RESOLUCION No. 311-2022
(09 NOVIEMBRE DE 2022)

POR MEDIO DE LA CUAL SE ESTABLECE LA POLITICA DE CONTROL DE ACCESO Y CONTRASEÑA DEL HOSPITAL DEPARTAMENTAL SAN RAFAEL ESE

El Gerente del Hospital Departamental San Rafael De Zarzal E.S.E., Valle del Cauca, en uso de las atribuciones legales y constitucionales, y demás normas concordantes y reglamentarias, y,

CONSIDERANDO

El Decreto 1011 de 2006: "Por el cual se establece el sistema Obligatorio de Garantía de Calidad de la Atención de Salud del Sistema General de Seguridad Social en Salud".

El Ministerio de Tecnologías de la Información y las comunicaciones mediante el modelo de seguridad de la información de seguridad de la información: Estrategia de GOBIERNO EN LÍNEA de diciembre 2008.

La Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

La Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho al Acceso a la Información Pública Nacional y se dictan otras disposiciones.

El Decreto 103 de 2015: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

El Decreto 1078 de 2015: Decreto único reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

El Decreto 1494 de 2015: Por el cual se corrigen yernos en la Ley 1712 de 2014.

El Decreto 1499 de 2017: Por medio del cual se modifica el Decreto 1083 de 2015,

El Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

RESUELVE:

CAPITULO I
DISPOSICIONES GENERALES

ARTICULO 1. OBJETIVO. Garantizar que la información, las áreas de procesamiento de información, las redes de datos, los (equipos y/o dispositivos) de la plataforma tecnológica y los sistemas de información del Hospital Departamental San Rafael de Zarzal E.S.E. estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

ARTICULO 2. AMBITO DE APLICACIÓN. Esta política aplica a toda la información contenida en cualquier medio (digital o físico), áreas de procesamiento de información, redes de datos, (equipos y/o dispositivos) de la plataforma tecnológica y sistemas de información del Hospital Departamental San Rafael de Zarzal E.S.E. y personas que tengan acceso a las instalaciones de la Entidad y sistemas de información.

ARTICULO 3. DEFINICIONES

a) **Acceso**: En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas del Hospital Departamental San Rafael Zarzal en un momento dado.
b) **Acceso físico**: Significa ingresar a las áreas o instalaciones en general de un sitio de la entidad.
c) **Acceso lógico**: En general, el acceso lógico es un acceso en red, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos. La mayoría de los accesos lógicos del sistema de información se relacionan con algún tipo de información.
d) **Personal**: Es aquella persona que tiene una relación laboral directa o a través de un tercero, bajo cualquier tipo de vinculación Planta, contratistas, estudiantes en práctica, etc.

ARTICULO 4. GENERALIDADES. Para la Entidad es prioritario definir el personal que tenga acceso a información sensible, por lo cual limita el acceso de usuarios de aplicaciones computarizadas únicamente a los funcionarios y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades y funciones a cargo, debido a que la información puede ser sensible o tener un carácter confidencial. Así mismo es necesario restringir el acceso a las instalaciones donde dicha información se encuentra guardada, garantizando así la confidencialidad e integridad de la misma. La plataforma tecnológica es responsabilidad de la Oficina de sistemas, así como los sistemas de información de la Entidad que formalmente le han sido asignados, en donde se establecen los controles de acceso pertinentes a dichos recursos. Hospital Departamental San Rafael de Zarzal E.S.E., es responsable de garantizar entornos con controles de acceso idóneos, los cuales aseguren el perímetro, tanto en oficinas, como en entornos abiertos para evitar el acceso no autorizado a ellos.

DIRECTRICES DE SEGURIDAD PARA TODO EL PERSONAL

Para dar cumplimiento al control de acceso a la información, todos los involucrados en el alcance deberán acatar lo siguiente:

- Se deberá asignar un nombre de usuario y contraseña para conceder el acceso a los sistemas de información del Hospital.
- Para generar acceso al sistema a proveedores o contratistas, el supervisor del contrato o al que designe debe realizar la solicitud al área de sistemas, registrando la información sea digital o en físico en el formato de autorización de acceso al sistema.
- Se deberá inactivar en el sistema de información asistencial y financiero los usuarios correspondientes al personal que ya no tenga relación con el Hospital.
- Se deberán realizar revisiones periódicas en los diferentes sistemas del Hospital para garantizar que se inactiven los usuarios redundantes o que no trabajan ya en el Hospital, mínimo una vez al mes.
- Cada miembro del personal del Hospital, deberá hacerse responsable de los usuarios y contraseñas asignados para el acceso a los servicios de red, y acceso al (Sistema de información Administrativo y Asistencial), igualmente a las IP fijas asignadas para el acceso al internet y de todos los recursos de la plataforma tecnológica y los sistemas de información.

