POLITICA DE CONTROL DE ACCESO

Con el propósito de proteger los activos de información y cumplir con estándares de seguridad reconocidos internacionalmente, se establece la Política de Control de Acceso de la ESE ISABU. Esta política define las directrices y procedimientos para asegurar un control de acceso seguro y efectivo a los recursos de información de la entidad.

1. OBJETIVO

Establecer un marco de control de acceso que asegure la confidencialidad, integridad y disponibilidad de la información, mitigando los riesgos asociados con accesos no autorizados

2. ALCANCE

Esta política se aplica a todos los sistemas de información administrados por el proceso de Gestión de las TICS y su parque informático de la ESE ISABU – Instituto de Salud de Bucaramanga.

3. RESPONSABLE

- Coordinador de TI
- Líder de sistemas de información
- Líder de infraestructura
- Oficial de seguridad de la información
- Usuarios finales

4. DEFINICIONES

Acuerdo de nivel de servicio (SLA)(ANS): Service Level Agreement (SLA). Un acuerdo entre un proveedor de servicios de Tecnologías de la Información (TI) y un cliente que en este caso será la Oficina de Tecnología e Informática.
Auditoria: La auditoría se refiere a la evaluación sistemática, independiente y documentada para obtener evidencia objetiva y evaluarla de manera imparcial con el fin de determinar en qué medida se cumplen los criterios de auditoría. (ISO/IEC 27001:2022).
Capacidad: El máximo rendimiento que se puede obtener de un Ítem de configuración o Servicio de TI con el objetivo de cumplir los niveles de servicio acordados.
Ciberseguridad: La ciberseguridad se refiere a la protección de los sistemas y datos informáticos contra el acceso no autorizado, el uso malintencionado, la modificación, el robo o la destrucción. La ciberseguridad incluye medidas técnicas, físicas y administrativas para proteger la información. (ISO/IEC 27001:2022).
Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. (mintic, s.f.)
Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. (mintic, s.f.)
Incidente de seguridad de la información: Un incidente de seguridad en informática es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización, en el caso de que disponga de ella.
Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.
Información: Datos relacionados que tienen significado para la entidad1. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. (mintic, s.f.)

Riesgos: Los riesgos se refieren a la posibilidad de que ocurra un evento que pueda tener un impacto negativo en un proyecto, una organización o una persona. Los riesgos pueden ser internos o externos, y pueden ser gestionados mediante la identificación, evaluación y mitigación. (ISO/IEC 27001:2022).
Sistema de Información: Conjunto de aplicaciones, servicios, tecnología de información u otros componentes de manejo de información. (ISO/IEC 27001:2022).
Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información. (mintic, s.f.)
Id.: Un Id. de usuario es un identificador único de cliente mediante el cual un anunciante elige identificar a un usuario que visita su sitio web. (Ayuda de Google Ads, s.f.)
TI.: El concepto de tecnología de la información refiere al uso de equipos de telecomunicaciones y computadoras (ordenadores) para la transmisión, el procesamiento y el almacenamiento de datos. (Pérez Porto, 2014).

5. DESARROLLO

5.1 LINEAMIENTOS GENERALES

La ESE ISABU tiene como objetivo proporcionar la seguridad de la información necesaria a todos los activos de información mediante los diferentes controles de acceso tanto lógicos como físicos. El dueño de la información autorizará los permisos necesarios para acceder a la información propia de las funciones de la entidad.

Cualquier intento de violación de seguridad de la información o de vulnerabilidades de los sistemas internos o externos, ejecutadas por funcionarios o contratistas no autorizados para ello, será considerado como una falta a la política de seguridad de la información.

LA ESE ISABU toma como principio básico para la elaboración de esta política los siguientes principios:

- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información del ISABU, debe ser asignado de acuerdo con la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de la Institución, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.
- Los responsables de la administración de la infraestructura tecnológica y sistemas de información del ISABU asignaran los accesos a plataformas, usuarios y segmentos de red de acuerdo con procesos formales de autorización los cuales deben ser revisados de manera periódica por el área responsable.
- La autorización para el acceso a los sistemas de información debe ser definida y aprobada por la dependencia propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los funcionarios e implementada por el área de Sistemas.
- Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información del ISABU, sea por Internet, o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.
- Todos los funcionarios deberán contar con perfiles y credenciales de acceso a las diferentes plataformas, portales y aplicativos ejecutados sobre la infraestructura del ISABU.
- La asignación de la menor cantidad de privilegios posibles para llevar a cabo una tarea dentro de la infraestructura de TI.
- La concesión de esos privilegios solamente por el tiempo que sea necesario para el desarrollo de las actividades para lo cual fue contratado.
- El alta, la baja o la modificación de los privilegios o cuentas de usuario se realiza por medio del procedimiento de altas y bajas.
- Las cuentas de usuario solo se emitirán después de la respectiva solicitud de creación de usuarios.

