Tecnologías de la Información BioCubaFarma

División de Ciberseguridad
Calle 18 N° 4310 e/ 43 Y 47, Miramar. La Habana, Cuba
Teléfono: 72152188-89
www.eti.cu

La Habana, 29 de enero de 2024
"Año 65 de la Revolución"

Propuesta de cómo crear Política de Control de Acceso a Servicios Tecnológicos

1. Preámbulo

La Política de Control de Acceso a Servicios Tecnológicos está enfocada en la definición, establecimiento, implementación, mantenimiento y mejora continua de los accesos lógicos a la información, de manera que los procedimientos que se definan (conforme a las necesidades de protección de los servicios), con sus controles y medidas asociadas, estén encauzados a hacer frente a las amenazas presentes y disminuir la probabilidad de explotación de posibles vulnerabilidades de los elementos básicos de este nuevo contexto digital, siempre enfocada garantizar la confiabilidad en el aseguramiento de la información.

2. Objetivo General

La presente Política debe tener como objetivo controlar y gestionar el acceso lógico a los activos de información asociados a los servicios tecnológicos; los cuales serán restringidos sobre la base de requisitos de Seguridad de la Información y conforme a los recursos disponibles optimizar su utilización.

La finalidad es que los actores involucrados tengan un acceso apropiado y controlado a los sistemas de información y recursos tecnológicos, validando su autentificación, autorización y auditoría.

3. Alcance

La política establecida deberá ser de aplicación obligatoria para todos los actores involucrados con acceso a Servicios Tecnológicos, ya sea a los recursos informáticos y los sistemas de información habilitados. Todos los actores tienen la responsabilidad de conocer y aplicar la presente política.

4. Conceptos

Activos de información: Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Institución cualquiera sea el formato que la contenga y los equipos y sistemas que la soporten. Por ejemplo: dispositivos móviles, tarjetas de accesos, software, equipamiento computacional.

Terceros: Persona u organismo reconocido como independiente y que no forman parte de la institución, se entenderá como también a:

- Terceros temporales

- Proveedores de servicios y de red.
- Proveedores de productos de software y servicios de información.
- Outsourcing de instalaciones y operaciones.
- Servicios de asesoría de seguridad.
- Auditores externos.

Principios de seguridad:

a) Confidencialidad: La información solo podrá ser accedida, modificada y/o eliminada por quienes estén autorizados/as para ello.

b) Disponibilidad: La información deberá estar accesible siempre que se requiera.

c) Integridad: La información deberá preservar su veracidad y fidelidad a la fuente, independientemente del lugar y de la forma de almacenamiento y transmisión.

Modelo de estandarización RBAC: sistema de control de acceso relativamente nuevo que mapea a las estructuras específicas de la organización de una manera que reduce los costos administrativos indirectos y mejora la seguridad. La elección del RBAC permite el cumplimiento de reglas básicas asociadas a la segregación de la asignación de funciones, autorización de funciones y la autorización de permisos, despojándose de las recetas tradicionales de gestión de la seguridad con controles de listas de control de acceso.

Control de acceso lógico: Referido a la restricción de acceso a los datos. Se lleva a cabo mediante técnicas de ciberseguridad como la identificación, autenticación y autorización.

5. Roles y Responsabilidades

Los roles propuestos son, teniendo en cuenta la separación de funciones y tareas hacia lo interno y externo, según el proceso.

Responsabilidades:

1) *Responsabilidad legal y especificación de requisitos*: Dirección de la entidad y Responsables de la Información y del Servicio.

   La responsabilidad legal estará matizada por el cumplimiento estricto del marco legal y resoluciones dispuestas, así como del compromiso de la entidad con la seguridad y su adecuada implantación, gestión y mantenimiento.

2) *Supervisión:* Responsable de la Seguridad acompañado por el Responsable del Sistema para el tratamiento de los datos personales.

Supervisión asociada a la vigilancia del estado de la seguridad, verificando el correcto funcionamiento de las medidas de seguridad adoptadas, así como el cumplimiento de lo establecido legalmente para asegurar que la información no está comprometida. Todo ello mediante la ejecución de controles, auditorías, evaluaciones e investigaciones de incidentes de seguridad.

3) *Operación del sistema de información*: Responsable del Sistema.

La operación tendrá la responsabilidad de llevar a cabo la implementación, configuración y operación de los controles establecidos por el Responsable del Servicio. Monitoreo de indicadores de controles de seguridad.

Responsable	Rol	Funciones
Responsable de la Información	Liderar la definición e implementación de la Política de Control de Acceso a los Servicios Tecnológicos	1. Generar lineamientos y criterios generales. 2. Definir requisitos técnicos necesarios para la materialización de la presente política. 3. Asignar recursos según se requiriera, para la gestión lógica de los activos de información institucionales.
Responsable del Servicio	Gestionar la implementación de la Política de Control de Acceso a los Servicios Tecnológicos	1. Administrar el ciclo de vida de los usuarios a nivel lógico, desde la creación de sus cuentas y accesos a los diferentes sistemas y aplicaciones, hasta la gestión de redes y servicios de red que correspondan. Esto, sin perjuicio de la gestión asociada a todos los demás roles, permisos, accesos y privilegios necesarios para sus operaciones diarias (a partir de requerimientos solicitados de forma previa). 2. Autorizar los derechos de acceso de un usuario a los sistemas y bases de datos que están bajo su gestión. 3. Garantizar la disponibilidad del servicio durante todo el período de empleo de la infraestructura tecnológica.