- El personal no deberá compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes, este funcionario se hace responsable de lo que se haga en el sistema con su usuario asignado en el sistema de información.
- Después de la asignación de la clave de acceso al sistema de información el usuario deberá cambiar la clave que se le asigna en sistemas, teniendo en cuenta que debe contener números letras mayúsculas, minúsculas o un carácter especial y deberá ser cambiada al menos trimestralmente.
- Los jefes de área del Hospital y de sus sedes serán los encargados de informar los permisos de acceso a los usuarios adecuados para cada funcionario que entre al sistema de información y a las redes.
- El acceso al correo electrónico institucional será exclusivo del empleado y si es retirado de la institución no podrá hacer uso de él.
- El acceso al sistema de información externamente debe ser autorizado por el jefe del área, que será el encargado de firmar "formato de autorización de acceso al sistema", el cual reposará en el área de sistemas de información.
- Las contraseñas no deben tener nombres que identifiquen fechas de nacimiento o nombre de la familia para que sea más difícil la identificación.

NORMAS DE SEGURIDAD PARA EL CONTROL DE ACCESO LÓGICO

- El jefe de área o líder de proceso, agremiación sindical, talento humano o área de contratación deberá ser el único autorizado para solicitar el acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información; así mismo debe especificar los privilegios de acceso usando el formato de autorización de acceso al sistema.
- La administración de los perfiles de usuario es responsabilidad de los administradores de cada aplicación (sistema) y de las áreas responsables de dicho activo.
- Los administradores de cada aplicación (sistema) deberán crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información cuando esto sea solicitado por el jefe de área o líder de proceso.
- Sistemas entrega los usuarios y contraseñas al personal interno y externo que tendrán acceso a los servicios de red del Hospital, a los recursos de la plataforma tecnológica o a los sistemas de información, la clave asignada debe ser cambiada después de entregada.
- Talento humano, agremiación y contratación deberá verificar periódicamente las novedades de personal y validar la eliminación, reasignación o la inactivación de las cuentas de acceso como también los cambios de puesto de trabajo para la reasignación de permisos y del activo fijo (recursos tecnológicos y sistemas de información) del Hospital.
- Se deberá establecer controles de acceso a los sistemas de información y garantizar que solo el personal autorizado tenga los privilegios adecuados para garantizar el acceso a la información.
- Se deberán establecer mecanismos de auditoria al personal encargado de la administración del acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información.

- Para el ingreso y retiro del personal tanto de planta como contratados y Ordenes de servicios se registrará la autorización en el formato establecido.
- Para el acceso al sistema de información administrativo y Asistencial, se inactivará al personal tanto de planta y contratados y ordenes de trabajo que tenga novedad de ausentismo por retiro, incapacidad, licencia luto, permiso mayor a 3 días, permiso.
- No se creará ningún usuario al sistema de información financiero y asistencial sin la autorización del área de talento humano, la coordinación de la agremiación sindical y el área de contratación para los contratados por órdenes de servicios.

DIRECTRICES DE SEGURIDAD PARA EL CONTROL DE ACCESO FÍSICO

- Se deberá identificar el personal que requiere acceso al área de sistemas, autorizar su ingreso.
- Se deberá contar con mecanismos de control de acceso para guardar las llaves, de los gabinetes del área de sistemas.
- Las puertas de acceso al área de sistemas de información, deberán permanecer siempre cerradas y aseguradas. De igual manera, los gabinetes y puertas de los equipos que se encuentran en las áreas mencionadas deberán permanecer cerradas.
- Se deberá acompañar permanentemente a los visitantes durante su estancia en las áreas mencionadas.
- Se deberá monitorear los ingresos al centro de cableado permanentemente para identificar accesos no autorizados.
- Se deberá restringir de manera inmediata los privilegios de acceso físico a las instalaciones del Hospital tan pronto el personal termine su vinculación.
- Se deberá implementar controles de acceso físico al centro de cómputo para evitar la manipulación no autorizada del cableado.

ARTICULO 5. INCUMPLIMIENTO

El incumplimiento de esta política de seguridad y privacidad de la información traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

ARTICULO 6. RESPONSABILIDADES

a) **Equipo de Seguridad de la Información:** Velar por el cumplimiento de la presente política para garantizar el adecuado control de acceso lógico y físico definido por el Hospital.
b) **Jefe de la Oficina de sistemas:** Poner a disposición los recursos necesarios para el cumplimiento de los lineamientos descritos en la presente política.
c) **Talento Humano de planta y de contrato, adscritos:** Deberán informar a la Oficina del sistema cuando finalice el contrato de cualquier miembro del personal del Hospital Departamental San Rafael de Zarzal E.S.E.
d) Todo el Personal: No deberán acceder a las áreas seguras sin autorización, a excepción que sea en cumplimiento de sus obligaciones con el Hospital. Dar cumplimiento a esta política.

ARTICULO 7: La presente resolución rige a partir de la fecha de su expedición

COMUNIQUESE, NOTIFIQUESE Y CUMPLASE:

Dada en Zarzal Valle del Cauca, a los nueve (09) días del mes de noviembre del año dos mil veintidos (2022).

Julián Andrés Correa Trujillo
Gerente
Hospital Departamental San Rafael Zarzal E.S.E.

Elaboro: Sandra Rincón – Coordinadora de sistemas
Reviso: Paulo Castillo Ferreira – Asesor de Calidad
Aprobó: Julián Andrés Correa Trujillo – Gerente