- Los ID son únicos y personales.
- El ISABU brinda tecnologías de acceso por VPN para que funcionarios, o algunos usuarios externos puedan ingresar a las plataformas y aplicativos remotamente.
- Las cuentas de usuario son de entera responsabilidad del funcionario, contratista o practicante al que se le asigne. La cuenta es para uso personal e intransferible.
- Si se detecta o sospecha que las actividades de una cuenta de usuario pueden comprometer la integridad y seguridad de la información, el acceso a dicha cuenta será suspendida temporalmente y es reactivada sólo después de haber tomado las medidas necesarias a consideración de la Oficina gestión de las TICS

5.2 POLITICA DE CONTRASEÑAS

Para garantizar la política de control de acceso, LA ESE ISABU, definió una política de contraseñas de la siguiente forma:

- Las contraseñas de las aplicaciones y sistemas de información deben solicitar cambio por primera vez
- La composición de las contraseñas deben ser mínimo de ocho (8) caracteres, alfanumérica, contener mayúsculas, minúsculas y un (1) carácter especial.
- Para las aplicaciones que lo permitan deben tener habilitado doble factor de autenticación(2FA)
- Las contraseñas cuentan con una vigencia de noventa (90) días
- Las contraseñas no pueden ser reutilizadas
- Se realiza bloqueo de pantalla de los equipos de cómputo luego de cinco (5) minutos de inactividad
- Luego de 5 intentos fallidos por acceso al sistema, la cuenta de usuario es bloqueada.

5.3 BLOQUEO DE PANTALLAS

Todos los usuarios son responsables de cerrar la sesión de su computadora al retirarse del puesto. La sesión solo podrá ser desbloqueada mediante la contraseña del usuario. Además, al finalizar sus actividades, se deben cerrar todas las aplicaciones y apagar los equipos.

5.4 ALTAS Y BAJAS DE USUARIOS

El proceso de gestión de las TIC cuenta con un procedimiento establecido para administrar altas y bajas de usuarios. De acuerdo con nuestra política general, la activación de usuarios se realiza en un plazo máximo de 24 horas hábiles después de recibir la solicitud correspondiente. Respecto a la inactivación de usuarios o la modificación de privilegios, estas acciones se llevan a cabo, a más tardar, en la fecha de retiro registrada en la solicitud o en el momento del cambio de la relación laboral. Este proceso garantiza una administración eficiente y oportuna de los accesos, asegurando la seguridad y el cumplimiento de las normativas.

5.5 PROVISIÓN DE ACCESO A LOS USUARIOS

Como política general, la activación de los usuarios se realizará máximo 24 horas hábiles luego de la solicitud de la activación, una vez el requerimiento es gestionado, se activa el procedimiento de aprovisionamiento y entrega de credenciales por parte de sistemas de información o infraestructura.

Como lineamiento general se ejecuta la siguiente actividad:

- Creación de alta de usuario.
- Creación de los diferentes usuarios y contraseñas temporales.
- Las contraseñas temporales asignadas al usuario serán notificadas por correo electrónico para garantizar la seguridad de los datos.

5.6 GESTIÓN DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN DE LOS USUARIOS

Para LA ESE ISABU garantizar la entrega de ID y contraseñas es un aspecto fundamental, es por ello que se garantizan los siguientes lineamientos:

- En el acta de capacitación en seguridad de la información, ciberseguridad y protección de la privacidad se encuentra incluido las condiciones de entrega de contraseñas para la autenticación
- Las contraseñas inicialmente asignadas, son temporales, luego exige cambio luego de su primer uso
- Los ID de usuarios y contraseñas serán trasmitidos por medio de correo electrónico directamente al usuario.
- Se cuenta con política de contraseña seguras y son personales e intransferibles.

5.7 REVISIÓN DE DERECHOS DE ACCESO DE USUARIO

El proceso de Gestión de las TICS define los siguientes controles para establecer una revisión periódica de los permisos de accesos de los usuarios.

- Se revisan los derechos de acceso a la terminación de empleo o cambios en la entidad por medio de su procedimiento de altas y bajas de usuarios.
- Limitar en el tiempo los derechos de acceso con fecha de vencimiento de contraseñas.
- El proceso de gestión de las TICS revisará de manera periódica de acuerdo a la matriz de roles los permisos de los usuarios, en caso de encontrar alguna novedad, dejará el registro el formato de gestión de incidentes de seguridad de la información.

5.8 USO DE LA INFORMACIÓN DE AUTENTICACIÓN SECRETA

LA ESE ISABU define los lineamientos frente al uso correcto de los ID y contraseña de autenticación para toda la entidad.

- Durante el proceso de inducción y sensibilización, se señalará la importancia de que las contraseñas no sean divulgadas.
- No está permitido el uso de registros de contraseñas (papel, archivos etc.).
- Se cuenta con una política definida para la calidad de las contraseñas.
- Se evitará el almacenamiento de contraseñas.
- Se garantiza el cambio de contraseñas iniciales.

