GUÍA DE SEGURIDAD DE LA INFORMACIÓN

GUÍA 20 DE SEGURIDAD SOBRE BUENAS PRÁCTICAS CUANDO SE UTILICEN MEDIOS TECNOLÓGICOS EN LA MODALIDAD DE TRABAJO NO PRESENCIAL

Código de identificación:	**GUÍA-20**
Versión y fecha:	**V1 marzo 2021**
Clasificación:	**FCC_USO_INTERNO**
Destinatario:	**Dirección de Sistemas y Tecnologías de la Información** **Todo el personal de las empresas del Grupo FCC cuya actividad pueda prestarse en la modalidad de trabajo no presencial (y utilicen Medios Tecnológicos para ello).**

INDICE

INTRODUCCIÓN

Como consecuencia de las medidas de contención sanitaria derivadas de la COVID-19 de las que se ha derivado excepcionalmente el desarrollo de la actividad laboral en la modalidad de trabajo a distancia, el Grupo FCC ha considerado necesario elaborar una Guía específica en la que se detallen un conjunto de buenas prácticas relacionadas con la materia de Protección de Datos y de Seguridad de la Información.

OBJETO

La presente Guía tiene por objeto detallar el conjunto de buenas prácticas definidas por el Dpto. Seguridad de la Información y Gestión de Riesgos Tecnológicos en materia de Protección de Datos y Seguridad de la Información, relativas al desarrollo de la prestación de servicios (a través de Medios Tecnológicos) por las personas trabajadoras de las empresas del Grupo FCC cuando presten sus servicios fuera de las instalaciones de éstas (en conjunto y en adelante, modalidad de "trabajo no presencial").

Todo lo anterior se debe al tratamiento de información corporativa que lleva a cabo la persona trabajadora cuando presta servicios fuera de las oficinas. A este respecto, debe entenderse como información corporativa a los efectos del presente documento "toda información empleada en el desarrollo de la actividad laboral", entre la que se encuentra, entre otras:

- Nombres de usuario y contraseñas.
- Documentación de trabajo de cualquier tipo, independientemente del soporte en que se encuentre.
- Información tratada a través de sistemas y aplicaciones corporativas (SAP, Outlook, Sharepoint, etc.).

ALCANCE

Esta Guía define las buenas prácticas de actuación en materia de Protección de Datos y Seguridad de la Información a observar por las personas trabajadoras cuando presten sus servicios en modalidad de trabajo no presencial.

En el mismo sentido, esta Guía abarca a todo equipo informático propiedad de las Entidades del Grupo FCC del tipo ordenador (portátil o fijo) que sean facilitados a las personas trabajadoras para el desempeño de sus funciones laborales (en adelante, los "equipos").

RECOMENDACIONES PARA LA PERSONA TRABAJADORA EN MATERIA DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

El presente apartado tiene como objetivo establecer unas recomendaciones cuando la persona trabajadora preste sus servicios fuera de las oficinas de la Empresa:

A) Protección de Datos Personales y confidencialidad de la información:

Toda persona trabajadora que acceda/gestione datos personales está obligada a conocer, observar y cumplir con lo establecido por la normativa en materia de Protección de Datos y, en especial, con lo siguiente:

- Acceder únicamente a aquella información o recursos a la que hubieran sido autorizados y que resulte mínima e imprescindible para el desarrollo de sus funciones. Cuando la persona trabajadora pueda acceder a información excesiva no necesaria para el desarrollo de sus funciones (por ejemplo, el acceso a carpetas de SharePoint o perfiles innecesarios en SAP), deberá poner esta circunstancia en conocimiento de sus responsables, para su revisión.

- Aplicar las funcionalidades de la herramienta corporativa Microsoft Teams (o la autorizada en cada momento) que permitan difuminar/modificar el fondo cuando se utilice la cámara, evitando que puedan aparecer personas ajenas a la organización, con especial cuidado con los menores. En el mismo sentido, la utilización de auriculares en las reuniones mediante llamada o videoconferencia permitirá preservar la confidencialidad de la información de Grupo FCC y sus empresas.

- Recapacitar, por adelantado, sobre la sensibilidad de los temas a tratar, la identidad de los participantes y la posible difusión en caso de que la reunión sea grabada.

- En caso de grabar la reunión, informar previa y adecuadamente a los asistentes de la finalidad de la grabación y en qué momento se inicia/detiene la misma.

- Cuando termine la reunión, asegurarse de utilizar un dispositivo que inhabilite físicamente la cámara (pestaña, adhesivo o similar).

- Almacenar la información únicamente en aplicaciones corporativas, en SharePoint o en carpetas de red corporativas, porque tienen implantadas las correspondientes medidas de seguridad. Nunca en el disco duro del equipo.

