CIRCULAR 62 DE 2014

(junio 16)

<Fuente: Archivo interno entidad emisora>

MINISTERIO DE RELACIONES EXTERIORES

Bogotá, D.C.,

Para:	Servidores Públicos
De:	María Ángela Holguín Cuéllar Ministra de Relaciones Exteriores
Asunto:	Instrucciones Seguridad Institucional

Respetados Servidores:

Con sujeción a la dispuesto en los Decretos 1599 de 2005, 4485 de 2009 mediante los cuales se adopta el Modelo Estándar de Control Interno para el Estado Colombiano, y se aprueba la actualización de la Norma Técnica de Calidad en la Gestión Pública NTCGP 1000, los Códigos Único Disciplinario y de Ética, respectivamente, el Manual de Seguridad Informática adoptado por el Mínisterio, y el Contrato de Prestación de Servicios de seguridad y vigilancia privadas suscrito por el Fondo Rotatorio de Relaciones Exteriores, resulta importante recordar algunos de los deberes y obligaciones de los funcionarios, contratistas, proveedores y grupos relacionados en materia de seguridad.

I. SEGURIDAD DE LAS INSTALACIONES, CONTROL DE INGRESO Y SALIDA PEATONAL Y VEHICULAR.

Con el fin de que las medidas y procedimientos de seguridad implementados al interior de esta Entidad, contribuyan a la protección efectiva de los activos oficiales, y a la creación de un ambiente seguro, resulta importante recordar algunos de los deberes y obligaciones de los funcionarios, contratistas, proveedores y grupos relacionados en materia de seguridad:

- Porte obligatorio del carnet vigente, dentro de las instalaciones del Ministerio, pata los funcionarios, contratistas, pasantes o judicantes.

- Instalación en las porterías de un nuevo software de control de visitantes, con registro de fotografía y huella dactilar, y traspaso al visitante de un porta sticker con cordón de color para su diferenciación, previa entrega por parte del visitante de un documento con foto, que no corresponda a la cédula de ciudadanía.

- Requisa de bolsos y paquetes que entren o salgan del Ministerio y monitoreo permanente por parte de los guardas de seguridad en los pasillos, quienes deberán informar inmediatamente al supervisor de turno cualquier novedad que se le presente en su puesto de trabajo.

- Ingreso y retiro de equipos, medios de informacíón etc, de las instalaciones del Ministerio de Relaciones Exteriores, por parte de servidores públicos o visitantes, mediante el diligenciamiento en las porterías de acceso peatonal, del formato de control de entrada y salida de elementos.

- Ingreso del visitante, previa autorización de un servidor público de Cancillería (Funcionarios, contratista, pasante, judicante etc), quien deberá recogerlo en la portería y volverlo a dejar allí

para su salida de la Entidad.

El visitante que ingresa a la Entidad, por ningún motivo puede quedar solo en las instalaciones del Ministerio de Relaciones Exteriores.

- Identificación plena de los funcionarios que ingresan con los vehículos. Revisión del baúl de los vehículos, incluyendo espejo convexo y detector de metales.

- Prohibición de ingreso al Ministerio, de personal externo, a través del acceso vehicular. El visitante sólo podrá acceder a la Entídad a través de las entradas peatonales, y siempre sujetándose al procedimiento arriba indicado.

Por tanto, los guardas de seguridad no permitirán el ingreso de visitantes dentro de los vehículos y motos, de servidores públicos.

- Prohibición de ingreso o retiro de cualquier equipo en los vehículos de los funcionarios, contratistas, judicantes, pasantes etc, sin el debido registro en las porterías establecidas para el efecto.

- Guarda bajo Ilave de los equipos de cómputo portátiles, proyectores, teléfonos celulares, Emp3, gps, cámaras fotográficas, de video, ipad, iphone, tabletas etc, asignados a los servidores públicos, para el cumplimiento de sus tareas, al finalizar la jornada laboral o durante su retiro prolongado de la oficina.

- Cuidado permanente de los objetos personales por parte los funcionarios, contratistas, pasantes, judicantes etc. Todos los escrítorios y puestos de trabajo cuentan con cerraduras en los cajones para guardar con llave sus pertenencias.

El acatamiento de las medidas relacionadas contribuirá significativamente a gestionar el siempre presente riesgo sobre los activos y los datos oficiales.

II. SEGURIDAD INFORMÁTICA

La información es el activo más importante de cualquier organización y su gestión y administración comporta un proceso de la mayor importancia que involucra una estrategia de administración de riesgos y la consolidación de una cultura de seguridad.