5.9 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN

Los sistemas de información y aplicaciones cuentan con las restricciones de control de acceso determinadas, para fortalecer la confidencialidad de la información, es por ello por lo que se cuentan con los siguientes lineamientos:

- Se utiliza menús para controlar el acceso a las distintas funcionalidades.
- Se inhabilitan las funciones de administración a los usuarios habituales.
- Se restringe de forma selectiva derechos de lectura / escritura / eliminación / ejecución etc.
- Se cuenta con cierre de sesión automático por periodo de inactividad.

5.10 PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN

- El inicio de sesión seguro de los sistemas de información y aplicaciones es capaz de corroborar la identidad del usuario.
- Cuando la clasificación de la información lo requiera por política, se considera la autenticación sólida por encima y más allá de la simple identificación de usuario y contraseña.
- Los formularios de acceso se validan solo cuando se han completado evitando mensajes de error con información y tener algún sistema para proteger múltiples intentos de acceso mediante "fuerza bruta"
- Los sistemas de información y aplicaciones registran intentos fallidos al sistema.
- Las contraseñas se trasmiten en un formato encriptado.
- Las sesiones inactivas se cerrarán después de cierto periodo de inactividad.

5.11 ACCESO FISICO A LAS INSTALACIONES

El acceso a las instalaciones del Hospital Local del Norte se gestiona de manera segura mediante control de acceso por parte de una empresa de seguridad privada. En el caso particular del ingreso al Data Center se ha implementado un sistema de control de acceso basado en huella digital. Este enfoque biométrico añade un nivel adicional de autenticación, asegurando que solo personal autorizado tenga acceso a áreas más sensibles. La utilización de la huella digital como método de identificación no solo fortalece la seguridad, sino que también simplifica y agiliza el proceso de ingreso para los colaboradores autorizados.

En conjunto, estas medidas de control de acceso no solo protegen las instalaciones y los recursos internos, sino que también contribuyen a la preservación de la privacidad y la confidencialidad de la información en áreas críticas.

- **PERÍMETRO DE SEGURIDAD FÍSICA**

Con el propósito de proteger las zonas que contienen información y otros controles asociados, se establecen directrices claras para la definición y utilización de perímetros de seguridad. En este contexto, se cuenta controles físicos y tecnológicos, como sistemas de acceso restringido, cámaras de vigilancia y controles de acceso, para asegurar la protección integral de los activos físicos y equipos de cómputo propios de la entidad.

- **ENTRADA FISICA**

Con el objetivo de salvaguardar la zona segura y asegurar la integridad de los controles de entrada, se implementan medidas específicas para el acceso físico a la entidad y a las oficinas. La protección de esta zona se realiza a través de controles de entrada y puntos de acceso adecuados, garantizando una gestión efectiva y segura de la seguridad física.

Asimismo, para el ingreso de invitados, se sigue un proceso anunciado y regulado. Los invitados son anunciados previamente. Este procedimiento garantiza que las visitas sean debidamente registradas y cuenten con la autorización correspondiente para acceder a las instalaciones.

- **SEGURIDAD OFICINAS E INSTALACIONES**

El acceso a las áreas internas de trabajo se protege mediante puertas con cerraduras. Esta capa adicional de seguridad restringe el acceso solo a personal debidamente autorizados.

- **MONITOREO DE LA SEGURIDAD FÍSICA**

En aras de garantizar la seguridad física de las instalaciones, se establece un riguroso sistema de monitoreo continuo para la detección temprana de accesos no autorizados. Este control es responsabilidad exclusiva de la seguridad

privada, el cual opera con su propio sistema de vigilancia, diseñado para garantizar la protección constante de las instalaciones.

El sistema de vigilancia, bajo la supervisión del personal de seguridad del hospital, realiza un monitoreo activo de todos los accesos físicos durante las 24 horas del día, los 7 días de la semana. Este monitoreo incluye la revisión constante de las cámaras de seguridad distribuidas estratégicamente en puntos clave, con el objetivo de identificar cualquier actividad sospechosa o intento de acceso no autorizado.

6. DOCUMENTOS REFERENCIADOS

-, M. d.-M. (2022). *NTC ISO/IEC 27001:2022 Anexo A GTC ISO/IEC 27002:2022, CONTROLES ORGANIZACIONALES 5.15 CONTROL DE ACCESO, 5.16 GESTIÓN DE IDENTIDADES, 5.7 INFORMACIÓN DE AUTENTICACIÓN, 5.18 DERECHOS DE ACCESO.*

-, M. d.-M. (2022). *NTC ISO/IEC 27001:2022 Anexo A GTC ISO/IEC 27002:2022, CONTROLES TECNOLOGICOS 8.5 ATENTICACION SEGURA.*

7. CONTROL DE MODIFICACIONES

CONTROL DE MODIFICACIONES			
Versión	**Fecha**	**Descripción de la Modificación**	**Realizada por**
1	7/02/2024	Emisión inicial del documento	Ingeniero de seguridad y privacidad de la información – Proceso de gestión de TI