- Eliminar periódicamente la información temporal que pueda quedar almacenada en el equipo.

- Adoptar las precauciones y medidas de seguridad necesarias para garantizar la confidencialidad de la información corporativa que se está gestionando o a la

que se pueda tener acceso en la modalidad de trabajo no presencial, impidiendo el acceso por parte de terceros (salvo prestadores de servicios, cuando sea necesario para la prestación de los mismos).

- No utilizar USB/disco duro portátil para almacenar/extraer información con datos personales, por el alto riesgo de pérdida o falta de securización suficiente que existe.

- Almacenar la información únicamente por el tiempo imprescindible según las funciones laborales de cada persona trabajadora.

- Minimizar o, en la medida de lo posible, evitar la salida de documentación en soporte papel de las oficinas. En caso de que se deba mover circunstancialmente, mantenerla siempre localizada y con las medidas de seguridad adecuadas, de forma que se garantice su confidencialidad, integridad y disponibilidad.

- Las personas trabajadoras de las empresas del Grupo FCC deberán evitar emplear los equipos y sistemas corporativos para fines distintos del desarrollo de la actividad laboral.

- Almacenar la información (que se encuentre en soporte papel) en archivadores o cajones cerrados con llave. No obstante, no será necesario mantener archivada la documentación cuando se encuentre en proceso de revisión o tramitación por la persona trabajadora en la misma jornada, siendo ésta responsable de su custodia en todo momento y de archivarla al finalizar la jornada.

- Destruir los originales, copias o reproducciones de documentos con datos de carácter personal que ya no sean necesarios o que sean desechados, mediante el uso de máquinas destructoras de papel o por cualquier medio que impida que la información pueda ser recuperada.

- Notificar, de forma inmediata, cualquier violación de la seguridad (brecha de seguridad) que ocasione (o pueda ocasionar) la destrucción, accesos no autorizados, bloqueo de acceso, pérdida o alteración accidental o ilícita de la información transmitida, conservada o tratadas (p.e. pérdida o robo de un equipo) al Dpto. Seguridad de la Información a través de sdseguridad@fcc.es.

En todo caso, la persona trabajadora debe ser consciente de la importancia de sus responsabilidades en cuanto a no poner en peligro la integridad, disponibilidad y confidencialidad de la información que maneja de la organización y a la que tiene acceso por razón de sus funciones, así como de las consecuencias asociadas a la vulneración de dicho compromiso.

Por ello, la persona trabajadora se compromete a mantener la más estricta confidencialidad respecto de todos los documentos e información (tenga datos personales o no) que, por razón de sus funciones, pueda llegar a conocer, siguiendo las instrucciones del presente documento y no proporcionará información a ninguna persona externa o interna, excepto a las personas a las cuales esté autorizada por

razón de sus funciones y responsabilidades en el curso de su trabajo o, cuando una Ley así lo exija.

B) Seguridad de la Información

- Evitar la conexión de los dispositivos a la red corporativa desde lugares públicos o WIFI abiertas no seguras, así como desde equipos o sistemas que no sean corporativos o no hayan sido facilitados por la Empresa para el cumplimiento de sus funciones.

- Desactivar las conexiones WIFI, Bluetooth, NFC y similares que no estén siendo utilizadas.

- Para la gestión de las contraseñas, se deberá atender a lo indicado en la documentación elaborada y publicada por la Empresa en el documento NRM-11 Norma Seguridad Contraseñas, disponible en FCCOne.

- Proteger los mecanismos de autenticación definidos (certificados, contraseñas, tokens, sistemas de doble factor, etc.).

- Verificar la legitimidad de los correos recibidos, comprobando que el dominio electrónico del que procede es válido y conocido, y desconfiando de la descarga de ficheros adjuntos con extensiones inusuales o el establecimiento de conexiones a través de enlaces incluidos en el cuerpo del correo que presenten cualquier patrón fuera de lo normal. Ante cualquier duda sobre una situación que pudiera ser constitutiva de una brecha de seguridad de la información, contactar directamente con sdseguridad@fcc.es.

- Desconectar la sesión de acceso remoto y apagar o bloquear el acceso al dispositivo una vez concluida la jornada de trabajo.

- Si se trabaja habitualmente desde lugares públicos, es recomendable utilizar un filtro de privacidad para la pantalla y utilizar auriculares para conversaciones.

- No realizar ningún cambio, manipulación o modificación del hardware o software del dispositivo.

- No almacenar o dejar el equipo en una zona pública o en el coche.

