail), con la finalidad de proteger la confidencialidad de la información institucional.

- La SIC, a través de Oficina de Tecnología e Informática - OTI, podrá acceder a la ubicación del dispositivo móvil de forma remota, siempre y cuando exista una solicitud escrita del propietario del dispositivo debidamente justificada (memorando o e-mail), con la finalidad de recuperar el dispositivo y la información contenida en él, en caso de extravío.

- La SIC, a través de Oficina de Tecnología e Informática - OTI, podrá eliminar la cuenta institucional del dispositivo móvil de forma remota, cuando se identifique el incumplimiento de cualquiera de las políticas de seguridad de la información de la SIC o finalice la relación laboral o contractual con la entidad, con la finalidad de proteger la confidencialidad, integridad y disponibilidad de la información institucional.

Nota: Las acciones y políticas configuradas en el dispositivo móvil podrán ser consultadas en la aplicación Google Apps Device Policy.
Lo anterior, atendiendo y procurando el ejercicio de los derechos fundamentales, se establece por mandato legal, mediante Ley 1581 de 2012, el derecho de protección de datos personales, el cual se refiere a conocer, actualizar y rectificar cualquier información que sobre las personas se haya recopilado en bases de datos.

Los titulares de los datos gozarán de los derechos contemplados en la Ley y en la Política de Tratamiento de Datos Personales de la SIC, a la cual podrán acceder a través del siguiente link:

http://www.sic.gov.co/sites/default/files/files/Politicas_Habeas_Data_0.pdf.

5.2 Verificar el cumplimiento de las condiciones en equipos portátiles.

Antes de ingresar a la red de datos cableada o inalámbrica de la SIC, el usuario debe garantizar la implementación de los siguientes controles o requisitos en su equipo portátil personal:

Tipo de requisito	Descripción
Mecanismo de autenticación.	Debe tener un esquema de autenticación y desbloqueo por contraseña.
Bloqueo programado.	Debe bloquearse automáticamente tras un periodo de inactividad.
Actualización del sistema operativo.	Debe tener actualizado el sistema operativo con los últimos parches de seguridad.
Propiedad intelectual.	El software instalado debe ser de uso legal.
Protección contra malware.	Debe contar con antivirus actualizado para evitar el riesgo de infección por malware.
No tener software P2P.	No debe tener instalado programas P2P (peer-to-peer), utilizados para descarga e intercambio de archivos, por ejemplo: Ares, Emule, Bit Torrent, entre otros.
Control de redes.	Debe tener activo el firewall del equipo portátil, para limitar el acceso desde otras redes.
Acceso a la red corporativa.	Debe tener instalado el agente (NAC), el cual permitirá el acceso a la red corporativa, verificando previamente el estado de la

Tipo de requisito	Descripción
	seguridad del equipo.

El jefe inmediato, para el caso de los servidores públicos, o el supervisor del contrato, para los contratistas, debe solicitar a través de la mesa de servicios, las configuraciones necesarias para que el usuario pueda acceder a la red de datos cableada o red inalámbrica de la SIC desde su equipo portátil personal.

La mesa de servicios debe instalar el agente: *Extreme NAC Assessment* en el equipo portátil del usuario, el cual permitirá el acceso, siempre y cuando haya cumplido con los requisitos mínimos anteriormente mencionados.

Si el usuario ha decidido ingresar a la red de datos de la SIC desde su portátil personal, debe cumplir con las siguientes condiciones de uso:

- Hacer uso productivo y seguro de la red de datos.
- No realizar escaneos de vulnerabilidades sobre la red de datos de la SIC.
- Cifrar la información de la SIC, categorizada como reservada y/o clasificada, que esté almacenada en el equipo portátil personal.
- Informar a la SIC incidentes relacionados con fuga de información reservada y/o clasificada almacenada en el equipo portátil personal.

Nota: Un usuario que de manera temporal requiera el acceso a internet, deberá utilizar la red inalámbrica "Zona Wifi GRATIS para la gente".

6. DOCUMENTOS RELACIONADOS

SC05-I01 Políticas del Sistema de Gestión de Seguridad de la Información - SGSI.

7. RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Creación del documento.

_____

Fin documento