Conscientes de las necesidades actuales, debe implernentarse un modelo de gestión de seguridad de la información como una herramienta que permita identificar y minimizar los riesgos a los cuales se expone la información, ayude a la reducción de costos operativos y financieros y establezca una cultura de seguridad., donde los usuarios son el punto más vulnerable en la cadena de seguridad, ya que su desconocimiento de unas buenas prácticas puede ocasionar incidentes que ponen en riesgo la SEGURIDAD, CONFIDENCIALIDAD E INTEGRIDAD de la información.

Con fundamento en lo expuesto, paso a destacar las principales prácticas informáticas que deben ser aplicadas por todos los servidores de Cancillería (Funcionarios, contratistas, pasantes, judicantes y terceros), a saber:

- Uso de los activos de información para actividades no relacionadas con las funciones asignadas.

- Instalación en los equipos de la Entidad, de programas, macros, programas, applets, controles ActiveX, etc.) o cualquier dispositivo físico o cualquier otro tipo de secuencia de órdenes.

- Reproducción en los Sistemas de Información o en la Red Corporativa contenidos, groseros, amenazadores, ínmorales u ofensivos.

- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

- Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados, sin la previa autorización del jefe inmediato.

- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos informáticos telemáticos o acceder de manera indebida a la información de otros funcionarios.

- Intentar destruir, alterar, inutilizar o dañar los datos, programas o documentos electrónicos.

- Albergar datos de carácter institucional para uso no autorizado.

- Incurrir en cualquiera de las conductas contempladas en la Ley 1273 de 2009 sobre protección de Información y de datos.

- Usar de manera indebida, mal intencionada, imprudente el servicio de internet, el cual al ser una herramienta de trabajo, debe colocarse al servicio de la Entidad en la ejecución responsable y confiable de las labores asignadas.

- Modificar o alterar la configuración de los computadores, dispositivos o equipos de comunicación para ingresar a sitios no autorizados.

- Transmitir información no autorizada o de carácter confidencial o reservada, de propiedad del Ministerio de Relaciones Exteriores y/o su Fondo Rotatorio, de los ciudadanos, de sus funcionarios y/o terceros.

- No otorgar acceso a cuentas de correo electrónico a estudiantes que estén realizando su pasantía con el Ministerio de Relaciones Exteriores.

- Usar la cuenta de usuario de correo electrónico solamente para el desempeño de las funciones, las cuales se encuentran bajo el dominio cancillería.gov.cosiendo de propiedad del Ministerio de Relaciones Exteriores.

-

No se pueden ejecutar a través de ella, actividades que vayan en contravía de la ley, de carácter malintencionado o que atenten contra terceros o la seguridad de la información.

- Enviar información corporativa, de manera exclusiva, a través de la cuenta de correo que el Ministerio de Relaciones Exteriores proporciona.

- Responder de todas las actividades realizadas con las cuentas de correo proporcionada por la Entidad, dado el carácter personal e intransferible del mismo y de sus claves, las cuales son confidenciales.

- Envío de correo masivos y/o publicitarios, únicamente a través de las cuentas institucionales creadas para tal fin.

- Borrar o descargar oportunamente los correos con el fin de liberar espacio en el servidor, evitando el bloqueo del buzón. Lo anterior teniendo en cuenta usuario con correo electrónico corporativo tiene derecho a la asignación de un espacio limitado de almacenamiento en el servidor.

- Tratar con precaución el correo proveniente de un destinatario no conocido. Por ninguna razón debe ser respondido, ni ejecutar archivos adjuntos que contenga.

- Avisar a mesa de ayuda, cualquier eventualidad en el servicio de correo electrónico que comprometa la integridad y confidencialidad de la información del buzón como: uso no autorizado, suplantación, abuso, pérdida de la contraseña, entre otras.

Así las cosas, me permito convocar a todos los funcionarios, contratistas, pasantes y terceros del Ministerio, a las jornadas de reinducción que serán impartidas por la Dirección de Gestión de Información y Tecnología y la Coordinación de Servicios Generales, según cronograma anexo a esta Circular, y a que participen activamente en la aplicación de las políticas de seguridad definidas en el Manual de seguridad de la Información expedido por la Entidad, el cual recoge un conjunto de buenas prácticas de seguridad mostrando la forma más correcta de actuar ante situaciones del día a día en el entorno profesional.

En las condiciones anotadas, se agradece la colaboración de todos y cada uno de los servidores públicos vinculados bajo las distintas modalidades al Ministerio de Relaciones Exteriores.

Cordialmente,

MARÍA ÁNGELA HOLGUÍN CUÉLLAR
Ministra de Relaciones Exteriores

Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.
Normograma del Ministerio de Relaciones Exteriores
ISSN 2256-1633
Última actualización: 15 de enero de 2024 - (Diario Oficial No. 52.621 - 27 de diciembre de 2023)