



La Coordinadora Staff Tecnología de la Información y Comunicación del Hospital Alma Máter de Antioquia

Certifica que:

Que la Plataforma GHIPS, Sistema de información del Hospital Alma Máter de Antioquia, aplicación WEB desarrollada in house, cumple con los siguientes criterios para la seguridad de la información:

1. Dispone de mecanismos de Identificación y autenticación que previenen los accesos no autorizados basados en la existencia de un identificador unívoco de usuario y contraseña, personal e intransferible.
2. La creación de un nuevo usuario se realiza atendiendo al procedimiento establecido y controlado desde el proceso de Talento Humano y previa autorización del responsable competente.
3. Permite asociar períodos de validez a los usuarios del sistema de forma que fuera de ese rango de fechas el sistema prevenga la autenticación a través de dicho usuario.
4. Garantiza el cambio de la asignación de contraseña inicial obligando al cambio de contraseña en el primer ingreso del usuario al sistema.
5. Solicita el cambio de contraseña, obligatorio, de forma periódica cada 3 meses. Existe un histórico de contraseñas que previene la re-utilización de la contraseña anterior.
6. La contraseña tiene, al menos, una longitud mínima de 7 caracteres y unas reglas adicionales de complejidad en base al grado de madurez de los controles de seguridad implantados.
7. Las contraseñas se almacenan de forma encriptada.
8. Bloqueo automático de usuarios del sistema por intentos reiterados de acceso fallidos (6 intentos).
9. Bloqueo automático por no acceso en un determinado período de tiempo (tres meses) con objeto de regularizar las cuentas activas.
10. Bloqueo manual por parte del Administrador del sistema en caso de una situación que lo requiera.
11. No se permite, con carácter general, el acceso a través de usuarios genéricos.
12. El acceso está basado, en perfiles y roles:

Estos mecanismos determinan, en base a las necesidades autorizadas de los usuarios, dos aspectos fundamentales:

- Las funcionalidades (de las previstas por el sistema de información) a las que podrán acceder (basado en accesos del menú).
 - Los datos a los que deberán tener acceso.
13. Cierre de sesión por inactividad. Tras un período de inactividad (20 minutos) se activa un mecanismo de bloqueo que evite la suplantación del usuario en momentos en los que su equipo no esté atendido.



14. Los accesos al sistema mantienen un registro que incluye, la identificación del usuario, la fecha y hora en la que se realizó el acceso, la IP del equipo de cómputo desde el cual se realizó el acceso y si ha sido autorizado o denegado.
15. Los accesos a las Historias Clínicas mantienen un registro que incluye, la identificación del usuario, la fecha y hora en la que se realizó el acceso, el tipo de acceso.
16. Existe una separación efectiva entre los entornos de desarrollo de software y producción.
17. El área de desarrollo tiene implementado el proceso de Validación de los productos el cual consisten en la realización de las pruebas de revisión que verifican que el sistema de software producido cumple con las especificaciones y que logra su cometido.
18. El área de desarrollo tiene implementado el proceso de Gestión de la Configuración que incluye el Control de Versiones y Control de cambios de los sistemas de información.
19. Se cuenta con la debida documentación de las diversas versiones en el entorno de desarrollo (producción y despliegue).
20. La institución y el área de desarrollo garantizan la NO utilización de datos e información real extractada de la historia clínica electrónica y sus registros clínico asistencial y administrativos para ser utilizados durante las pruebas de producción o desarrollo de programas que puedan vulnerar la confidencialidad, reserva, intimidad y seguridad del paciente.
21. Revisiones periódicas de usuarios autorizados. Periódicamente, cada seis meses se realiza, por parte de los usuarios competentes, una revisión de los usuarios autorizados para identificar usuarios con acceso indebido potencial a los sistemas.
22. Registro de usuarios con privilegios de administración. Existe un registro de usuarios con privilegios de administración (asociados a tareas habituales de mantenimiento y explotación de sistemas o como consecuencia de accesos de soporte de usuarios de desarrollo a producción). Este registro incluye el usuario autorizado, el período de validez, el responsable de la autorización y las tareas a realizar por el mismo.
23. La red en la que se ubican los sistemas y a la que accedan los usuarios de los sistemas de información está protegida de accesos no autorizados.
24. Se desarrollan mecanismos de formación y concientización específicamente orientados a la seguridad de la información.
25. El acceso a otras redes está protegido a través de cortafuegos (firewalls) que aseguren en las comunicaciones a través de las redes locales un nivel de protección suficiente frente a las amenazas de terceros.
26. Existencia y actualización periódica de mecanismos de protección frente a virus u otros códigos maliciosos.
27. Con carácter general, los privilegios de administración en los propios equipos de los usuarios están restringidos. Es decir, se prevendrá la instalación de software no autorizado en los equipos de los usuarios por parte de los mismos.
28. La conectividad remota (“teletrabajo”) a través de redes públicas de datos estará adecuadamente protegida, en línea con las soluciones tecnológicas de seguridad existentes.
29. La conectividad a través de redes inalámbricas para acceder a los sistemas de información requiere de una configuración específica.



30. La administración de forma remota de los equipos y servidores, en caso de ser necesaria, se realiza mediante canales seguros.
31. Se realizan de copias de respaldo de las bases de datos y código fuente de las aplicaciones. Deben conservarse en un lugar diferente de aquel en el que se encuentren los equipos y servidores.
32. Se cuenta con un Plan de mantenimiento preventivo de servidores y dispositivos de comunicaciones, y su respectivo seguimiento.
33. La institución cuenta con unas Políticas definidas y socializadas para el uso de las Tecnologías de la información.
34. Se realiza un seguimiento para identificar software no corporativo instalado en los equipos de usuario.
35. Revisión periódica: Cada dos años se revisa el grado de implantación del modelo de seguridad sobre los sistemas de información e infraestructura tecnológica de la IPS Universitaria, incluye propuestas asociadas a la resolución de los aspectos susceptibles de mejora.
36. HelpDesk: Existe registros de incidencias o de solicitudes de soporte y se realiza un seguimiento de la resolución y cierre de las mismas.
37. Se cuenta con cláusulas contractuales que considerarán acuerdos de confidencialidad que prevalecerán aun cuando haya finalizado el contrato, con el personal vinculado, prestadores de servicios, aliados y proveedores.

A handwritten signature in black ink, appearing to read 'Luisa F. Correa P.'.

LUISA FERNANDA CORREA PÉREZ

Coordinadora Staff Tic

Supervisora Contrato GHIPS ERP 2024-0194