- Evitar, en la medida de lo posible, los accidentes (derrames de líquidos, niños o mascotas desatendidas, etc.) en el equipo y dispositivo electrónico de la organización.

- No deshabilitar las medidas de seguridad implantadas en los dispositivos. Esto incluye, entre otros, conseguir permisos de administrador o permitir instalar software de fuentes no fiables.

- Gestionar a través del Service Desk (sistema de gestión de incidencias del Grupo FCC) el funcionamiento anómalo de los equipos y sistemas utilizados.

Algunas incidencias pueden ser:
  - Dificultades en el acceso remoto a las instalaciones corporativas.
  - Problema con la cuenta de usuario (contraseñas, permisos, etc.).

- Asimismo, toda persona trabajadora deberá conocer y cumplir con el resto de normativa de Seguridad del Grupo FCC ubicada en FCCOne.

En todo caso, las recomendaciones detalladas en la presente Guía tienen, como fin último y esencial, garantizar los conceptos de integridad, confidencialidad, disponibilidad y resiliencia en el Grupo FCC:

- La confidencialidad es la cualidad de la información corporativa de estar únicamente accesible a personas o sistemas autorizados.

- La integridad que implica que los datos de carácter personal no se alteren o que se puedan realizar modificaciones no deseadas.

- La disponibilidad de la información refleja la capacidad de acceso a la información inmediato a aquellos que cuenten con autorización.

- La resiliencia es, por último, la capacidad de un sistema de información de continuar funcionando a pesar de todas las incidencias que pudiera sufrir.

Por tanto, en caso de no cumplir con las instrucciones y recomendaciones detalladas, la seguridad de la información corporativa podría verse comprometida en cualquier momento, con las implicaciones y consecuencias que ello conlleva.

OBLIGACIONES DE LAS EMPRESAS DEL GRUPO FCC RESPECTO AL ESTADO Y SEGURIDAD DE LOS EQUIPOS Y SISTEMAS EN LA MODALIDAD DE TRABAJO NO PRESENCIAL

Las Empresas del Grupo FCC asumen ciertas tareas y obligaciones que tiene que llevar a cabo para garantizar la seguridad de la información en cualquier modalidad de trabajo no presencial.

En todo caso:

- Deberán mantener los equipos y dispositivos electrónicos, propiedad de la misma, actualizados según los requerimientos del DSTI.

- El software o sistema que deberá mantenerse actualizado e implantado incluye, entre otros:
  - Sistema operativo de los equipos y dispositivos electrónicos.
  - Versión de sistemas y aplicaciones.
  - Software antivirus y cortafuegos.
  - Controladores de los distintos sistemas y programas.
  - Software antimalware actualizado.

- Acceso restringido por contraseña.
- Bloqueo automático de sesión.

MONITORIZACIÓN

FCC ostenta un derecho de supervisión y control (uno de carácter regular, preventivo y aleatorio; y otro de carácter investigador y específico) que gestiona de conformidad con lo previsto en la Política de Uso de Medios Tecnológicos que se encuentra disponible en la Intranet (https://fccone.fcc.es/web/one-tiseguridad/-/politicas-normas-y-guias-de-seguridad-de-la-informacion).

En el caso de que se detecte que se han utilizado indebidamente los Medios Tecnológicos o para comprobar el correcto cumplimiento por sus personas trabajadoras de sus obligaciones laborales, las empresas del Grupo FCC podrán adoptar las medidas que resulten necesarias y, entre ellas, poner fin a las conductas prohibidas, y adoptar las medidas disciplinarias correspondientes. Todo ello, respetando los derechos de las personas trabajadoras y los requisitos que se establecen en la normativa que sea de aplicación.

REVISION DE ESTA GUÍA

Entre los supuestos que podrán originar una revisión de esta Guía se encuentran:

- Propuestas de mejora formuladas por las auditorías efectuadas.
- Cambios tecnológicos significativos.
- Cambio en la legislación vigente concerniente a lo que a esta Guía expresa.

La información que se tome como base para la revisión de esta Guía, será comunicada a la Dirección de Seguridad de la Información, quien a su vez la trasmitirá al Comité de Dirección de la Seguridad de la Información.

REFERENCIAS

Normativa relacionada

- Política de Seguridad de la Información de FCC.
- Control 6.2.2 Teletrabajo de la ISO 27001.
- Política de Uso de Medios Tecnológicos de FCC

CONTROL DE CAMBIOS EN DOCUMENTO

Información de Documento

NOMBRE FICHERO:				
VERSION	FECHA	CAMBIO	AUTOR	REVISADO

				POR
1.0	20/04/2021	Generación del documento	DSIGRT	DSIGRT

FIN DEL DOCUMENTO