		4. Realizar las pruebas necesarias para prepararse ante contingencias a fin de garantizar un rápido restablecimiento en caso de incidentes de seguridad. 5. Ofrecer seguridad en el consumo del servicio aplicando mecanismos de acceso a través de protocolos de seguros al proponer y/o definir requisitos técnicos necesarios para la materialización de la presente política.
Responsable de la Seguridad	Coordinar los avances en la implementación y funcionamiento de la Política y sus Procedimientos	1. Coordinar el análisis, levantamiento y documentación de los procesos de la Institución en temáticas referidas a Control de Acceso Lógico. 2. Registrar los dispositivos para acceder a la infraestructura tecnológica, garantizando la confidencialidad del usuario a operar con la misma. 3. Realizar chequeos de seguridad que garanticen los principios de seguridad para la infraestructura. 4. Supervisar la implementación de los mecanismos de seguridad a la Infraestructura Tecnológica que garanticen la confidencialidad, la integridad, el control de accesos, la autenticación y el no repudio, según corresponda. 5. Establecer niveles de seguridad para el manejo de la infraestructura por diferentes tipos de usuarios. 6. Definir que herramientas de monitoreo se utilizarán para la detección de incidentes sobre la Infraestructura.
	Asesorar y apoyar en	1. Realizar salvas de datos con la regularidad requerida en cada caso a fin de garantizar su restablecimiento en caso de incidentes de seguridad.

Responsable del Sistema	temáticas relacionadas al control de acceso a los Servicios Tecnológicos	2. Realizar toma de requisitos funcionales para aplicar mejoras y corregir no conformidades. 3. Establecer separación de roles de control de acceso para los usuarios que interactúan con los recursos/servicios. 4. Gestionar y/o escalar los requerimientos de acceso lógico 5. Controlar los accesos a la información contenidos en los recursos/servicios sobre la base de requisitos de seguridad.
Usuario	Colaborar con la Implementación de la Política de Control de Acceso a los Servicios Tecnológicos	1. Los usuarios que operan directamente con los recursos/servicios, están en la obligación de notificar cualquier no conformidad o deficiencia identificada en su cuenta, a los máximos responsables de la Infraestructura tecnológica 2. Los usuarios serán responsables del manejo de sus credenciales para operar en los recursos/servicios (identificación, autenticación y control de acceso).

6. Definiciones y Normativas Vigentes

1. Para acceder a los servicios tecnológicos los usuarios debe tener relación laboral con la Institución, o contar con la autorización a través de un modelo de negocio conciliado con los responsables del recurso/servicio habilitado para su acceso.
2. Derechos de acceso del usuario (proceso detallado):
   - Emisión de los privilegios o cuentas de usuario
   - Modificación de privilegios
   - Revocación de privilegios
   - Determinación del ciclo de vida del ID de usuario

3. Quienes utilicen los recursos/servicios tecnológicos son responsables por su cuenta de usuario y contraseña para el uso y acceso a los recursos informáticos.
4. Las cuentas de usuario contarán con los privilegios mínimos necesarios para acceder a los diferentes recursos/servicios, coherentes con el desarrollo de las funciones asignadas.
5. Se debe efectuar la implementación de controles de accesos mediante técnicas de autentificación, autorización y contabilidad, basados en el Protocolo de Seguridad Informática AAA, teniendo en cuenta el modelo RBAC.
6. Queda prohibida la utilización de la infraestructura tecnológica para obtener acceso lógico no autorizado a la información y a otros recursos/servicios del Proveedor, o de terceros.
7. Queda prohibido proporcionar a personal externo, información de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del Proveedor de Servicios Tecnológicos.
8. Se deben revocar en forma inmediata los derechos de acceso lógico a aquellos usuarios que se desvinculan del uso de los recursos/servicios en forma permanente. Esto, previa notificación del Responsable del Sistema.
9. Los accesos con más alto privilegio tanto como ROOT o Administrador, deben ser restringidos y controlados por el Responsable del Servicio, dado su alto riesgo en la continuidad operacional de la Infraestructura Tecnológica.
10. Las reglas de acceso a la red a través de los puertos estarán basadas en la premisa: "todo está restringido, a menos que este expresamente permitido".
11. Los recursos/servicios en la Infraestructura tecnológica que requieran de conexión remota para su acceso, emplearán conexiones seguras a través de una Solución VPN brindada por el Proveedor de Servicios.

7. Incumplimiento

El incumplimiento de esta política de control de acceso traerá consigo las consecuencias legales que apliquen a la normativa de la Institución, también definidas en los Aviso Legal dispuestos en los recursos, incluyendo lo establecido en el marco regulatorio cubano en cuanto a seguridad de la información.

8. Revisiones

Con el fin de asegurar su vigencia, actualización y mejora continua, la presente Política deberá ser revisada al menos una vez por año por parte del Responsable de la Información de Conjunto con los Responsables del Servicio, Seguridad y Sistema

respectivamente en el espacio empresarial, proponiendo de manera transparente, las mejoras a implementar o la mantención de ésta.

La forma de verificar la realización de esta revisión, será el acta del espacio empresarial donde se tramite el tema, de la sesión correspondiente.

9. Relación con otras políticas institucionales

La presente Política de Control de Acceso a los Servicios Tecnológicos debe ser aplicada de manera adicional con las demás políticas internas y gubernamentales, así como otros documentos pertinentes.

10. Mecanismos de Difusión

La difusión de la presente política se realizará mediante el Plan de Seguridad Informática (público), e informando a todos los responsables, las políticas vigentes, su lugar de almacenamiento e invitándolos a revisarlas como parte de sus responsabilidades.